On the Functional Equation
of the Artin L-functions

Robert P. Langlands

TABLE OF CONTENTS

O. Introduction

In this paper I want to consider not just the L-functions introduced by Artin [1] but the more general functions introduced by Weil [15]. To define these one needs the notion of a Weil group as described in [3]. This notion will be explained in the first paragraph. For now a rough idea will suffice. If E is a global field, that is an algebraic number field of finite degree over the rationals or a function field over a finite field, C_E will be the idéle class group of E. If E is a local field, that is the completion of a global field at some place [16], archimedean or nonarchimedean, C_E will be the multiplicative group of E. If K/E is a finite Galois extension the Weil group $W_{K/E}$ is an extension of $\mathfrak{G}(K/E)$, the Galois group of K/E, by C_K. It is a locally compact topological group.

If $E \subseteq E' \subseteq K$ and K/E is finite and Galois $W_{K/E'}$ may be regarded as a subgroup of $W_{K/E}$. It is closed and of finite index. If $E \subseteq K \subseteq L$ there is a continuous map of $W_{L/E}$ onto $W_{K/E}$. Thus any representation of $W_{K/E}$ may be regarded as a representation of $W_{L/E}$. In particular the representations ρ_1 of $W_{K_1/E}$ and ρ_2 of $W_{K_2/E}$ will be called equivalent if there is a Galois extension L/E containing K_1/E and K_2/E such that ρ_1 and ρ_2 determine equivalent representations of $W_{L/E}$. This allows us to refer to equivalence classes of representations of the Weil group of E without mentioning any particular extension field K.

In this paper a representation of $W_{K/E}$ is understood to be a continuous representation ρ in the group of invertible linear transformations of a finite-dimensional complex vector space which is such that $\rho(w)$ is diagonalizable, that is semisimple, for all w in $W_{K/E}$. Any one-dimensional representation of $W_{K/E}$ can be obtained by inflating a one-dimensional representation of $W_{E/E} = C_E$. Thus equivalence classes of one-dimensional representations of the Weil group of E correspond to quasi-characters of C_E, that is, to continuous homomorphisms of C_E into $\mathbb{C}^\times$.

Suppose E is a local field. There is a standard way of associating to each equivalence class ω of one-dimensional representations a meromorphic function $L(s,\omega)$. Suppose ω corresponds to the quasi-character χ_E. If E is nonarchimedean and ϖ_E is a generator of the prime ideal $\mathcal{P}_E$ of O_E, the ring of integers in E, we set

$$L(s,\omega) = \frac{1}{1 - \chi_E(\varpi_E)\,|\varpi_E|^s}$$

if χ_E is unramified. Otherwise we set $L(s,\omega) = 1$. If $E = \mathbb{R}$ and

$$\chi_E(x) = (\operatorname{sgn} x)^m \; |x|^r$$

with m equal to 0 or 1 we set

$$L(s,\omega) = \pi^{-\frac{1}{2}\,(s+r+m)}\;\Gamma\left(\frac{s+r+m}{2}\right).$$

If $E = \mathbb{C}$ and $z \in E$ then, for us, $|z|$ will be the square of the ordinary absolute value. If

$$\chi_E(z) = |z|^r z^m \bar{z}^n$$

where m and n are integers such that $m+n \geq 0$, $mn = 0$, then

$$L(s,\omega) = 2\,(2\pi)^{-(s+r+m+n)}\;\Gamma(s+r+m+n)$$

It is not difficult to verify, and we shall do so later, that it is possible, in just one way, to define $L(s,\omega)$ for all equivalence classes so that it has the given form when ω is one-dimensional, so that

$$L(s,\omega_1 \oplus \omega_2) = L(s,\omega_1)\, L(s,\omega_2)$$

so that if E' is a separable extension of E and ω is the equivalence class of the representation of the Weil group of E induced from a representation of the Weil group of E' in the class Θ then $L(s,\omega) = L(s,\Theta)$.

Now take E to be a global field and ω an equivalence class of representations of the Weil group of E. It will be seen later how, for each place v, ω determines an equivalence class ω_v of representations of the Weil group of the corresponding local field E_v. The product

$$\prod\nolimits_v L(s,\omega_v)$$

which is taken over all places, including the archimedean ones, will converge if the real part of s is sufficiently large. The function it defines can be continued to a function $L(s,\omega)$ meromorphic in the whole complex plane. This is the Artin L-function associated to ω. It is fairly well-known that if $\widetilde{\omega}$ is the class contragredient to ω there is a functional equation connecting $L(s,\omega)$ and $L(1-s,\widetilde{\omega})$.

The factor appearing in the functional equation can be described in terms of the local data. To see how this is done we consider separable extensions E of the fixed local field F. If Ψ_F is a non-trivial additive character of F let $\psi_{E/F}$ be the non-trivial additive character of E defined by

$$\psi_{E/F}(x) = \psi_F(S_{E/F}x)$$

where $S_{E/F}x$ is the trace of x. We want to associate to every quasi-character χ_E of C_E and every non-trivial additive character ψ_E of E a non-zero complex number $\Delta(\chi_E,\psi_E)$. If E is nonarchimedean, if $\mathfrak{P}_E^m$ is the conductor of χ_E, and if $\mathfrak{P}_E^{-n}$ is the largest ideal on which ψ_E is trivial choose any γ with $O_E\gamma = \mathfrak{P}_E^{m+n}$ and set

$$\Delta(\chi_E,\psi_E) = \chi_E(\gamma)\ \frac{\int_{U_E}\psi_E\ \left(\frac{\alpha}{\gamma}\right)\ \chi_E^{-1}(\alpha)d\alpha}{\left|\int_{U_E}\psi_E\ \left(\frac{\alpha}{\gamma}\right)\chi_E^{-1}(\alpha)d\alpha\right|}.$$

The right side does not depend on γ. If $E = \mathbb{R}$,

$$\chi_E(x) = (\mathrm{sgn} x)^m\ |x|^r$$

with m equal to 0 or 1, and $\psi_E(x) = e^{2\pi i u x}$ then

$$\Delta(\chi_E,\psi_E) = (i\ \mathrm{sgn} u)^m\ |u|^r.$$

If $E = \mathbb{C},\ \psi_{\mathbb{C}}(z) = e^{4\pi i\ \mathrm{Re(wz)}}$, and

$$\chi_{\mathbb{C}}(z) = |z|^r z^m \bar{z}^n$$

with $m+n \geq 0,\ \ mn = 0$ then

$$\Delta(\chi_{\mathbb{C}},\ \psi_{\mathbb{C}}) = i^{m+n}\ \chi_{\mathbb{C}}(w).$$

The bulk of this paper is taken up with a proof of the following theorem.

Theorem A

Suppose F is a given local field and ψ_F a given non-trivial additive character of F. It is possible in exactly one way to assign to each separable extension E of F a complex number $\lambda(E/F,\psi_F)$ and to each equivalence class ω of representations of the Weil group of E a complex number $\varepsilon(\omega,\Psi_{E/F})$ such that

(i) *If ω corresponds to the quasi-character χ_E then*

$$\varepsilon(\omega,\psi_{E/F})=\Delta(\chi_E,\psi_{E/F}).$$

(ii)

$$\varepsilon(\omega_1\oplus\omega_2,\ \psi_{E/F})=\varepsilon(\omega_1,\ \psi_{E/F})\ \varepsilon(\omega_2,\ \psi_{E/F}).$$

(iii) *If ω is the equivalence class of the representation of the Weil group of F induced from a representation of the Weil group of E in the class θ then*

$$\varepsilon(\omega,\psi_F)=\lambda(E/F,\ \psi_F)^{\dim\theta}\ \varepsilon(\theta,\psi_{E/F}).$$

α_F^s will denote the quasi-character $x\longrightarrow|x|_F^s$ of C_F as well as the corresponding equivalence class of representations. Set

$$\varepsilon(s,\omega,\psi_F)=\varepsilon\left(\alpha_F^{s-\frac{1}{2}}\otimes\omega,\ \psi_F\right).$$

The left side will be the product of a non-zero constant and an exponential function.

Now take F to be a global field and ω to be an equivalence class of representations of the Weil group of F. Let $\mathbb{A}$ be the adéle group of F and let ψ_F be a non-trivial character of $\mathbb{A}/F$. For each place v let ψ_v be the restriction of ψ_F to F_v. ψ_v is non-trivial for each v and almost all the functions $\varepsilon(s,\omega_v,\psi_v)$ are identically 1 so that we can form the product

$$\prod\nolimits_v\ \varepsilon(s,\omega_v,\psi_v).$$

Its value will be independent of ψ_F and will be written $\varepsilon(s,\omega)$.

Theorem B

The functional equation of the L-function associated to ω is

$$L(s,\omega)=\varepsilon(s,\omega)\ L(1-s,\widetilde{\omega}).$$

This theorem is a rather easy consequence of the first theorem together with the functional equations of the Hecke L-functions.

For archimedean fields the first theorem says very little. For nonarchimedean fields it can be reformulated as a collection of identities for Gaussian sums. Four of these identities which we formulate as our four main lemmas are basic. All the others can be deduced from them by simple group-theoretic arguments. Unfortunately the only way at present that I can prove the four basic identities is by long and involved, although rather elementary, computations. However Theorem A promises to be of such importance for the theory of automorphic forms and group representations that we can hope that eventually a more conceptual proof of it will be found. The first and the second, which is the most difficult, of the four main lemmas are due to Dwork [6]. I am extremely grateful to him not only for sending me a copy of the dissertation of Lakkis [9] in which a proof of these two lemmas is given but also for the interest he has shown in this paper.

Chapter One.

Weil Groups

The Weil groups have many properties, most of which will be used at some point in the paper. It is impossible to describe all of them without some prolixity. To reduce the prolixity to a minimum I shall introduce these groups in the language of categories.

Consider the collection of sequences

$$S : C \xrightarrow{\lambda_1} G \xrightarrow{\mu} \mathfrak{G}$$

of topogical groups where λ is a homeomorphism of C with the kernel of μ and μ induces a homeomorphism of $G/\lambda C$ with $\mathfrak{G}$. Suppose

$$S_1 : C_1 \xrightarrow{\lambda_1} G_1 \xrightarrow{\mu_2} \mathfrak{G}_1$$

is another such sequence. Two continuous homomorphisms φ and ψ from G to G_1 which take C into C_1 will be called equivalent if there is a c in C_1 such that $\psi(g) = c\varphi(g)c^{-1}$ for all g in G. $\mathcal{S}$ will be the category whose objects are the sequences S and $\mathrm{Hom}_{\mathcal{S}_0}(\mathrm{S}, \mathrm{S}_1)$ will be the collection of these equivalence classes. $\mathcal{S}$ will be the category whose objects are the sequences S for which C is locally compact and abelian and $\mathfrak{G}$ is finite; if S and S_1 belong to $\mathcal{S}$

$$\mathrm{Hom}_{\mathcal{S}}(\mathrm{S}, \mathrm{S}_1) = \mathrm{Hom}_{\mathcal{S}_0}(\mathrm{S}, \mathrm{S}_1).$$

Let P_1 be the functor from $\mathcal{S}$ to the category of locally compact abelian groups which takes S to C and let P_2 be the functor from $\mathcal{S}$ to the category of finite groups which takes S to $\mathfrak{G}$. We have to introduce one more category $\mathcal{S}_{1,0}$. The objects of $\mathcal{S}_1$ will be the sequences on $\mathcal{S}$ for which G^c, the commutator subgroup of G, is closed. Moreover the elements of $\mathrm{Hom}_{\mathcal{S}_1}(\mathrm{S}, \mathrm{S}_1)$ will be the equivalence classes in $\mathrm{Hom}_{\mathcal{S}}(S, S_1)$ all of whose members determine homeomorphisms of G with a closed subgroup fo finite index in G_1.

If S is in $\mathcal{S}_1$ let $V(S)$ be the topological group G/G^c. If $\Phi \in \mathrm{Hom}_{\mathcal{S}_1}(S, S_1)$ let φ be a homeomorphism in the class Φ and let $\overline{G} = \varphi(G)$. Composing the map $G_1/G_1^c \longrightarrow \overline{G}/\overline{G}^c$ given by the transfer with the map $\overline{G}/\overline{G}^c \longrightarrow G/G^c$ determined by the inverse of φ we obtain a map $\Phi_v : V(S_1) \longrightarrow V(S)$ which depends only on Φ. The map $S \longrightarrow V(S)$ becomes a contravariant functor from $\mathcal{S}_1$ to the category of locally compact abelian groups. If S is the sequence

$$C \longrightarrow G \longrightarrow \mathfrak{G}$$

the transfer from G to C determines a homomorphism τ from G/G^c to the group of G-invariant elements in C. τ will sometimes be regarded as a map from G to this subgroup.

The category $\mathcal{E}$ will consist of all pairs K/F where F is a global or local field and K is a finite Galois extension of F. $\mathrm{Hom}(K/F,\, L/E)$ will be a certain collection of isomorphisms of K with a subfield of L under which F corresponds to a subfield of E. If the fields are of the same type, that is all global or all local we demand that E be finite and separable over the image of F. If F is global and E is local we demand that E be finite and separable over the closure of the image of F. I want to turn the map which associates to each K/F the group C_K into a contravariant functor which I will denote by

C^*. If $\varphi : K/F \longrightarrow L/E$ and F and E are of the same type let K_1 be the image of K in L and let φ_{C^*} be the composition of N_{L/K_1} with the inverse of φ. If F is global and E is local let K_1 be the closure in L of the image of K. As usual C_{K_1} may be considered a subgroup of the group of idèles of K. φ_{C^*} is the composition of N_{L/K_1} with the projection of the group of idèles onto C_K.

If K is given let $\mathcal{E}^K$ be the subcategory of $\mathcal{E}$ whose objects are the extensions with the larger field equal to K and whose maps are equal to the identity on K. Let C_* be the functor on $\mathcal{E}^K$ which takes K/F to C_F. If F is given let $\mathcal{E}_F$ have as objects the extensions with the smaller field equal to F. Its maps are to equal the identity on F.

A Weil group is a contravariant functor W from $\mathcal{E}$ to $\mathcal{S}$ with the following properties:

(i) *$P_1 \circ W$ is C^*.*

(ii) *$P_2 \circ W$ is the functor $\mathfrak{G} : L/F \longrightarrow \mathfrak{G}(L/F)$.*

(iii) *If $\varphi \in \mathfrak{G}(L/F) \subseteq \mathrm{Hom}(L/F, L/F)$ and g is any element of $W_{L/F}$, the middle group of the sequence $W(L/F)$, whose image in $\mathfrak{G}(L/F)$ is φ then the map $h \longrightarrow ghg^{-1}$ is in the class φ_w.*

(iv) *The restriction of W to $\mathcal{E}^K$ takes values in $\mathcal{S}_1$. Moreover, if K/F belongs to $\mathcal{E}^K$*

$$\tau\colon W_{K/F}/W^c_{K/F} \longrightarrow C_F$$

is a homeomorphism. Finally, if $\varphi : K/F \longrightarrow K/E$ is the identity on K and $\Phi = \varphi_w$ then the diagram

$$\begin{array}{ccc} W_{K/F}/W^c_{K/F} & \xrightarrow{\Phi_v} & W_{K/E}/W^c_{K/E} \\ \tau\downarrow & & \downarrow\tau \\ C_F & \xrightarrow[\varphi_{C^*}]{} & C_E \end{array}$$

is commutative and if $\psi : F/F \longrightarrow K/F$ is the imbedding, ψ_W is τ.

Since the functorial properties of the Weil group are not all discussed by Artin and Tate, we should review their construction of the Weil group pointing out, when necessary, how the functorial properties arise. There is associated to each K/F a fundamental class $\alpha_{K/F}$ in $H^2(\mathfrak{G}(K/F), C_K)$. The group $W(K/F)$ is any extension of $\mathfrak{G}(K/F)$ by C_K associated to this element. We have to show, at least, that if $\varphi : K/F \longrightarrow L/E$ the diagram

$$\begin{array}{ccccccccc} 1 & \longrightarrow & C_L & \longrightarrow & W_{L/E} & \longrightarrow & \mathfrak{G}(L/E) & \longrightarrow & 1 \\ & & \downarrow\varphi_{C^*} & & & & \downarrow\varphi_{\mathfrak{G}} & & \\ 1 & \longrightarrow & C_K & \longrightarrow & W_{K/F} & \longrightarrow & \mathfrak{G}(K/F) & \longrightarrow & 1 \end{array}$$

can be completed to a commutative diagram by inserting $\widehat{\varphi} : W_{L/E} \longrightarrow W_{K/F}$. The map φ_{C^*} commutes with the action of $\mathfrak{G}(L/E)$ on C_L and C_K so that $\widehat{\varphi}$ exists if and only if $\varphi_{C^*}(\alpha_{L/E})$ is the restriction $\varphi^*_{\mathfrak{G}}(\alpha_{K/F})$ of $\varphi_{K/F}$ to $\mathfrak{G}(L/E)$. If this is so, the collection of equivalence classes to which $\widehat{\varphi}$ may belong is a principal homogeneous space of $H^1(\mathfrak{G}(L/E), C_K)$. In particular, if this group is trivial, as it is when $\varphi_{\mathfrak{G}}$ is an injection, the class of $\widehat{\varphi}$ is uniquely determined.

An examination of the definition of the fundamental class and shows that it is canonical. In other words, if φ is an isomorphism of K and L and of F and E, then $\varphi^*_{\mathfrak{G}}(\alpha_{K/F}) = \varphi^{-1}\alpha_{L/E} = \varphi_{C^*}(\alpha_{L/E})$. If $K = L$ and φ is the identity on K, the relation $\varphi^*_{\mathfrak{G}}(\alpha_{K/F}) = \alpha_{L/E} = \varphi_{C^*}(\alpha_{L/E})$ is one of the basic properties of the fundamental class. Thus in these two cases $\widehat{\varphi}$ exists and its class is unique.

Now take K to be global and L local. Suppose at first that K is contained in L, that its closure is L, and that $F = K \cap E$. Then, by the very definition of $\alpha_{K/F}$, $\varphi^*_{\mathfrak{G}}(\alpha_{K/F}) = \varphi_{C^*}(\alpha_{L/E})$. More generally, if K_1 is the image of K in L, and F_1 the image of F in E, we can write φ as $\varphi_1\varphi_2\varphi_3$ where $\varphi_3 : K/F \longrightarrow K_1/F_1$, $\varphi_2 : K_1/F_1 \longrightarrow K_1/K_1 \cap E$, and $\varphi_1 : K_1/K_1 \cap E \longrightarrow L/E$. $\widehat{\varphi}_3$ and $\widehat{\varphi}_2$ exist. If the closure of K_1 is L then $\widehat{\varphi}_1$ and therefore $\widehat{\varphi} = \widehat{\varphi}_3\widehat{\varphi}_2\widehat{\varphi}_1$ also exist. The class of $\widehat{\varphi}$ is uniquely determined.

Artin and Tate show that $W^c_{K/F}$ is a closed subgroup of $W_{K/F}$ and that τ is a homeomorphism of $W_{K/F}/W^c_{K/F}$ and C_F. Granted this, it is easy to see that the restriction of W to ξ^K takes values in $\mathcal{S}_1$. Suppose we have the collection of fields in the diagram with L and K normal over F and L and K' normal over F'. Let α, β, and ν be the imbeddings $\alpha : L/F \longrightarrow L/K,\ \ \beta : L/F' \longrightarrow L/K',\ \ \nu : L/F \longrightarrow L/F'$.

$$\begin{tikzcd}[arrows=dash]
L \arrow[dd] \arrow[dr] & \\
 & K' \arrow[dl] \arrow[dd] \\
K \arrow[dd] & \\
 & F' \arrow[dl] \\
F &
\end{tikzcd}$$

We have shown the existence of $\widehat{\alpha}, \widehat{\beta}$, and $\widehat{\nu}$. It is clear that $\widehat{\nu}\widehat{\beta}(W_{L/K'})$ is contained in $\widehat{\alpha}(W_{L/K})$. Thus we have a natural map

$$\pi : \widehat{\nu}\widehat{\beta}(W_{L/K'})/\widehat{\nu}\widehat{\beta}(W^c_{L/K'}) \longrightarrow \widehat{\alpha}(W_{L/K})/\widehat{\alpha}(W^c_{L/K}).$$

Let us verify that the diagram

$$\begin{array}{ccc}
W_{L/K}/W^c_{L/K'} \longrightarrow \widehat{\nu}\widehat{\beta}(W_{L/K'})/\widehat{\nu}\widehat{\beta}(W^C_{L/K'}) & \xrightarrow{\pi} \widehat{\alpha}(W_{L/K})/\widehat{\alpha}(W^c_{K/K}) \longrightarrow & W_{L/K}/W^c_{L/K} \\
\downarrow \tau & & \downarrow \tau \\
C_{k'} & \xrightarrow{\hspace{6em} N_{K'/K} \hspace{6em}} & C_k
\end{array} \qquad \text{(A)}$$

is commutative. To see this let $W_{L/K'}$ be the disjoint union

$$U^r_{i=1}\ C_K h_i.$$

Then we can choose $h'_i,\ g'_j,\ \ 1 \le i \le r,\ \ 1 \le j \le s$ so that $W_{L/K}$ is the disjoint union

$$\bigcup_{i=1}^{r} \quad \bigcup_{j=1}^{s} \quad C_K\, g'_j h'_i$$

and $\widehat{\nu}\widehat{\beta}(h'_i) = \widehat{\alpha}(h_i)$. Using these coset representatives to compute the transfer one immediately verifies the assertion. We should also observe that the transitivity of the transfer implies the commutativity of the diagram

$$\begin{array}{ccc}
W_{K/F}/W^c_{K/F} & \xrightarrow{\Phi_v} & W_{K/F'}/W^c_{K/F'} \\
\tau \downarrow & & \downarrow \\
C_F & \xrightarrow[\varphi_{C^*}]{} & C_{F'}
\end{array}$$

if Φ is the class of an imbedding $\widehat{\varphi}$ where φ is an imbedding $K/F \longrightarrow K/F'$.

We have still not defined φ_W for all φ. However we have defined it when φ is an isomorphism of the two larger fields or when the second large field is the closure of the first. Moreover the definition is such that the third condition and all parts of the fourth condition except the last are satisfied. The last condition of (iv) can be made a definition without violating (i) and (ii). What we do now is show that there is one and only one way of extending the definition of φ_W to all φ without violating conditions (i) or (ii) and the functorial property.

Suppose $F \subseteq K \subseteq L,\ \ K/F$ and L/F are Galois, and ψ is the imbedding $L/F \longrightarrow L/K$. It is observed in Artin and Tate that there is one and only class of maps $\{\theta\}$ which make the following diagram commutative

$$\begin{array}{ccccccccc} 1 \longrightarrow & W_{L/K}/W^c_{L/K} & \longrightarrow & \widehat{\psi}W_{L/K}/\widehat{\psi}W^c_{L/K} & \longrightarrow & W_{L/F}/\widehat{\psi}W^c_{L/K} & \longrightarrow & W_{L/F}/\widehat{\psi}W_{L/K} & \longrightarrow 1 \\ & \tau\downarrow & & & & \downarrow\theta & & \downarrow & \\ 1 \longrightarrow & C_K & & \longrightarrow & & W_{K/F} & \longrightarrow & \mathfrak{G}(K/F) & \longrightarrow 1. \end{array}$$

The homomorphism on the right is that deduced from

$$W_{L/F}/W_{L/K} = \mathfrak{G}(L/F)/\mathfrak{G}(L/K) \simeq \mathfrak{G}(K/F).$$

Let φ, μ, and ν be imbeddings $\varphi : K/F \longrightarrow L/F,\ \ \mu : K/K \longrightarrow L/K,\ \ \nu : K/F \longrightarrow K/K$. Then $\psi \circ \varphi = \mu \circ \nu$, so that $\widehat{\nu} \circ \widehat{\mu} = \widehat{\varphi} \circ \widehat{\psi}$. Moreover $\widehat{\nu} \circ \widehat{\mu}$ is the composition of the map $\tau : W_{L/K} \longrightarrow C_K$ and the imbedding of C_K in $W_{K/F}$. Thus the kernel of $\widehat{\varphi}$ contains $\widehat{\psi}W^c_{L/K}$ so that $\widehat{\varphi} \circ \widehat{\psi}$ restricted to $W_{L/K}/W^c_{L/K}$ must be τ and the only possible choice for $\widehat{\varphi}$ is, apart from equivalence, θ. To see that this choice does not violate the second condition observe that the restriction of τ to C_L will be $N_{L/K}$ and that $\widehat{\psi}$ is the identity on C_L.

Denote the map $\theta : W_{L/F} \longrightarrow W_{K/F}$ by $\theta_{L/K}$ and the map $\tau : W_{K/F} \rightarrow C_K$ by $\tau_{K/F}$. It is clear that $\tau_{K/F} \circ \theta_{L/K}$ is the transfer from $W_{L/F}/W^c_{L/F}$ to $\widehat{\psi}W_{L/K}/\widehat{\psi}W^c_{L/K}$ followed by the transfer from $\widehat{\psi}W_{L/K}/\widehat{\psi}W^c_{L/K}$ to $\widehat{\psi}C_L = C_F$. By the transitivity of the transfer $\tau_{K/F} \circ \theta_{L/K} = \tau_{L/F}$. It follows immediately that if $F \subseteq K \subseteq L \subseteq L'$ and all extensions are Galois the map $\theta_{L'/K}$ and $\theta_{L/K}\theta_{L'/L}$ are in the same class.

Suppose that φ is an imbedding $K/F \longrightarrow K'/F'$ and choose L so that $K' \subseteq L$ and L/F is Galois. Let $\psi : K'/F' \longrightarrow L/F',\ \ \mu : K/F \longrightarrow L/F,\ \ \nu : L/F \longrightarrow L/F'$ be imbeddings. Then $\psi \circ \varphi = \nu \circ \mu$ so that $\widehat{\mu} \circ \widehat{\nu} = \widehat{\varphi} \circ \widehat{\psi}$. If $\alpha : L/F \longrightarrow L/K,\ \ \beta : L/F' \longrightarrow L/K'$ are the imbeddings then the kernel of $\widehat{\psi}$ is $\widehat{\nu}\widehat{\beta}W^c_{L/K'}$ which is contained in $\widehat{\alpha}W^c_{L/K}$ the kernel of $\widehat{\mu}$. Thus there is only one way to define $\widehat{\varphi}$ so that $\widehat{\mu} \circ \widehat{\nu} = \widehat{\varphi} \circ \widehat{\psi}$. The diagram

$$\begin{array}{ccccc} W_{L/K'}/W^c_{L/K'} & \xrightarrow{\widehat{\beta}} & W_{L/F'}/\widehat{\beta}W^c_{L/K'} & \xrightarrow{\qquad\widehat{\psi}\qquad} & W_{K'/F'} \\ & & \downarrow\ \widehat{\nu} & & \downarrow\ \widehat{\varphi} \\ & & W_{L/F}/\widehat{\nu}\widehat{\beta}W^c_{L/K'} & \longrightarrow W_{L/F}/\widehat{\alpha}W^c_{L/K} \xrightarrow{\widehat{\mu}} & W_{K/F} \end{array}$$

will be commutative. Since $\widehat{\psi}\circ\widehat{\beta}=\tau_{L/K'}$ and $\widehat{\mu}\circ\widehat{\alpha}=\tau_{K/F}$ diagram (A) shows that $\widehat{\varphi}$ has the required effect on C_K.

To define φ_W in general, we observe that every φ is the composition of isomorphisms, imbeddings of fields of the same type, and a map $K/F \longrightarrow K'/F'$ where K is global, K' is local, K' is the closure of K, and $F = F'\cap K$. Of course the identity

$$(\varphi\circ\psi)_W = \psi_W\varphi_W$$

must be verified. I omit the verification which is easy enough. The uniqueness of the Weil groups in the sense of Artin and Tate implies that the functor W is unique up to isomorphism.

The sequence

$$S(n,\mathbb{C}):\;\; GL(n,\mathbb{C}) \xrightarrow{\text{id}} GL(n,\mathbb{C}) \longrightarrow 1$$

belongs to $\mathcal{S}_1$. If $S : C \longrightarrow G \longrightarrow \mathfrak{G}$ belongs to $\mathcal{S}_1$ then

$$\mathrm{Hom}_{\mathcal{S}_0}(S,\; S(n,\mathbb{C}))$$

is the set of equivalence classes of n-dimensional complex representations of G. Let $\Omega_n(S)$ be the set of all Φ in $\mathrm{Hom}_{\mathcal{S}_0}(S, S(n,\mathbb{C}))$ such that, for each $\varphi\in\Phi$, $\varphi(g)$ is semi-simple for all g in G. $\Omega_n(S)$ is a contravariant functor of S and so is $\Omega(S)=\bigcup_{n=1}^{\infty}\Omega_n(S)$. On the category $\mathcal{S}_1$, it can be turned into a covariant functor. If $\psi : S \longrightarrow S_1$, if $\Phi\in\Omega(S)$, and if $\varphi\in\Phi$, let ψ associate to Φ the matrix representations corresponding to the induced representation $\mathrm{Ind}(G_1,\psi(G),\varphi\circ\psi^{-1})$. It follows from the transitivity of the induction process that Ω is a covariant functor of $\mathcal{S}_1$.

To be complete a further observation must be made.

Lemma 1.1 *Suppose H is a subgroup of finite index in G and ρ is a finite-dimensional complex representation of H such that $\rho(L)$ is semi-simple for all h in H. If*

$$\sigma = \mathrm{Ind(G,H,}\rho)$$

then $\sigma(g)$ is semi-simple for all g.

H contains a subgroup H_1 which is normal and of finite index in G, namely, the group of elements acting trivially on $H\backslash G$. To show that a non-singular matrix is semi-simple one has only to show that some power of it is semi-simple. Since $\sigma^n(g)=\sigma(g^n)$ and g^n belongs to H_1 for some n we need only show that $\sigma(g)$ is semi-simple for g in H_1. In that case $\sigma(g)$ is equivalent to $\sum_{i=1}^{r}\oplus\rho(g_igg_i^{-1})$ if G is the disjoint union

$$\bigcup_{i=1}^{r} Hg_i$$

Suppose L/F and K/F belong to $\mathcal{E}_F$ and $\varphi\in\mathrm{Hom}_{\mathcal{E}_F}(L/F,K/F)$. Since the maps of the class φ_W all take $W_{K/F}$ onto $W_{L/F}$ the associated map $\Omega(W(L/F))\longrightarrow\Omega(W(K/F))$ is injective. Moreover it is independent of φ. If L_1/F and L_2/F belong to $\mathcal{E}_F$ there is an extension K/F and maps $\varphi_1\in\mathrm{Hom}_{\mathcal{E}_F}(L_1/F,K/F)$, $\varphi_2\in\mathrm{Hom}_{\mathcal{E}_F}(L_2/F,K/F)$. ω_1 in $\Omega(W(L_1/F))$ and ω_2 in $\Omega(W(L_2/F))$ have the same image in $\Omega(W(K/F))$ for one such K if and only if they have the same image for all such K. If this is so we say that ω_1 and ω_2 are equivalent. The collection of equivalence classes will be denoted by $\Omega(F)$. Its members are referred to as equivalence classes of representations of the Weil group of F.

Let $\mathcal{F}$ be the category whose objects are local and global fields. If F and E are of the same type $\mathrm{Hom}_{\mathcal{F}}(F,E)$ consists of all isomorphisms of F with a subfield of E over which E is separable. If F is global and E is local $\mathrm{Hom}_{\mathcal{F}}(F,E)$ consists of all isomorphisms of F with a subfield of E over whose closure E is separable. $\Omega(F)$ is clearly a covariant functor on $\mathcal{F}$. Let $\mathcal{F}_{g\ell}$, and F_{loc} be the subcategories consisting of the global and local fields respectively. Suppose F and E are of the same type and $\varphi \in \mathrm{Hom}_{\mathcal{F}}(F,E)$. If $\omega \in \Omega(E)$ choose K so that ω belongs to $\Omega(W(K/E))$. We may assume that there is an L/F and an isomorphism ψ from L onto K which agrees with φ on F. Then $\psi_W : W_{K/E} \longrightarrow W_{L/F}$ is an injection. Let θ be the equivalence class of the representation

$$\sigma = \mathrm{Ind}(\mathrm{W_{L/F}}, \psi_{\mathrm{W}}(\mathrm{W_{K/E}}),\ \rho \circ \psi_{\mathrm{W}}^{-1})$$

with ρ in ω. I claim that θ is independent of K and depends only on ω and φ. To see this it is enough to show that if $L \subseteq L',\ L'/F$ is Galois, ψ' is an isomorphism from L' to K' which agrees with ψ on L, and ρ' is a representation of $W_{K'/F}$ in ω the class of

$$\sigma' = \mathrm{Ind}(\mathrm{W_{L'/F}},\ \ \psi'_{\mathrm{W}}(\mathrm{W_{K'/E}}),\ \ \rho' \circ \psi'^{-1}_{\mathrm{w}})$$

is also Θ. Suppose μ is a map from $W_{K'/E}$ to $W_{K/E}$ associated to the imbedding $K/E \longrightarrow K'/E$ and ν is a map from $W_{L'/F}$ to $W_{L/F}$ associated to the imbedding $L/F \longrightarrow L'/F$. We may suppose that $\psi_W \circ \mu = \nu \circ \psi'_W$. The kernel of μ is $W^c_{K'/K}$ if, for simplicity of notation, $W_{K'/K}$ is regarded as a subgroup of $W_{K'/E}$ and that of ν is $W^c_{L'/L}$. Moreover $\psi'_W(W^c_{K'/K}) = W^c_{L'/L}$. Take $\rho' = \rho \circ \mu$. Then σ acts on the space V of functions f on $W_{K/F}$ satisfying $f(vw) \equiv \rho(\psi_w^{-1}(h))f(w)$ for v in $\psi_w(W_{K/E})$. Let V' be the analogous space on which σ' acts. Then

$$V' = \{f \circ \nu \mid f \in V\}.$$

The assertion follows. Thus $\Omega(F)$ is a contravariant functor on $\mathcal{F}_{g\ell}$ and $\mathcal{F}_{\mathrm{loc}}$.

After this laborious and clumsy introduction we can set to work and prove the two theorems. The first step is to reformulate Theorem A.

Chapter Two.

The Main Theorem

It will be convenient in this paragraph and at various later times to regard $W_{K/E}$ as a subgroup of $W_{K/F}$ if $F \subseteq E \subseteq K$. If $F \subseteq E \subseteq L \subseteq K$ we shall also occasionally take $W_{L/E}$ to be $W_{K/E}/W^c_{K/L}$.

If K/F is finite and Galois, $\mathcal{P}(K/F)$ will be the set of extensions E'/E with $F \subseteq E \subseteq E' \subseteq K$ and $\mathcal{P}_\circ(K/F)$ will be the set of extensions in $\mathcal{P}(K/F)$ with the lower field equal to F.

Theorem 2.1

Suppose K is a Galois extension of the local field F and ψ_F is a given non-trivial additive character of F. There is exactly one function $\lambda(E/F, \psi_F)$ defined on $\mathcal{P}_\circ(K/F)$ with the following two properties

(i)
$$\lambda(F/F, \psi_F) = 1.$$

(ii) *If $E_1, \ldots, E_r,\ E'_1, \ldots, E'_s$ are fields lying between F and K, if $\chi_{E_i},\ 1 \le i \le r$, is a quasi-character of C_{E_i}, if $\chi_{E'_j},\ 1 \le j \le s$, is a quasi-character of $C_{E'_j}$, and if*

$$\oplus_{i=1}^r \ \mathrm{Ind}(\mathrm{W_{k/F}}, \mathrm{W_{K/E_i}},\ \chi_{\mathrm{E_i}})$$

is equivalent to

$$\oplus_{j=1}^s \ \mathrm{Ind}(\mathrm{W_{K/F}}, \mathrm{W_{K/E'_j}},\ \chi_{\mathrm{E'_j}})$$

then

$$\prod_{i=1}^r \ \Delta(\chi_{E_i}, \psi_{E_i/F})\lambda(E_i/F,\ \psi_F)$$

is equal to

$$\prod_{j=1}^s \ \Delta(\chi_{E'_j}, \psi_{E'_j/F})\lambda(E'_j/F,\ \psi_F).$$

A function satisfying the conditions of this theorem will be called a λ-function. It is clear that the function $\lambda(E/F,\, \psi_F)$ of Theorem A when restricted to $\mathcal{P}_\circ(K/F)$ becomes a λ-function. Thus the uniqueness in this theorem implies at least part of the uniqueness of Theorem A. To show how this theorem implies all of Theorem A we have to anticipate some simple results which will be proved in paragraph 4.

First of all a λ-function can never take on the value 0. Moreover, if $F \subseteq K \subseteq L$ the λ-function on $\mathcal{P}_\circ(K/F)$ is just the restriction to $\mathcal{P}_\circ(K/F)$ of the λ-function on $\mathcal{P}_\circ(L/F)$. Thus $\lambda(E/F,\, \psi_F)$ is defined independently of K. Finally if $E \subseteq E' \subseteq E''$

$$\lambda(E''/E,\ \psi_E) = \lambda(E''/E',\, \psi_{E'/E})\lambda(E'/E,\, \psi_E)^{[E'':E']}.$$

We also have to use a form of Brauer's theorem [4]. If G is a finite group there are nilpotent subgroups $N_1, \ldots, N_m$, one-dimensional representations $\chi_1, \ldots, \chi_m$ of $N_1, \ldots, N_m$ respectively, and integers $n_1, \ldots, n_m$ such that the trivial representation of G is equivalent to

$$\oplus_{i=1}^m \ n_i \mathrm{Ind}(\mathrm{G}, \mathrm{N_i}, \chi_{\mathrm{i}}).$$

The meaning of this when some of the n_i are negative is clear

Lemma 2.2

Suppose F is a global or local field and ρ is a representation of $W_{K/F}$. There are intermediate fields $E_1, \ldots, E_m$ such that $\mathfrak{G}(K/E_i)$ is nilpotent for $1 \le i \le m$, one-dimensional representations χ_{E_i} of W_{K/E_i}, and integers $n_1, \ldots, n_m$ such that ρ is equivalent to

$$\oplus_{i=1}^{m} n_i \mathrm{Ind}(\mathrm{W_{K/F}}, \mathrm{W_{K/E_i}}, \chi_{\mathrm{E_i}}).$$

Theorem 2.1 and Lemma 2.2 together imply the uniqueness of Theorem A. Before proving the lemma we must establish a simple and well-known fact.

Lemma 2.3

Suppose H is a subgroup of finite index in the group G. Suppose τ is a representation of G, σ a representation of H, and ρ the restriction of τ to H. Then

$$\tau \otimes \ \mathrm{Ind}(\mathrm{G}, \mathrm{H}, \sigma) \simeq \mathrm{Ind}(\mathrm{G}, \mathrm{H}, \rho \otimes \sigma).$$

Let τ act on V and σ on W. Then $\mathrm{Ind}(G, H, \sigma)$ acts on X, the space of all functions f on G with values in W satisfying

$$f(hg) = \sigma(h)\, f(g)$$

while $\mathrm{Ind}(G, H, \rho \otimes \sigma)$ acts on Y, the space of all functions f on G with values in $V \otimes W$ satisfying

$$f(hg) = (\rho(h) \otimes \sigma(h))\, f(g).$$

Clearly, $V \otimes X$ and Y have the same dimension. The map of $V \otimes X$ to Y which sends $v \otimes f$ to the function

$$f'(g) = \tau(g) v \otimes f(g)$$

is G-invariant. If it were not an isomorphism there would be a basis $v_1, \ldots, v_n$ of V and functions $f_1, \ldots, f_n$ which are not all zero such that

$$\Sigma_{i=1}^{n}\ \tau(g) v_i \otimes f_i(g) \equiv 0.$$

This is clearly impossible.

To prove Lemma 2.2 we take the group G of Brauer's theorem to be $\mathfrak{G}(K/F)$. Let F_i be the fixed field of N_i and let ρ_i be the tensor product of χ_i, which we may regard as a representation of W_{K/F_i} and the restriction of ρ to W_{K/F_i}. Then

$$\rho \simeq \rho \otimes 1 \simeq \oplus_{i=1}^{m} n_i \mathrm{Ind}(\mathrm{W_{K/F_i}}, \rho_{\mathrm{i}}).$$

This together with the transitivity of the induction process shows that in proving the lemma we may suppose that $\mathfrak{G}(K/F)$ is nilpotent.

We prove the lemma, with this extra condition, by induction on $[K : F]$. We use the symbol ω to denote an orbit in the set of quasi-characters of C_K under the action of $\mathfrak{G}(K/F)$. The restriction of ρ to C_K is the direct sum of one-dimensional representations. If ρ acts on V let V_ω be the space spanned by the vectors transforming under C_K according to a quasi-character in ω. V is the direct sum of the spaces V_ω which are each invariant under $W_{K/F}$. For our purposes we may suppose that $V = V_\omega$ for some ω. Choose χ_K in this ω and let V_0 be the space of vectors transforming under C_K according to χ_K. Let E be the fixed field of the isotrophy group of χ_K. V_0 is invariant under $W_{K/E}$. Let σ be the representation of $W_{K/E}$ in V_0. It is well-known that

$$\rho \simeq \mathrm{Ind}(\mathrm{W_{K/F}}, \mathrm{W_{K/E}}, \sigma).$$

To see this one has only to verify that the space X on which the representation on the right acts and V have the same dimension and that the map

$$f \longrightarrow \sum\nolimits_{W_{K/E}\backslash W_{K/F}} \ \rho(g^{-1})f(g)$$

of X into V which is clearly $W_{K/F}$-invariant has no kernel. It is easy enough to do this.

If $E \neq F$ the assertion of the lemma follows by induction. If $E = F$ choose L containing F so that K/L is cyclic of prime degree and L/F is Galois. Then $\rho(W_{K/L})$ is an abelian group and $W^c_{K/L}$ is contained in the kernel of ρ. Thus ρ may be regarded as a representation of $W_{L/F}$. The assertion now follows from the induction assumption and the concluding remarks of the previous paragraph.

Now take a local field E and a representation ρ of $W_{K/E}$. Choose intermediate fields $E_1, \ldots, E_m$, one-dimensional representations χ_{E_i} of W_{K/E_i}, and integers $n_1, \ldots, n_m$ so that

$$\rho \simeq \oplus_{i=1}^m n_i \ \mathrm{Ind}(\mathrm{W_{K/E}}, \mathrm{W_{K/E_i}}, \chi_{\mathrm{E_i}}).$$

If ω is the class of ρ set

$$\varepsilon(\omega, \psi_E) = \prod\nolimits_{i=1}^m \ \{\Delta(\chi_{E_i}, \Psi_{E_i/E})\lambda(E_i/E, \Psi_E)\}^{n_i}.$$

Theorem 2.1 shows that the right side is independent of the way in which ρ is written as a sum of induced representations. The first and second conditions of Theorem A are clearly satisfied. If ρ is the representation above and σ the representation

$$\mathrm{Ind}(\mathrm{W_{K/F}}, \mathrm{W_{K/E}}, \rho)$$

then

$$\sigma \simeq \oplus_{i=1}^m n_i \mathrm{Ind}(\mathrm{W_{K/F}}, \mathrm{W_{K/E_i}}, \chi_{\mathrm{E_i}}).$$

Thus if ω' is the class of σ

$$\varepsilon(\omega', \psi_F) = \prod\nolimits_{i=1}^m \{\Delta(\chi_{E_i}, \psi_{E_i/F})\lambda(E_i/F, \psi_F)\}^{n_i}$$

while

$$\varepsilon(\omega, \psi_{E/F}) = \prod\nolimits_{i=1}^m \ \{\Delta(\chi_{E_i}, \psi_{E_i/F}) \ \lambda(E_i/E, \psi_{E/F})\}^{n_i}.$$

The third property follows from the relations

$$\dim \omega = \Sigma_{i=1}^m \quad n_i \, [E_i : E]$$

and

$$\lambda(E_i/F, \psi_F) = \lambda(E_i/E, \, \psi_{E/F}) \ \lambda(E/F, \psi_F)^{[E_i:E]}$$

Chapter Three.

The Lemmas of Induction

In this paragraph we prove two simple but very useful lemmas.

Lemma 3.1

Suppose K is a Galois extension of the local field F. Suppose the subset $\mathfrak{A}$ of $\mathcal{P}(K/F)$ has the following four properties.

(i) *For all E, with $F \subseteq E \subseteq K,\ E/E \in \mathfrak{A}$.*

(ii) *If E''/E' and E'/E belong to $\mathfrak{A}$ so does E''/E.*

(iii) *If L/E belongs to $\mathcal{P}(K/F)$ and L/E is cyclic of prime degree then L/E belongs to $\mathfrak{A}$.*

(iv) *Suppose that L/E in $\mathcal{P}(K/F)$ is a Galois extension. Let $G = \mathfrak{G}(L/E)$. Suppose $G = H \cdot C$ where $H \neq \{1\},\ H \cap C = \{1\}$, and C is a non-trivial abelian normal subgroup of G which is contained in every non-trivial normal subgroup of G. If E' is the fixed field of H and if every E''/E in $\mathcal{P}_\circ(L/E)$ for which $[E'' : E] < [E' : E']$ is in $\mathfrak{A}$ so is E'/E. Then $\mathfrak{A}$ is all of $\mathcal{P}(K/F)$.*

It is convenient to prove another lemma first.

Lemma 3.2

Suppose K is a Galois extension of the local field F and $F \subsetneq E \subseteq K$. Suppose that the only normal subfield of K containing E is K itself and that there are no fields between F and E. Let $G = \mathfrak{G}(K/F)$ and let E be the fixed field of H. Let C be a minimal non-trivial abelian normal subgroup of G. Then $G = HC,\ H \cap C = \{1\}$ and C is contained in every non-trivial normal subgroup of G. In particular if $H = \{1\},\ G = C$ is abelian of prime order.

H is contained in no subgroup besides itself and G contains no normal subgroup but $\{1\}$. Thus if H is normal it is $\{1\}$ and G has no proper subgroups and is consequently cyclic of prime order. Suppose H is not normal. Since G is solvable it does contain a minimal non-trivial abelian normal subgroup C. Since C is not contained in H, $H \subsetneq HC$ and $G = HC$. Since $H \cap C$ is a normal subgroup of G it is $\{1\}$. If D is a non-trivial normal subgroup of G which does not contain C then $D \cap C = \{1\}$ and D is contained in the centralizer Z of C. Then DC is also and Z must meet H non-trivially. But $Z \cap H$ is a normal subgroup of G. This is a contradiction and the lemma is proved.

The first lemma is certainly true if $[K : F] = 1$. Suppose $[K : F] > 1$ and the lemma is valid for all pairs $[K' : F']$ with $[K' : F'] < [K : F]$. If the Galois extension L/E belongs to $\mathcal{P}(K/F)$ then $\mathfrak{A} \cap \mathcal{P}(L/E)$ satisfies the condition of the lemma with K replaced by L and F by E. Thus, by induction, if $[L : E] < [K : F],\ \mathcal{P}(L/E) \subseteq \mathfrak{A}$. In particular if E'/E is not in $\mathfrak{G}$ then $E = F$ and the only normal subfield of K containing E' is K itself. If $\mathfrak{A}$ is not $\mathcal{P}(K/F)$ then amongst all extensions which are not in $\mathfrak{G}$ choose one E/F for which $[E : F]$ is minimal. Because of (ii) there are no fields between F and E. Lemma 3.2, together with (iii) and (iv), show that E/F is in $\mathfrak{A}$. This is a contradiction.

There is a variant of Lemma 3.1 which we shall have occasion to use.

Lemma 3.3

Suppose K is a Galois extension of the local field F. Suppose the subset $\mathfrak{A}$ of $\mathcal{P}_\circ(K/F)$ has the following properties.

(i) *$F/F \in \mathfrak{A}$.*

(ii) *If L/F is normal and $L \underset{\neq}{\subset} K$ then $\mathcal{P}_\circ(L/F) \subseteq \mathfrak{A}$.*

(iii) *If $F \subset E \subseteq E' \subseteq K$ and E/F belong to $\mathfrak{G}$ then E'/F belong to $\mathfrak{A}$.*

(iv) *If L/F in $\mathcal{P}_\circ(K/F)$ is cyclic of prime degree then $L/F \in \mathfrak{A}$.*

(v) *Suppose that L/F in $\mathcal{P}_\circ(K/F)$ is Galois and $G = \mathfrak{G}(L/F)$. Suppose $G = HC$ where $H \neq \{1\}$, $H \cap C = \{1\}$, and C is a non-trivial abelian normal subgroup of G which is contained in every non-trivial normal subgroup. If E is the fixed field of H and if every E'/F in $\mathcal{P}_\circ(L/F)$ for which $[E' : F] < [E : F]$ is in $\mathfrak{A}$ so is E/F.*

Then $\mathfrak{A}$ is $\mathcal{P}_\circ(K/F)$.

Again if $\mathfrak{A}$ is not $\mathcal{P}_\circ(K/F)$ there is an E/F not in $\mathfrak{A}$ for which $[E : F]$ is minimal. Certainly $[E : F] > 1$. By (ii) and (iii), E is contained in no proper normal subfield of K and there are no fields between E and F. Lemma 3.2 together with (iv) and (v) lead to the contradiction that E/F is in $\mathfrak{A}$.

Chapter Four.

The Lemma of Uniqueness

Suppose K/F is a finite Galois extension of the local field F and ψ_F is a non-trivial additive character of F. A function $E/F \longrightarrow \lambda(E/F,\,\psi_F)$ on $\mathcal{P}_\circ(K/F)$ will be called a weak λ-function if the following two conditions are satisfied.

(i) $\lambda(F/F,\,\Psi_F) = 1$.

(ii) If $E_1,\ldots,E_r,\,E'_1,\ldots,E'_s$ are fields lying between F and K, if $\mu_i,\ 1 \le i \le r$, is a one-dimensional representation of $\mathfrak{G}(K/E_i)$, if $\nu_j,\ 1 \le j \le s$, is a one-dimensional representation of $\mathfrak{G}(K/E'_j)$, and if

$$\bigoplus_{i=1}^{r} \quad \mathrm{Ind}(\mathfrak{G}(\mathrm{K/F}), \mathfrak{G}(\mathrm{K/E_i}),\,\mu_\mathrm{i})$$

is equivalent to

$$\bigoplus_{j=1}^{s} \quad \mathrm{Ind}(\mathfrak{G}(\mathrm{K/F}), \mathfrak{G}(\mathrm{K/E_j}),\,\nu_\mathrm{j})$$

then

$$\prod_{i=1}^{r} \quad \Delta(\chi_{E_i},\psi_{E_i/F})\lambda(E_i/F,\,\psi_F)$$

is equal to

$$\prod_{j=1}^{s} \quad \Delta(\chi_{E'_j}\,\psi_{E'_j/F})\lambda(E'_j/F,\,\psi_F)$$

if χ_{E_i} is the character of C_{E_i} corresponding to μ_i and $\chi_{E'_j}$ is the character of $C_{E'_j}$ corresponding to ν_j.

Supposing that a weak λ-function is given on $\mathcal{P}_\circ(K/F)$, we shall establish some of its properties.

Lemma 4.1

(i) *If L/F in $\mathcal{P}_\circ(K/F)$ is normal the restriction of $\lambda(\cdot,\psi_F)$ to $\mathcal{P}_\circ(L/F)$ is a weak λ-function.*

(ii) *If E/F belongs to $\mathcal{P}_\circ(K/F)$ and $\lambda(E/F,\,\psi_F) \ne 0$ the function on $\mathcal{P}_\circ(K/E)$ defined by*

$$\lambda(E'/E,\,\psi_{E/F}) = \lambda(E'/F,\,\psi_F)\ \lambda(E/F,\,\psi_F)^{-[E':E]}$$

is a weak λ-function.

Any one-dimensional representation μ of $\mathfrak{G}(L/E)$ may be inflated to a one-dimensional representation, again called μ, of $\mathfrak{G}(K/E)$ and

$$\mathrm{Ind}(\mathfrak{G}(\mathrm{K/F}), \mathfrak{G}(\mathrm{K/E}),\ \mu)$$

is just the inflation to $\mathfrak{G}(K/F)$ of

$$\mathrm{Ind}(\mathfrak{G}(\mathrm{L/F}), \mathfrak{G}(\mathrm{L/E}),\ \mu).$$

The first part of the lemma follows immediately from this observation.

As for the second part, the relation

$$\lambda(E/E,\,\psi_{E/F}) = 1$$

is clear. If fields $E_i,\ 1 \le i \le r,\quad E'_j,\ 1 \le j \le s$, lying between E and K and representations μ_i and ν_j are given as prescribed and if

$$\bigoplus_{i=1}^{r} \mathrm{Ind}(\mathfrak{G}(\mathrm{K/E}), \mathfrak{G}(\mathrm{K/E_i}),\ \mu_\mathrm{i}) = \rho$$

is equivalent to

$$\bigoplus_{j=1}^{s} \mathrm{Ind}(\mathfrak{G}(\mathrm{K/E}), \mathfrak{G}(\mathrm{K/E'_j}),\ \nu_\mathrm{j}) = \sigma$$

then

$$\bigoplus_{i=1}^{r} \mathrm{Ind}(\mathfrak{G}(\mathrm{K/F}), \mathfrak{G}(\mathrm{K/E_i},\ \mu_\mathrm{i})$$

is equivalent to

$$\bigoplus_{j=1}^{s} \mathrm{Ind}(\mathfrak{G}(\mathrm{K/F}), \mathfrak{G}(\mathrm{K/E'_j}),\ \nu_\mathrm{j})$$

so that

$$\prod_{i=1}^{r} \Delta(\chi_{E_i}, \psi_{E_i/F})\ \lambda(E_1/F,\ \psi_F) \tag{A}$$

is equal to

$$\prod_{j=1}^{s} \Delta(\chi_{E'_j},\ \psi_{E'_j/F})\ \lambda(E'_j/F,\ \psi_F). \tag{B}$$

Since ρ and σ have the same dimension

$$\Sigma_{i=1}^{r}\,[E_i : E] = \Sigma_{j=1}^{s}\,[E'_j : E]$$

so that

$$\prod_{i=1}^{r} \lambda(E/F,\ \Psi_F)^{[E_i:E]} = \prod_{j=1}^{s} \lambda(E/F,\ \psi_F)^{[E'_j:F]}.$$

Dividing (A) by the left side of this equation and (B) by the right and observing that the results are equal we obtain the relation needed to prove the lemma.

If K/F is abelian $S(K/F)$ will be the set of characters of C_F which are 1 on $N_{K/F}C_K$.

Lemma 4.2

If K/F is abelian

$$\lambda(K/F,\ \Psi_F) = \prod_{\mu_F \in S(K/F)} \Delta(\mu_F, \psi_F).$$

μ_F determines a one-dimensional representation of $\mathfrak{G}(K/F)$ which we also denote by μ_F. The lemma is an immediate consequence of the equivalence of

$$\mathrm{Ind}(\mathfrak{G}(\mathrm{K/F}), \mathfrak{G}(\mathrm{K/K}), 1)$$

and

$$\bigoplus_{\mu_F \in S(K/F)} \mathrm{Ind}(\mathfrak{G}(\mathrm{K/F}), \mathfrak{G}(\mathrm{K/F}), \mu_\mathrm{F}).$$

Lemma 4.3

Suppose K/F is normal and $G = \mathfrak{G}(K/F)$. Suppose $G = HC$ where $H \cap C = \{1\}$ and C is a non-trivial abelian normal subgroup. Let E be the fixed field of H and L that of C. Let T be a set of *representatives of the orbits of $S(K/L)$ under the action of G. If $\mu \in T$ let B_μ be the isotropy group of μ and let $B_\mu = \mathfrak{G}(K/L_\mu)$. Then $[L_\mu : F] < [E : F]$ and*

$$\lambda(E/F,\, \psi_F) = \prod\nolimits_{\mu \in T}\ \Delta(\mu', \psi_{L_\mu/F})\ \lambda(L_\mu/F,\, \psi_F).$$

Here $\mathfrak{G}(K/L_\mu) = \mathfrak{G}(K/L) \cdot (\mathfrak{G}(K/L_\mu) \cap \mathfrak{G}(K/E))$ and μ' is the character of C_{L_μ} associated to the character of $\mathfrak{G}(K/L_\mu) : g \longrightarrow \mu(g_1)$ if

$$g = g_1 g_2, \quad g_1 \in \mathfrak{G}(K/L), \quad g_2 \in \mathfrak{G}(K/L_\mu) \cap \mathfrak{G}(K/E),$$

We may as well denote the given character of $\mathfrak{G}(K/L_\mu)$ by μ' also. To prove the lemma we show that

$$\mathrm{Ind}(\mathfrak{G}(\mathrm{K/F}), \mathfrak{G}(\mathrm{K/E}),\, 1) = \sigma$$

is equivalent to

$$\bigoplus\nolimits_{\mu \in T}\ \mathrm{Ind}(\mathfrak{G}(\mathrm{K/F}), \mathfrak{G}(\mathrm{K/L}_\mu),\, \mu').$$

Since T has at least two elements it will follow that

$$[E : F] = \dim \mathrm{Ind}(\mathfrak{G}(\mathrm{K/F}), \mathfrak{G}(\mathrm{K/E}),\, 1)$$

is greater than

$$[L_\mu : F] = \dim \mathrm{Ind}(\mathfrak{G}(\mathrm{K/F}), \mathfrak{G}(\mathrm{K/L}_\mu),\, \mu').$$

The representation σ acts on the space of functions on $H\backslash G$. If $\nu \in S(K/L)$, that is, is a character of C, let $\psi_\nu(hc) = \nu(c)$ if $h \in H, \quad c \in C$. The set

$$\{\psi_\nu \mid \nu \in S(K/L)\}$$

is a basis for the functions on $H\backslash G$. If $\mu \in T$ let S_μ be its orbit; then

$$V_\mu = \Sigma_{\nu \in S_\mu} \mathbb{C}\psi_\nu$$

is invariant and irreducible under G. Moreover, if g belongs to $\mathfrak{G}(K/L_\mu)$

$$\sigma(g)\psi_\mu = \mu'(g)\psi_\mu.$$

Since

$$\dim\ V_\mu = [\mathfrak{G}(K/F), \mathfrak{G}(K/L_\mu)]$$

the Frobenius reciprocity theorem implies that the restriction of σ to V_μ is equivalent to

$$\mathrm{Ind}(\mathfrak{G}(\mathrm{K/F}), \mathfrak{G}(\mathrm{K/L}_\mu),\, \mu').$$

Lemma 4.2 is of course a special case of Lemma 4.3.

Lemma 4.4

$\lambda(E/F, \Psi_F)$ is different from 0 for all E/F in $\mathcal{P}_\circ(K/F)$.

The lemma is clear if $[K : F] = 1$. We prove it by induction on $[K : F]$. Let $\mathfrak{S}$ be the set of E/F in $\mathcal{P}_\circ(K/F)$ for which $\lambda(E/F,\, \psi_F) \neq 0$. We may apply Lemma 3.3. The first condition of that lemma is clearly satisfied. The second follows from the induction assumption and the first part of Lemma 4.1; the third from the induction assumption and the second part of Lemma 4.1. The fourth and fifth follow from Lemmas 4.2 and 4.3 respectively. We of course use the fact that $\Delta(\chi_E, \Psi_E)$, which is basically a Gaussian sum when E is non-archimedean, is never zero.

For every E'/E in $\mathcal{P}(K/F)$ we can define $\lambda(E'/E, \psi_{E/F})$ to be

$$\lambda(E'/F,\, \psi_F)\ \lambda(E/F,\, \psi_F)^{-[E':E]}.$$

Lemma 4.5

If E''/E' and E'/E belong to $\mathcal{P}(K/F)$ then

$$\lambda(E''/E, \psi_{E/F}) = \lambda(E''/E', \psi_{E'/F})\lambda(E'/E,\, \psi_{E/F})^{E'':E']}.$$

Indeed

$$\lambda(E''/E, \psi_{E/F}) = \lambda(E''/F, \psi_F)\ \lambda(E/F, \psi_F)^{-[E'':E]}$$

which equals

$$\left\{\lambda(E''/F, \psi_F)\, \lambda(E'/F, \psi_F)^{-[E'':E']}\right\}\ \left\{\lambda(E'/F, \psi_F)^{[E'':E']}\ \lambda(E/F, \psi_F)^{-[E'':E]}\right\}$$

and this in turn equals

$$\lambda(E''/E', \psi_{E'/F})\ \lambda(E'/E, \psi_{E/F})^{[E'':E']}.$$

Lemma 4.6

If $\lambda_1(\cdot, \Psi_F)$ and $\lambda_2(\cdot, \Psi_F)$ are two weak λ-functions on $\mathcal{P}_\circ(K/F)$ then

$$\lambda_1(E'/E, \psi_{E/F}) = \lambda_2(E'/E, \psi_{E/F})$$

for all E'/E in $\mathcal{P}(K/F)$.

We apply Lemma 3.1 to the collection $\mathfrak{S}$ of all pairs E'/E in $\mathcal{P}(K/F)$ for which the equality is valid. The first condition of that lemma is clearly satisfied. The second is a consequence of the previous lemma. The third and fourth are consequences of Lemmas 4.2 and 4.3 respectively.

Since a λ-function is also a weak λ-function the uniqueness of Theorem 2.1 is now proved.

Chapter Five.

A Property of λ-Functions

It follows immediately from the definition that if $\psi'_E(x) = \psi_E(\beta x)$ then

$$\Delta(\chi_E, \psi'_E) = \chi_E(\beta)\Delta(\chi_E, \psi_E).$$

Associated to any equivalence class ω of representations of the Weil group of the field F is a one-dimensional representation or, what is the same, a quasi-character of C_F. It is denoted $\det\omega$ and is obtained by taking the determinant of any representation in ω. Suppose ρ is in the class ω and ρ is a representation of $W_{K/F}$. To find the value of the quasi-character $\det\omega$ at β choose w in $W_{K/F}$ so that $\tau_{K/F}w = \beta$. Then calculate $\det(\rho(w))$ which equals $\det\omega(\beta)$.

If $F \subseteq E \subseteq K$ the map $\tau = \tau_{K/F}$ can be effected in two stages. We first transfer $W_{K/F}/W^c_{K/F}$ into $W_{K/E}/W^c_{K/E}$; then we transfer $W_{K/E}/W^c_{K/E}$ into C_K. If $W_{K/F}$ is the disjoint union

$$\bigcup_{i=1}^r W_{K/E}w_i$$

and if $w_i w = u_i(w)w_j(i)$ then the transfer of w in $W_{K/E}/W^c_{K/E}$ is the coset to which $w' = \prod_{i=1}^r u_i(w)$ belongs.

Suppose σ is a representation of $W_{K/E}$ and

$$\rho = \mathrm{Ind}(\mathrm{W_{K/F}}, \mathrm{W_{K/E}}, \sigma).$$

ρ acts on a certain space V of functions on $W_{K/F}$ and if V_i is the collection of functions in V which vanish outside of $W_{K/E}w_i$ then

$$V = \bigoplus_{i=1}^r V_i.$$

We decompose the matrix of $\rho(w)$ into corresponding blocks $\rho_{ji}(w)$. $\rho_{ji}(w)$ is 0 unless $j = j(i)$ when $\rho_{ji}(w) = \sigma(u_i, (w))$. This makes it clear that if $\iota_{E/F}$ is the representation of $W_{K/F}$ induced from the trivial representation of $W_{K/E}$

$$\det(\rho(w)) = \det(\iota_{E/F}(w))^{\dim\sigma}\det(\sigma(w'))$$

or, if θ is the class of σ,

$$\det\omega(\beta) = \{\det\ \iota_{E/F}(\beta)\}^{\dim\theta}\{\det\theta(\beta)\}.$$

Lemma 5.1

Suppose F is a local field and $E/F \longrightarrow \lambda(E/F, \psi_F)$ and $\omega \longrightarrow \varepsilon(\omega, \psi_{E/F})$ satisfy the conditions of Theorem A for the character ψ_F. Let $\psi'_F(x) = \psi_F(\beta x)$ with β in C_F. If $E/F \longrightarrow \lambda(E/F, \psi'_F)$ and $\omega \longrightarrow \varepsilon(\omega, \psi'_{E/F})$ satisfy the conditions of Theorem A for ψ'_F then

$$\lambda(E/F, \psi'_F) = \det\iota_{E/F}(\beta)\ \lambda(E/F, \psi_F)$$

and

$$\varepsilon(\omega, \psi'_{E/F}) = \det\omega(\beta)\ \varepsilon(\omega, \psi_{E/F}).$$

Because of the uniqueness all one has to do is verify that the expressions on the right satisfy the conditions of the theorem for the character ψ'_F. This can now be done immediately.

Chapter Six.

A Filtration of the Weil Group

In this paragraph I want to reformulate various facts found in Serre's book [12] as assertions about a filtration of the Weil group. Although some of the lemmas to follow will be used to prove the four main lemmas, the introduction of the filtration itself is not really necessary. It serves merely to unite in a form which is easily remembered the separate lemmas of which we will actually be in need.

Let K be a finite Galois extension of the non-archimedean local field F and let $G = \mathfrak{G}(K/F)$. Let O_F be the ring of integers in F and let $\mathfrak{p}_F$ be the maximal ideal of O_F. If $i \geq -1$ is an integer let G_i be the subgroup of G consisting of those elements which act trivially on $O_F/\mathfrak{p}_F^{i+1}$. If $u \geq -1$ is a real number and i is the smallest integer greater than or equal to u set $G_u = G_i$. Finally if $u \geq -1$ set

$$\varphi_{K/F}(u) = \int_0^u \frac{1}{[G_0 : G_t]}\, dt.$$

The integrand is not defined at -1 but that is of no consequence. $\varphi_{K/F}$ is clearly a piecewise linear, continuous, and increasing map of $[-1, \infty)$ onto itself. The inverse function* $\psi_{K/F}$ will have the same properties.

We take from Serre's book the following lemma.

Lemma 6.1

If $F \subseteq L \subseteq K$ and L/F is normal then $\varphi_{K/F} = \varphi_{L/F} \circ \varphi_{K/L}$ and $\psi_{K/F} = \psi_{K/L} \circ \psi_{L/F}$.

The circle denotes composition not multiplication. This lemma allows us to define $\varphi_{E/F}$ and $\psi_{E/F}$ for any finite separable extension E/F by choosing a Galois extension L of F which contains E and setting

$$\varphi_{E/F} = \varphi_{L/F} \circ \psi_{L/E}$$
$$\psi_{E/F} = \varphi_{L/E} \circ \psi_{L/F}$$

because if L' is another such extension we can choose a Galois extension K containing both L and L' and

$$\varphi_{L/F} \circ \psi_{L/E} = \varphi_{L/F} \circ \varphi_{K/L} \circ \psi_{K/L} \circ \psi_{L/E} = \varphi_{K/F} \circ \psi_{K/E} = \varphi_{L'/F} \circ \psi_{L'/E}$$
$$\varphi_{L/E} \circ \psi_{L/F} = \varphi_{L/E} \circ \varphi_{K/L} \circ \psi_{K/L} \circ \psi_{L/F} = \varphi_{K/E} \circ \psi_{K/F} = \varphi_{L'/E} \circ \psi_{L'/F}.$$

Of course $\psi_{E/F}$ is the inverse of $\varphi_{E/F}$.

Lemma 6.2

If $E \subseteq E' \subseteq E''$ and E''/E is finite and separable, $\varphi_{E''/E} = \varphi_{E'/E} \circ \varphi_{E''/E'}$ and $\psi_{E''/E} = \psi_{E''/E'} \circ \psi_{E'/E}$.

---

* In this chapter $\psi_{K/F}$ does not appear as an additive character. Nonetheless, there is a regrettable conflict of notation.

Each of these relations can be obtained from the other by taking inverses; we verify the second

$$\psi_{E''/E'} \circ \psi_{E'/E} = \varphi_{L/E''} \circ \psi_{L/E'} \circ \varphi_{L/E'} \circ \psi_{L/E} = \varphi_{L/E''} \circ \psi_{L/E} = \psi_{E''/E}.$$

It will be necessary for us to know the values of these functions in a few special cases.

Lemma 6.3

(i) *If K/F is Galois and unramified $\psi_{K|F}(u) \equiv u$.*

(ii) *If K/F is cyclic of prime degree ℓ and if $G = G_t$ while $G_{t+1} = \{1\}$ where t is a non-negative integer then*

$$\begin{aligned} \psi_{K/F}(u) &= u & u \le t \\ &= t + \ell(u-t) & u \ge t. \end{aligned}$$

These assertions follow immediately from the definitions.

Lemma 6.4

Suppose K/F is Galois and $G = \mathfrak{G}(K/F)$ is a product HC where $H \neq \{1\},\ H \cap C = \{1\}$, and C is a non-trivial abelian normal subgroup of G which is contained in every non-trivial normal subgroup.

(i) *If K/F is tamely ramified so that $G_1 = \{1\}$ then $G_0 = C$ is a cyclic group of prime order ℓ and $[G:G_0] = [H:1]$ divides $\ell - 1$. If E is the fixed field of H, $\psi_{E/F}(u) = u$ for $u \le 0$ and $\psi_{E/F}(u) = \ell u$ for $u \ge 0$.*

(ii) *If K/F is wildly ramified there is an integer $t \ge 1$ such that $C = G_1 = \ldots = G_t$ while $G_{t+1} = \{1\}$. $[G_0 : G_1]$ divides $[G_1 : 1] - 1$ and every element of C has order p or 1. If E is the fixed field of H and L that of C*

$$\begin{aligned} \psi_{L/F}(u) &= u & u \le 0 \\ &= [G_0 : G_1]u & u \ge 0 \end{aligned}$$

while

$$\begin{aligned} \psi_{E/F}(u) &= u & u \le \frac{t}{[G_0:G_1]} \\ &= \frac{t}{[G_0:G_1]} + [G_1:1]\left(u - \frac{t}{[G_0:G_1]}\right) & u \ge \frac{t}{[G_0:G_1]} \end{aligned}$$

We observed in the third paragraph that C must be its own centralizer. G_0 cannot be $\{1\}$. Thus $C \subseteq G_0$. In case (i) G_0 is abelian and thus $G_0 = C$. In both cases if ℓ is a prime dividing the order of C the set of elements in C of order ℓ or 1 is a non-trivial normal subgroup of G and thus C itself. In case (i) C is cyclic and thus of prime order ℓ. Moreover, H which is isomorphic to G/G_0 is abelian and, if $h \in H,\ \{c \in C | hc = ch\}$ is a normal subgroup of G and hence $\{1\}$ or C. If $h \neq 1$ it must be 1. Consequently each orbit of H in $C - \{1\}$ has $[H:1]$ elements and $[H:1]$ divides $\ell - 1$.

In case (ii) G_1 is a non-trivial normal subgroup and hence contains C. G_1 and C are both p-groups. The centralizer of G_1 in C is not trivial. As a normal subgroup of G it contains C. Therefore it is C and G_1 is contained in C which is its own centralizer. Since each $G_i,\ i \ge 1$, is a normal subgroup of G, it is either C or $\{1\}$. Thus there is an integer $t \ge 1$ such that $G_1 = G_t = C$ while $G_{t+1} = \{1\}$. If $i \ge 0$ is an integer let U_K^i be the group of units of O_K which are congruent to 1 modulo p_K^{i+1}; let $U_K^{(-1)} = C_K$, and if $U \geq -1$ is any real number let i be the smallest integer greater than or equal to u and set $U_K^u = U_K^i$. If θ_t is the map of G_t/G_{t+1} into p_K^t/p_K^{t+1} and θ_0 the map of G_0/G_1 into U_K^0/U_K^1 introduced in Serre then, for g in G_0 and h in C,

$$\theta_t(ghg^{-1}) = \theta_0(g)^t \Theta_t(h).$$

If $h \neq 1$, $ghg^{-1} = h$ if and only if $\theta_0(g)^t = 1$ and then g belongs to the centralizer of C, that is to G_1. Again $C - \{1\}$ is broken up into orbits, each with $[G_0 : G_1]$ elements and $[G_0 : G_1]$ divides $[G_i : 1] - 1$. Observe that t must be prime to $[G_0 : G_1]$.

It follows immediately from the definitions that $H_u = H \cap G_u$. In case (i) H_0 will be $\{1\}$ and $\varphi_{K/E}(u)$ will be identically u. Thus $\psi_{E/F} = \psi_{K/F}$ and, from the definition, $\psi_{K/F}(u) = u$ if $u \leq 0$ while $\psi_{K/F}(u) = [G_0 : 1]u$ if $u \geq 0$. In case (ii), $\varphi_{K/E}(u) = u$ if $u \leq 0$ and

$$\varphi_{K/E}(u) = \frac{u}{[H_0 : 1]} = \frac{u}{[G_0 : G_1]}$$

if $u \geq 0$ while $\psi_{K/F}(u) = u$ if $u \leq 0$ and

$$\begin{aligned} \psi_{K/F}(u) &= [G_0 : G_1]u & 0 \leq u \leq \frac{t}{[G_0 : G_1]} \\ &= t + [G_0 : 1]\left(u - \frac{t}{[G_0 : G_1]}\right) & \frac{t}{[G_0 : G_1]} \leq u. \end{aligned}$$

The lemma follows.

Lemma 6.5

For every separable extension E'/E the function $\psi_{E'/E}$ is convex, and if u is an integer so is $\psi_{E'/E}(u)$.

All we have to do is prove that the assertion is true for all E'/E in $\mathcal{P}(K/F)$ if F is an arbitrary non-archimedean local field and K an arbitrary Galois extension of it. To do this we just combine the previous three lemmas with Lemma 3.1. We are going to use the same method to prove the following lemma.

Lemma 6.6

For every separable extension E'/E and any $u \geq -1$

$$N_{E'/E}\,(U_{E'}^{\psi_{E'/E}(u)}) \subseteq U_E^u.$$

We have to verify that the set $\mathfrak{G}$ of all E'/E in $\mathcal{P}(K/F)$ for which the assertion is true satisfies the conditions of Lemma 3.1. There is no problem with the first two.

Lemma 6.7

E'/E belongs to $\mathfrak{G}$ if and only if for every integer $n \geq -1$

$$N_{E'/E}\left(U_{E'}^{\psi_{E'/E}(n)}\right) \subseteq U_E^n$$

and

$$N_{E'/E}\left(U_{E'}^{\psi_{E'/E}(n)+1}\right)\subseteq U_E^{n+1}.$$

If E'/E belongs to $\mathfrak{G}$ choose $\varepsilon>0$ so that $\psi_{E'/E}(n+\varepsilon)=\psi_{E'/E}(n)+1$. The smallest integer greater than or equal to $n+\varepsilon$ is at least $n+1$ so

$$N_{E'/E}\left(U_{E'}^{\psi_{E'/E}(n)+1}\right)\subseteq U_E^{n+\varepsilon}\subseteq U_E^{n+1}.$$

Conversely suppose the conditions of the lemma are satisfied and $n<u<n+1$. Since $\psi_{E'/E}(n)$ is an integer the smallest integer greater than or equal to $\psi_{E'/E}(u)$ is at least $\psi_{E'/E}(n)+1$. Thus

$$N_{E'/E}\left(U_{E'}^{\psi_{E'/E}(u)}\right)\subseteq N_{E'/E}\left(U_{E'}^{\psi_{E'/E}(n)+1}\right)\subseteq U_E^{n+1}=U_E^u.$$

Lemma 6.8

If L/E is Galois then, for every integer $n\geq-1$,

$$N_{L/E}\left(U_L^{\psi_{L/E}(n)}\right)\subseteq U_E^n$$

and

$$N_{L/E}\left(U_L^{\psi_{L/E}(n)+1}\right)\subseteq U_E^{n+1}.$$

The assertion is clear if $n=-1$. A proof for the case $n\geq0$ and L/E totally ramified is given in Serre's book. Since that proof works equally well for all L/E we take the lemma as proved.

Lemma 6.9

Suppose K/F is Galois and $G=\mathfrak{G}(K/F)$. Suppose $G=HC$ where $H\neq\{1\}$, $H\cap C=\{1\}$, and C is a non-trivial abelian normal subgroup of G which is contained in every non-trivial normal subgroup of G. If E is the fixed field of H

$$N_{E/F}\left(U_E^{\psi_{E/F}(u)}\right)\subseteq U_F^u$$

for all $u\geq-1$.

Let L be the fixed field of C. If K/F is tamely ramified K/E and L/F are unramified so that $\psi_{E/F}=\psi_{K/L}$ and $U_E^v=C_E\cap U_K^v$, $U_F^v=C_F\cap U_L^v$ for every $v\geq-1$. If α belongs to C_E, then delete $N_{K/L}\alpha=N_{E/F}\alpha$. Since K/L is Galois

$$N_{E/F}\left(U_E^{\psi_{E/F}(u)}\right)\subseteq C_F\cap N_{K/L}\left(U_L^{\psi_{K/L}(u)}\right)\subseteq C_F\cap U_L^u=U_F^u.$$

If K/F is not tamely ramified

$$\mathfrak{p}_E^n=E\cap p_k^{[G_0:G_1]n-m}$$

if $n\geq1$ and $0\leq m<[G_0:G_1]$. Thus

$$U_E^v=G_E\cap U_K^v$$

if $-1\leq v\leq0$ and

$$U_E^v=C_E\cap U_K^{[G_0:G_1]v}$$

if $v \geq 0$ or, more briefly,

$$U_E^v = C_E \cap U_K^{\psi_{K/E}(v)}$$

for all $v \geq -1$. In the same way we find

$$U_F^v = C_F \cap U_L^{\psi_{L/F}(v)}$$

for all $v \geq -1$. Since K/L is normal

$$N_{E/F}\left(U_E^{\psi_{E/F}(u)}\right) \subseteq C_F \cap N_{K/L}\left(U_K^{\psi_{K/F}(u)}\right) \subseteq C_F \cap U_L^{\psi_{L/F}(u)} = U_F^u.$$

Lemma 6.6 now follows immediately.

Lemma 6.10

(a) *Suppose K/F is Galois and $G = \mathfrak{G}(K/F)$. Suppose $t \geq -1$ is an integer such that $G = G_t \neq G_{t+1}$. Then $\psi_{K/F}(u) = u$ for $u \leq t$. Moreover $N_{K/F}$ defines an isomorphism of C_K/U_K^t with C_F/U_F^t and if $-1 \leq u \leq t$ the inverse image of U_F^u/U_F^t is U_K^u/U_K^t. However the map of C_K/U_K^{t+1} into C_F/U_F^{t+1} defined by the norm is not surjective.*

(b) *Suppose K/F is Galois and $G = \mathfrak{G}(K/F)$. Suppose $s \geq -1$ is an integer and $G = G_s$. If $F \subseteq E \subseteq K$, $\psi_{E/F}(u) = u$ for $u \leq s$ and $N_{E/F}$ defines an isomorphism of C_E/U_E^s and C_F/U_F^s. If $-1 \leq u \leq s$ the inverse image of U_F^u/U_F^s is U_E^u/U_E^s.*

If $t = -1$ the assertions of part (a) are clear. If $t \geq 0, K/F$ is totally ramified. The relation $\psi_{K/F}(u) = u$ for $u \leq t$ is an immediate consequence of the definition. Since the extension is totally ramified $N_{K/F}$ defines an isomorphism of U_K^{-1}/U_K^0 and U_F^{-1}/U_F^0. It follows from Proposition V.9 of Serre's book that if $0 \leq n < t$ the associated map $U_K^n/U_K^{n+1} \longrightarrow U_F^n/U_F^{n+1}$ is an isomorphism but that the map $U_K^t/U_K^{t+1} \longrightarrow U_F^t/U_F^{t+1}$ has a non-trivial cokernel. The first part of the lemma is an immediate consequence of these facts.

To prove part (b) we first observe that there is a $t \geq s$ such that $G = G_t \neq G_{t+1}$. It then follows from part (a) that the map $N_{K/F}$ determines an isomorphism of C_K/U_K^s and C_F/U_F^s under which U_K^u/U_K^s and U_F^u/U_F^s correspond if $-1 \leq u \leq s$. Let E be the fixed field of H. We have $H_s = H \cap G_s = H$, so that $N_{K/E}$ determines on isomorphism of C_K/U_K^s and C_E/U_E^s under which U_K^u/U_K^s and U_E^u/U_E^s correspond if $-1 \leq u \leq s$. Moreover if $u \leq s$, $\psi_{K/F}(u) = \psi_{K/E}(u) = u$ so that $\psi_{E/F}(u) = u$. Part (b) follows from these observations and the relation $N_{K/F} = N_{E/F}N_{K/E}$.

If E is any non-archimedean local field and $u > -1$

$$U_E^u = \cap_{v<u} U_E^v.$$

If α belongs to C_E set

$$v_E(\alpha) = \sup\{u | \alpha \in U_E^u\}.$$

Then $v_E(1) = \infty$, but $v_E(\alpha)$ is finite if $\alpha \neq 1$ and α belongs to $U_E^{v_E(\alpha)}$.

If $F \subseteq L \subseteq K$, $\tau_{K/F,L/F}$ will be any of the maps $W_{K/F} \longrightarrow W_{L/F}$ associated to the imbedding $L/F \longrightarrow K/F$. We abbreviate $\tau_{K/F,F/F}$ to $\tau_{K/F}$. If w belongs to $W_{K/F}$, $\sigma(w)$ is the image of w in $\mathfrak{G}(K/F)$, and E is the fixed field of $\sigma(w)$, we set

$$v_{K/F}(w) = \varphi_{E/F}(v_E(\tau_{K/E}(w))).$$

Note that we regard $W_{K/E}$ as a subgroup of $W_{K/F}$. If $v \geq -1$ let

$$W^v_{K/F} = \{w \,|\, v_{K/F}(w) \geq v\}.$$

We shall show that $W^v_{K/F}$ is a normal subgroup of $W_{K/F}$. These groups provide a filtration of the Weil group, some of whose properties are established in the following lemmas.

Lemma 6.11

If $\sigma \in \mathfrak{G}(K/F)$ and $t = \sup\{u \,|\, \sigma \in G_u\}$, set $v_{K/F}(\sigma) = \varphi_{K/F}(t)$. Then

$$v_{K/F}(\sigma) = \max\{v_{K/F}(w) \,|\, \sigma(w) = \sigma\}.$$

If $\sigma = 1$ both sides are infinite and the assertion is clear. If $\sigma \neq 1$ let E be the fixed field of σ. If $\sigma(w) = \sigma,$ w belongs to $W_{K/E}$ and $v_{K/F}(w) = \varphi_{E/F}(v_{K/E}(w))$. Also $v_{K/F}(\sigma) = \varphi_{E/F}(v_{K/E}(\sigma))$. Consequently it is sufficient to prove the lemma when $F = E$. The set

$$S = \{\tau_{K/F}(w) \,|\, \sigma(w) = \sigma\}$$

is a coset of $N_{K/F}(C_K)$ in C_F and C_F is generated by $N_{K/F}(C_K)$ together with any element of S. Moreover $s = \max\{v_F(\beta) \,|\, \beta \in S\}$ is the largest integer such that $S \cap U^s_F$ is not empty. Since $G = G_t \neq G_{t+1}$ the preceding lemma shows that $s = t = \varphi_{K/F}(t)$.

Lemma 6.12

(a) *For all w and w_1 in $W_{K/F}, v_{K/F}(w) = v_{K/F}(w^{-1})$ and $v_{K/F}(w_1 w\, w_1^{-1}) = v_{K/F}(w)$.*

(b) *If $F \subseteq E \subseteq K$ and w belong to $W_{K/E}$ then*

$$v_{K/F}(w) = \varphi_{E/F}(v_{K/E}(w)).$$

(c) *For all w in $W_{K/F}$, $\tau_{K/F}(w) \subset U_F^{v_{K/F}(w)}$.*

The first two assertions follow immediately from the definitions and the basic properties of the Weil group. I prove only the third. Let me first observe that if $F \subseteq E \subseteq K$ and $w \subset W_{K/E}$, then

$$\tau_{K/F}(w) = N_{E/F}(\tau_{K/E}(w)).$$

To see this, choose a set of representatives $w_1, \dots, w_r$ for the cosets of C_K in $W_{K/E}$ and then a set of representatives $v_1, \dots, v_s$ for the cosets of $W_{K/E}$ in $W_{K/F}$. Let $w_i w = a_i w_{j(i)}$ with a_i in C_K; then

$$\tau_{K/E}(w) = \prod\nolimits_{i=1}^r a_i.$$

However $v_j w_i w = v_j a_i v_j^{-1} v_j w_{j(i)}$ so that

$$\tau_{K/F}(w) = \prod\nolimits_{j=1}^s \prod\nolimits_{i=1}^r \, v_j a_i v_j^{-1} = \prod\nolimits_{j=1}^s \, v_j \tau_{K/E}(w) v_j^{-1} = N_{E/F}(\tau_{K/E}(w)).$$

In particular, if E is the fixed field of $\sigma(w)$, $\tau_{K/E}(w)$ is contained $U_E^{\psi_{E/F}(v_{K/F}(w))}$ and $\tau_{K/F}(w)$ is contained in

$$N_{E/F}\,(U_E^{\psi_{E/F}(v_{K/F}(w))}) \subseteq U_F^{v_{K/F}(w)}.$$

Lemma 6.13

If u and v belong to $W_{K/F}$ then

$$v_{K/F}(uv) \geq \min\{v_{K/F}(u), v_{K/F}(v)\}.$$

Let $\sigma = \sigma(u)$ and let $\tau = \sigma(v)$. Because of the second assertion of the previous lemma we may assume that σ and τ generate $\mathfrak{G}(K/F)$. Let E be the fixed field of $\sigma\tau$. If

$$t = \{\min\left(\psi_{K/F}(v_{K/F}(\sigma)), \psi_{K/F}(v_{K/F}(\tau)\right)\}$$

and $G = \mathfrak{G}(K/F)$ then $G = G_t \neq G_{t+1}$. According to Lemma 6.11, if

$$s = \min\{v_{K/F}(u), v_{K/F}(v)\},$$

then $t \geq \psi_{K/F}(s)$ which, by Lemma 6.10, is therefore equal to s. Since $\tau_{K/F}(uv) = \tau_{K/F}(u)\tau_{K/F}(v)$, $\tau_{K/F}(uv)$ lies in U_F^s. On the other hand

$$\tau_{K/F}(uv) = N_{E/F}(\tau_{K/E}(uv))$$

so that, by Lemma 6.10 again, $\tau_{K/E}(uv)$ belongs to U_E^s and

$$v_{K/F}(uv) \geq \varphi_{E/F}(s) = s.$$

Thus the sets $W_{K/F}^x$, $x \geq -1$, give a filtration of $W_{K/F}$ by a collection of normal subgroups. The next sequence of lemmas show that the filtration is quite analogous to the upper filtration of the Galois groups.

Lemma 6.14

For each $x \geq -1$ the map $\tau_{K/F,L/F}$ takes $G_{K/F}^x$ into $G_{L/F}^x$.

If w belongs to $W_{K/F}$ let $\bar{w} = \tau_{K/F,L/F}(w)$. We must show that

$$v_{L/F}(\bar{w}) \geq v_{K/F}(w).$$

Let $\sigma = \sigma(w)$ and let $\bar{\sigma} = \sigma(\bar{w})$. If E is the fixed field of σ then $\overline{E} = E \cap L$ is the fixed field of $\bar{\sigma}$. Since

$$v_{L/F}(\bar{w}) = \varphi_{\overline{E}/F}(v_{L/\overline{E}}(\bar{w}))$$

and

$$v_{K/F}(w) = \varphi_{\overline{E}/F}(v_{K/\overline{E}}(w))$$

we may suppose $\overline{E} = F$. Since $\tau_{K/F}(w) = \tau_{L/F}(\bar{w})$, Lemma 6.12 implies that $\tau_{L/F}(\bar{w})$ lies in $U_F^{v_{K/F}(w)}$. Thus

$$v_{L/F}(\bar{w}) = v_F(\tau_{L/F}(\bar{w})) \geq v_{K/F}(w).$$

Of course $W_{F/F}$ is C_F and, if $v \geq -1$, $W_{F/F}^v = U_F^v$.

Lemma 6.15

For each $v \geq -1$, $\tau_{K/F}$ *maps* $W^v_{K/F}$ *onto* U^v_F.

Since $v_1 \leq v_2$ implies $W^{v_2}_{K/F} \subseteq W^{v_1}_{K/F}$ it is enough to prove the lemma when $v = n$ is an integer. The lemma is clear if $[K : F] = 1$; so we proceed by induction on $[K : F]$. If $[K : F] > 1$, choose an intermediate normal extension L so that $[L : F] = \ell$ is a prime. Let $\overline{G} = \mathfrak{G}(L/F)$. Lemma 6.12 implies that

$$W^{\psi_{L/F}(v)}_{K/L} = W_{K/L} \cap W^v_{K/F}.$$

There is an integer $t \geq -1$ such that $\overline{G} = \overline{G}_t$ and $\overline{G}_{t+1} = \{1\}$. It is shown in Chapter V of Serre's book that if $n > t$

$$N_{L/F}\ \left(U^{\psi_{L/F}(n)}_L\right) = U^n_F.$$

By induction

$$\tau_{K/L}\left(W^{\psi_{L/F}(n)}_{K/L}\right) = U^{\psi_{L/F}(n)}_L.$$

Since $\tau_{K/F}(w) = N_{L/F}(\tau_{K/L}(w))$ if w is in $W_{K/L}$,

$$\tau_{K/F}(W^n_{K/F}) = U^n_F$$

if $n > t$. Suppose $\overline{\sigma}$ generates $\overline{G}$. Then $V_{L/F}(\overline{\sigma}) = t$. By Herbrand's theorem there is a σ in $\mathfrak{G}(K/F)$ with $v_{K/F}(\sigma) = t$ whose restriction to L is $\overline{\sigma}$. By Lemma 6.11 there is a w in $W_{K/F}$ such that $\sigma = \sigma(w)$ and $v_{K/F}(w) = t$. Then $\tau_{K/F}(w)$ lies in U^t_F but not in $N_{L/F}(C_L)$. From Serre's book again

$$\left[U^t_F : N_{L/F}\ U^{\psi_{L/F}(t)}_F\right] = \ell$$

so that U^t_F is generated by $\tau_{K/F}(w)$ and $N_{L/F}(U^{\psi_{L/F}(t)}_L)$ and hence is contained in the image of $W^t_{K/F}$. To complete the proof of the lemma we have only to observe that Lemma 6.10 implies that

$$U^n_F = U^t_F\, N_{L/F}\ \left(U^{\psi_{L/F}(n)}_L\right)$$

if $n \leq t$.

Lemma 6.16

Suppose $F \subseteq L \subseteq K$ *and* L/F *and* K/F *are Galois. Then, for each* $v \geq -1$, $\tau_{K/F,L/F}$ *maps* $W^v_{K/F}$ *onto* $W^v_{L/F}$.

If $[L : F] = 1$ this is just the previous lemma so we proceed by induction on $[L : F]$. We have to show that if $\overline{w}$ belongs to $W_{L/F}$ there is a w in $W_{K/F}$ such that $\overline{w} = \tau_{K/F,L/F}(w)$ and $v_{K/F}(w) \geq v_{L/F}(\overline{w})$. Let $\overline{\sigma} = \sigma(\overline{w})$ and let $\overline{E}$ be the fixed field of $\overline{\sigma}$. If $\overline{E} \neq F$ then, by the induction assumption, there is a w in $W_{K/E}$ such that $\tau_{K/\overline{E},L/\overline{E}}(w) = \overline{w}$ and $v_{K/\overline{E}}(w) \geq v_{L/\overline{E}}(\overline{w})$. By Lemma 6.12, $v_{K/F}(w) \geq v_{L/F}(\overline{w})$. Moreover, we may assume that $\tau_{K/\overline{E},L/\overline{E}}$ is the restriction to $W_{K/\overline{E}}$ of $\tau_{K/F,L/F}$.

Suppose $\overline{E} = F$. Then $v_{L/F}(\overline{w}) = v_F(\tau_{L/F}(\overline{w}))$. Choose w_1 in $W_{K/F}$ so that $\tau_{K/F}(w_1) = \tau_{L/F}(\overline{w})$ and $v_{K/F}(w_1) \geq v_F(\tau_{L/F}(\overline{w}))$. Let $\overline{w}_1 = \tau_{K/F,L/F}(w_1)$ and set $\overline{u} = \overline{w}_1^{-1}\overline{w}$. Certainly $v_{L/F}(\overline{u}) \geq v_{L/F}(\overline{w})$. Moreover, $\tau_{L/F}(\overline{u}) = 1$. Let $F \subseteq L_1 \subseteq L$ where L_1/F is cyclic of prime order. If $\overline{u}$ does not belong to W_{L/L_1} the group C_F is generated by $N_{L_1/F}(C_{L_1})$ and $\tau_{L/F}(\overline{u})$, which is impossible since $\tau_{L/F}(\overline{u}) = 1$. Thus $\overline{u}$ belongs to W_{L/L_1} and, as observed, there is a u in W_{K/L_1} such that $\tau_{K/F,L/F}(u) = \tau_{K/L_1,L/L_1}(u) = \overline{u}$. Then $\tau_{K/F,L/F}(uw_1) = \overline{w}$.

Chapter Seven.

Consequences of Stickelberger's Result

Davenport and Hasse [5] have shown that Stickelberger's arithmetic characterization of Gaussian sums over a finite field can be used to establish identities between these Gaussian sums. After reviewing Stickelberger's result we shall prove the identities of Davenport and Hasse together with some more complicated identities. However for the proof of Stickelberger's result itself, I refer to Davenport and Hasse.

If $Z = e^{\frac{2\pi i}{p}}$ and α belongs to $GF(p)$ the meaning of Z^α is clear. If κ is any finite field and S is the absolute trace of κ let ψ^0_κ be the character of κ defined by $\psi^0_\kappa(\alpha) = Z^{S(\alpha)}$. If χ_κ is any character of κ^* and ψ_κ is any non-trivial additive character of κ we will take the Gaussian sum $\tau(\chi_\kappa, \psi_\kappa)$ to be

$$-\sum\nolimits_{\alpha\in\kappa^*} \chi_\kappa^{-1}(\alpha)\psi_\kappa(\alpha).$$

We abbreviate $\tau(\chi_\kappa, \psi^0_\kappa)$ to $\tau(\chi_\kappa)$.

Let $\mathfrak{k}_n$ be the field obtained by adjoining the n^{th} roots of unity to the rational numbers. If $\varpi = Z-1$ then in $\mathfrak{k}_p$ the ideal (p) equals (ϖ^{p-1}). If $q = p^f$ and κ has q elements then in $\mathfrak{k}_{q-1}$ the ideal (p) is a product $\mathfrak{p}\mathfrak{p}' \ldots$ where the residue fields of $\mathfrak{p}\mathfrak{p}', \ldots$ are isomorphic to κ. In $\mathfrak{k}_{p(q-1)}$

$$(p) = (\mathfrak{p}\,\mathfrak{p}' \ldots)^{p-1}$$

with $\mathfrak{P} = (\mathfrak{p}, \varpi)$, $\mathfrak{P}' = (\mathfrak{p}', \varpi)$, and so on. The residue fields of $\mathfrak{P}, \mathfrak{P}', \ldots$ are also isomorphic to κ. Choose one of these prime ideals, say $\mathfrak{P}$. Once an isomorphism of the residue field with κ is chosen the map of the $(q-1)^{\text{th}}$ roots of unity to the residue field defines an isomorphism of κ^* and the group of $(q-1)^{\text{th}}$ roots of unity. Then χ_κ can be regarded as a character of the latter group. Choose $\alpha = \alpha(\chi_\kappa, \mathfrak{P})$ with $0 \le \alpha < q-1$ so that $\chi_\kappa(\zeta) = \zeta^\alpha$ for all $(q-1)^{\text{th}}$ roots of unity. Write

$$\alpha = \alpha_0 + \alpha_1 p + \ldots + \alpha_{f-1}p^{f-1} \qquad 0 \le \alpha_i < p.$$

Not all of the α_i can be equal to $p-1$. Set

$$\sigma(\alpha) = \alpha_0 + \alpha_1 + \ldots + \alpha_{f-1}$$
$$\gamma(\alpha = \alpha_0!\alpha_1! \ldots \alpha_{f-1}!$$

The following lemma is Stickelberger's arithmetical characterization of $\tau(\chi_\kappa)$.

Lemma 7.1

(a) *$\tau(\chi_\kappa)$ lies in $\mathfrak{k}_{p(q-1)}$ and is an algebraic integer.*

(b) *If $\chi_\kappa = 1$ then $\tau(\chi_\kappa) = 1$ but if $\chi_\kappa \ne 1$ the absolute value of $\tau(\chi_\kappa)$ and all its conjugates is $\sqrt{q}$.*

(c) *Every prime divisor of $\tau(\chi_\kappa)$ in $\mathfrak{k}_{p(q-1)}$ is a divisor of p.*

(d) *If β is a non-zero element of the prime field then the automorphism $Z \longrightarrow Z^\beta$ of $\mathfrak{k}_{p(q-1)}$ over $\mathfrak{k}_{q-1}$ sends $\tau(\chi_\kappa)$ to $\chi_\kappa(\beta)\,\tau(\chi_\kappa)$.*

(e) *If* $\mathfrak{P}$ *is a prime divisor of* p *in* $\mathfrak{k}_{p(q-1)}$ *and* $\alpha = \alpha(\chi_\kappa, p)$ *the multiplicative congruence*

$$\tau(\chi_\kappa) \equiv \frac{\varpi^{\sigma}(\alpha)}{\gamma(\alpha)} \qquad (\operatorname{mod}^* \mathfrak{P})$$

is valid.

(f) *Suppose* ℓ *is a prime dividing* $q-1$ *and* $\chi_\kappa = \chi'_\kappa \chi''_\kappa$ *where the order of* χ'_κ *is a power of* ℓ *and that of* χ''_κ *is prime to* ℓ. *If* ℓ^a *is the exact power of* ℓ *dividing* $q-1$ *and* $\lambda = \zeta_0 - 1$ *where* ζ_0 *is a primitive* ℓ^a*-th root of unity then*

$$\tau(\chi_\kappa) \equiv \tau(\chi''_\kappa) \pmod{\lambda}.$$

Before stating the identities for Gaussian sums which are implied by this lemma, I shall prove a few elementary lemmas.

Lemma 7.2

Suppose $0 \le \alpha < p^f - 1$ *and*

$$\alpha = \alpha_0 + \alpha_1 p + \ldots + \alpha_{f-1} p^{f-1} \quad 0 \le \alpha_i < p.$$

Suppose also that $0 \le j_0 < j_1 < \ldots < j_r = f$ *and set*

$$\beta_s = \alpha_{j_s} + \alpha_{j_s+1}\, p + \ldots + \alpha_{j_{s+1}-1}\, p^{j_{s+1}-j_s-1}.$$

If $\sigma = \sum_{s=0}^{r-1} \beta_s$ *and* $\gamma = \prod_{s=0}^{r-1} \beta_s!$ *then*

$$\frac{\varpi^{\sigma}}{\gamma} = \frac{\varpi^{\sigma(\alpha)}}{\gamma(\alpha)} \quad (\operatorname{mod}^* \mathfrak{P}).$$

First of all, I remark once and for all that if $n \ge 1$, $0 < u \le p^n - 1$, and $v = u (\operatorname{mod} p^n)$ then $v \equiv u (\operatorname{mod}^* p)$. Thus if $0 \le u \le p^n - 1$ and $v \ge 0$

$$(u + vp^n)! = (vp^n)! \prod_{w=1}^{u} (w + vp^n) \equiv u!(vp^n)! \quad (\operatorname{mod}^* p).$$

Also if $v \ge 0$

$$\prod_{w=1}^{p^n} (vp^n + w) \equiv (v+1)\, p^n! \quad (\operatorname{mod}^* p)$$

and, by induction,

$$(vp^n)! \equiv v!(p^n!)^v \quad (\operatorname{mod}^* p).$$

In particular $p^{(n+1)}! \equiv p!(p^n!)^p \equiv (-p)\,(p^n!)^p$. Apply induction to obtain

$$p^n! \equiv (-p)^{\frac{p^n-1}{p-1}} \quad (\operatorname{mod}^* p).$$

From the relations

$$p = \prod_{i=1}^{p-1} (1 - Z^i) = (-\varpi)^{p-1} \prod_{i=1}^{p-1} \frac{Z^i - 1}{Z - 1}$$

and

$$\frac{Z^i - 1}{Z - 1} = 1 + Z + \ldots + Z^{i-1} \equiv i \pmod{^*p}.$$

We conclude that

$$p = (p-1)!(-\varpi)^{p-1} \equiv -\varpi^{p-1} \pmod{^*p}.$$

The lemma itself is clear if $r = f$ so we proceed by induction downward from f. Suppose $r < f$, $j_{s+2} - j_s = t > 1$, and the lemma is valid for the sequence $j_0, j_1, \ldots, j_{s+1} - 1$, $j_{s+1}, \ldots j_r$. To prove it for the given sequence we have only to show that if

$$x = \alpha_{j_s} + \alpha_{j_s+1}\, p + \ldots + \alpha_{j_{s+1}-2}\, p^{t-2}$$

and $y = \alpha_{j_{s+1}-1}$ then

$$\frac{\varpi^{x+y}}{x!y!} \equiv \frac{\varpi^{x+yp^{t-1}}}{(x+yp^{t-1})!} \pmod{^*p}.$$

But

$$\varpi^{y(p^{t-1}-1)} \equiv (-p)^{y\frac{p^{t-1}-1}{p-1}} \pmod{^*p}$$

and

$$(x+yp^{t-1})! = x!y!(p^{t-1}!)^y \equiv x!y!(-p)^{\frac{y^{t-1}-1}{p-1}} \quad (\mathrm{mod})^*p).$$

Lemma 7.3

Suppose $\beta_0, \ldots, \beta_{r-1}$ and $\gamma_0, \ldots, \gamma_{r-1}$ are non-negative integers all of which are less than or equal to $q-1$. Suppose that $q = p^f$ is a prime power and

$$\sum_{i=0}^{r-1} (\beta_i + \gamma_i) q^i < 2(q^r - 1).$$

Suppose also that $\delta_i, 0 \le i \le r-1$, are given such that $0 \le \delta_i \le q-1$,

$$\sum_{i=0}^{r-1} \delta_i q^i < q^r - 1$$

and

$$\sum_{i=0}^{r-1} (\beta_i + \gamma_i) q^i = \sum_{i=0}^{r-1} \delta_i q^i \pmod{q^r - 1}.$$

(a) *If $\sum_{i=0}^{r-1} (\beta_i + \gamma_i) q^i < q^{r-1}$ and if ν is the number of k, $1 \le k \le r$, for which $\sum_{i=0}^{k-1} (\beta_i + \gamma_i) \ge q^k$ then*

$$\sum_{i=0}^{r-1} (\beta_i + \gamma_i - \delta_i) = \nu(q-1).$$

(b) *If $\sum_{i=0}^{r-1} (\beta_i + \gamma_i) q^i \ge q^r - 1$ and if ν is the number of k, $1 \le k \le r$, for which $1 \ne \sum_{i=0}^{k-1} (\beta_i + \gamma_i) q^i \ge q^k$ then*

$$\sum_{i=0}^{r-1} (\beta_i + \gamma_i - \delta_i) = \nu(q-1).$$

Observe immediately that if $1 \le k \le r$, then $0 \le \beta_{k-1} + \gamma_{k-1} \le 2(q-1)$ and

$$\sum\nolimits_{i=0}^{k-1} (\beta_i + \gamma_i) q^i \le 2(q-1) \ \sum\nolimits_{i=0}^{k-1} q^i = 2(q^k - 1).$$

If $r = 1$ then $\beta_0 + \gamma_0 = \delta_0 + \varepsilon(q-1)$ with ε equal to 0 or 1. If $\varepsilon = 0$ we are in case (a) and $\nu = 0$ while $\beta_0 + \gamma_0 - \delta_0 = 0$. If $\varepsilon = 1$ we are in case (b); here $\nu = 1$ and $\beta_0 + \gamma_0 - \delta_0 = q - 1$. Suppose then that $r \ge 2$ and that if $\beta'_0, \dots, \beta'_{r-1}, \gamma'_0, \dots, \gamma'_{r-2}$, $\delta'_0, \dots, \delta'_{r-2}$, and ν' are given as in the lemma (with r replaced by $r-1$) then

$$\sum\nolimits_{i=0}^{r-2} (\beta'_i + \gamma'_i - \delta'_i) = \nu'(q-1).$$

We establish part (a) first. In this case

$$\sum\nolimits_{i=0}^{r-1} (\beta_i + \gamma_i) q^i = \sum\nolimits_{i=0}^{r-1} \ \delta_i q^i$$

and

$$\sum\nolimits_{i=0}^{r-2} (\beta_i + \gamma_i) q^i = \sum\nolimits_{i=0}^{r-2} \delta_i q^i + \varepsilon q^{r-1}$$

with $\varepsilon = \delta_{r-1} - \beta_{r-1} - \gamma_{r-1}$. If ε were negative the left side of the equation would be negative; if ε were greater than 1 the left side would be greater than $2(q^{r-1} - 1)$. Since neither of these possibilities occur ε is 0 or 1.

Suppose first that $\varepsilon = 0$. If $\sum_{i=0}^{r-2} \delta_i q^i < q^{r-1} - 1$ choose $\beta'_i = \beta_i,\ \gamma'_i = \gamma_i,\ 0 \le i \le r-2$. Then $\delta'_i = \delta_i,\ 0 \le i \le r-2$, and $\nu' = \nu$. The assertion of the lemma follows in this case. If $\sum_{1=0}^{r-2} \delta_i q^i = q^{r-1} - 1$ then $\delta_i = q-1,\ 0 \le i \le r-2$. Then $\beta_0 + \gamma_0 \equiv q - 1 \pmod q$ and, as a consequence, $\beta_0 + \gamma_0 = q - 1$. We show by induction that $\beta_i + \gamma_i = q - 1,\ 0 \le i \le r-2$. If this is so for $i < j$ then

$$\sum\nolimits_{i=j}^{r-2} (\beta_i + \gamma_i) q^i = \sum\nolimits_{i=j}^{r-2} (q-1) q^i.$$

Hence $\beta_j + \gamma_j \equiv q - 1 \pmod q$ and $\beta_j + \gamma_j = q - 1$. It follows immediately that $\nu = 0$ and $\sum_{i=0}^{r-1} (\beta_i + \gamma_i - \delta_i) = 0$.

Now suppose that $\varepsilon = 1$. If

$$\sum\nolimits_{i=0}^{r-2} (\beta_i + \gamma_i) q^i = 2(q^{r-1} - 1)$$

then $\beta_i = \gamma_i = q - 1,\ 0 \le i \le r-2,\ \delta_0 = q - 2$, and $\delta_i = q - 1,\ 1 \le i \le r-2$. Thus $\nu = r - 1$ and

$$\sum\nolimits_{i=0}^{r-1} (\beta_i + \gamma_i - \delta_i) = 1 + (r-1)(q-1) - 1 = (r-1)(q-1).$$

Suppose then that

$$\sum\nolimits_{i=0}^{r-2} (\beta_i + \gamma_i) q^i < 2(q^{r-1} - 1).$$

From the relation

$$\sum\nolimits_{i=0}^{r-2} (\beta_i + \gamma_i) q^i = \sum\nolimits_{i=0}^{r-2} \delta_i q^i + 1 + (q^{r-1} - 1).$$

We conclude that $\sum_{i=0}^{r-2}\delta_i q^i < q^{r-1}-1$. Then for some m, with $0 \le m \le r-2$, $\delta_m < q-1$. We choose the minimal value for m.

$$\sum_{i=0}^{r-2}(\beta_i+\gamma_i)q^i = (\delta_m+1)q^m + \sum_{i=m+1}^{r-2}\delta_i q^i + (q^{r-1}-1).$$

Thus if $\beta_i' = \beta_i,\ \gamma_i' = \gamma_i,\ 0 \le i \le r-2$, then $\delta_i' = 0,\ i < m,\ \delta_m' = \delta_m + 1$, and $\delta_i' = \delta_i,\ m < i \le r-2$. Arguing by congruences as before we see that $\beta_i + \gamma_i = q-1$ for $i < m$. Thus

$$\sum_{i=0}^{k-1}(\beta_i+\gamma_i)q^i = q^k - 1$$

for $k \le m$. However $\beta_m + \gamma_m \ne q-1$ and thus $\beta_m + \gamma_m + 1$ is prime to q. Moreover if $r-1 \ge k > m$

$$1 + \sum_{i=1}^{k-1}(\beta_i+\gamma_i)q^i \equiv (\beta_m+\gamma_m+1)q^m \pmod{q^{m+1}}.$$

Thus it is greater than or equal to q^k if and only if it is greater than or equal to q^k+1. It follows that $\nu' = \nu + m$ and that

$$\sum_{i=0}^{r-2}(\beta_i+\gamma_i-\delta_i) = -m(q-1) + \sum_{i=0}^{r-2}(\beta_i'+\gamma_i'-\delta_i') = \nu(q-1)+1.$$

Since $\beta_{r-1}+\gamma_{r-1}-\delta_{r-1} = -1$ the assertion of the lemma follows.

Now let us treat part (b). In this case

$$\sum_{i=0}^{r-1}(\beta_i+\gamma_i)q^i = \sum_{i=0}^{r-1}\delta_i q^i + (q^r-1)$$

and

$$1 + \sum_{i=0}^{r-2}(\beta_i+\gamma_i)q^i = \sum_{i=0}^{r-2}\delta_i q^i + \varepsilon q^{r-1}$$

with $\varepsilon = \delta_{r-1} - \beta_{r-1} - \gamma_{r-1} + q$. Again ε is 0 or 1. If $\beta_i = \gamma_i = q-1$ for $0 \le i \le r-2$ then $\varepsilon = 1$ and $\delta_i = q-1$ for $0 \le i \le r-2$. Also $\nu = r$ and

$$\sum_{i=0}^{r-1}(\beta_i+\gamma_i-\delta_i) = (r-1)\,(q-1) + \beta_{r-1}+\gamma_{r-1}-\delta_{r-1} = r(q-1).$$

Having taken care of this case, we suppose that

$$\sum_{i=0}^{r-2}(\beta_i+\gamma_i)q^i < 2(q^{r-1}-1).$$

First take $\varepsilon = 0$. If $\delta_0 = 0$ then $1+\beta_0+\gamma_0 \equiv 0 \pmod q$ and $\beta_0+\gamma_0 = q-1$. Thus one of them is less than $q-1$. By symmetry we may suppose it is β_0. Let $\beta_0' = \beta_0+1,\ \beta_i' = \beta_i,\ 1 \le i \le r-2$, and $\gamma_i' = \gamma_i,\ 0 \le i \le r-2$. Since $\delta_0 = 0$

$$\sum_{i=0}^{r-2}\delta_i q^i \le q^{r-1} - q < q^{r-1} - 1$$

and $\delta_i' = \delta_i$, $0 \le i \le r-1$. Also $\nu = \nu'+1$ so that

$$\sum_{i=0}^{r-1}(\beta_i+\gamma_i-\delta_i) = \sum_{i=0}^{r-2}(\beta_i'+\gamma_i'-\delta_i') - 1 + q = \nu(q-1)$$

as required. If $\delta_0 > 0$ take $\beta'_i = \beta_i$ and $\gamma'_i = \gamma_i$, $0 \le i \le r-2$. Then $\delta'_0 = \delta_0 - 1,\ \delta'_i = \delta_i,\ 1 \le i \le r-2$. Also if $k \le r-1$

$$\sum_{i=0}^{k-1} (\beta_i + \gamma_i) q^i \equiv \delta_0 - 1 \ne -1 (\operatorname{mod} q)$$

and the left-hand side is greater than or equal to q^k if and only if it is greater than or equal to $q^k - 1$. It follows that $\nu = \nu' + 1$. Consequently

$$\sum_{i=0}^{r-1} (\beta_i + \gamma_i - \delta_i) = \sum_{i=0}^{r-2} (\beta'_i + \gamma'_i - \delta'_i) - 1 + q = \nu(q-1).$$

If $\varepsilon = 1$ take $\gamma'_i = \gamma_i$ and $\beta'_i = \beta_i,\ 0 \le i \le r-2$. Then $\delta'_i = \delta_i,\ 0 \le i \le r-2$, and $\nu = \nu' + 1$ so that

$$\sum_{1=0}^{r-1} (\beta_i + \gamma_i - \delta_i) = \nu'(q-1) + (\beta_{r-1} + \gamma_{r-1} - \delta_{r-1}) = \nu(q-1).$$

Lemma 7.4

Suppose β_i and γ_i are two periodic sequences of integers with period r. That is $\beta_{i+r} = \beta_i$ and $\gamma_{i+r} = \gamma_i$ for all i in $\mathbb{Z}$. Suppose $0 \le \beta_i \le q-1,\ 0 \le \gamma_i \le q-1$ for all i and that none of the numbers

$$\varepsilon_k = \sum_{i=0}^{r-1} (\beta_{i+k} + \gamma_{i+k}) q^i$$

is divisible by $q^r - 1$. Let

$$\sum_{i=0}^{r-1} (\beta_i + \gamma_i) q^i \equiv \sum_{i=0}^{r-1} \delta_i q^i \ (\operatorname{mod} q^r - 1)$$

with $0 \le \delta_i \le q-1$ and $\sum_{i=0}^{r-1} \delta_i q^i < q^r - 1$. If μ is the number of $\varepsilon_k,\ 1 \le k \le r$, which are greater than or equal to $q^r - 1$ then

$$\sum_{i=0}^{r-1} (\beta_i + \gamma_i - \delta_i) = \mu(q-1).$$

Since $\varepsilon_0 \le 2(q^r - 1)$ and is not divisible by $q^r - 1$ it is less than $2(q^r - 1)$. Thus all we need do is show that the μ of this lemma is equal to the ν of the preceding lemma. Observe first of all that $\varepsilon_j \ge q^r - 1$ if and only if $\varepsilon_j \ge q^r$.

Suppose $\varepsilon_0 < q^r$. If $1 \le k < r$

$$\sum_{i=k}^{r-1} (\beta_i + \gamma_i) q^i < q^r$$

so that

$$\sum_{i=k}^{r-1} (\beta_i + \gamma_i) q^{i-k} < q^{r-k}.$$

Thus, if $\varepsilon_k \ge q^r$,

$$\begin{aligned} q^r &\le \sum_{i=r-k}^{r-1} (\beta_{i+k} + \gamma_{i+k})\, q^i + \sum_{i=0}^{r-k-1} (\beta_{i+k} + \gamma_{i+k}) q^i \\ &< q^{r-k} \sum_{i=0}^{k-1} (\beta_i + \gamma_i) q^i + q^{r-k} \end{aligned}$$

and

$$\sum_{i=0}^{k-1}(\beta_i+\gamma_i)q^i \geq q^k.$$

Conversely if $1 \leq k < r$ and

$$\sum_{i=0}^{k-1}(\beta_i+\gamma_i)q^i \geq q^k,$$

then

$$\begin{aligned}\sum_{i=0}^{r-1}(\beta_{i+k}+\gamma_{i+k})q^i &\geq \sum_{i=r-k}^{r-1}(\beta_{i+k}+\gamma_{i+k})q^i \\ &= q^{r-k}\sum_{i=0}^{k-1}(\beta_i+\gamma_i)q^i \geq q^r.\end{aligned}$$

Thus $\mu = \nu$ in this case.

Now suppose $\varepsilon_0 \geq q^r$. If $1 \leq k < r$

$$\sum_{i=k}^{r-1}(\beta_i+\gamma_i)q^i \geq q^r - \sum_{i=0}^{k-1}(\beta_i+\gamma_i)q^i \geq q^r - 2(q^k-1).$$

If

$$\sum_{i=0}^{k-1}(\beta_i+\gamma_i)q^i \geq q^k - 1$$

then

$$\begin{aligned}\sum_{i=0}^{r-1}(\beta_{i+k}+\gamma_{i+k})q^i &\geq \sum_{i=r-k}^{r-1}(\beta_{i+k}+\gamma_{i+k})q^i + \sum_{i=0}^{r-k-1}(\beta_{i+k}+\gamma_{i+k})q^i \\ &= q^{r-k}\sum_{i=0}^{k-1}(\beta_i+\gamma_i)q^i + q^{-k}\sum_{i=k}^{r-1}(\beta_i+\gamma_i)q^i \\ &\geq q^{r-k}(q^k-1) + q^{r-k} - 2 + 2q^{-k}.\end{aligned}$$

Thus $\varepsilon_k \geq q^r - 1$ and hence $\varepsilon_k \geq q^r$. Conversely if $\varepsilon_k \geq q^r$,

$$\begin{aligned}q^{r-k}\sum_{i=0}^{k-1}(\beta_i+\gamma_i)q^i &= \sum_{i=r-k}^{r-1}(\beta_{i+k}+\gamma_{i+k})q^i \\ &\geq q^r - \sum_{i=0}^{r-k-1}(\beta_{i+k}+\gamma_{i+k})q^i \\ &\geq q^r - 2(q^{r-k}-1) \\ &= q^r - 2q^{r-k} + 2.\end{aligned}$$

Thus

$$\sum_{i=0}^{k-1}(\beta_i+\gamma_i)q^i \geq q^k - 1$$

and again $\mu = \nu$.

Lemma 7.5

Suppose $q = p^f$ is a prime power, ℓ is a positive integer, and $(\ell, q) = 1$. Let $\ell m \equiv 1 \pmod{q}$ and if x is any integer let $\varphi(x)$, with $0 \leq \varphi(x) < q$, be the remainder of x upon division by q. If $0 \leq \beta < q$ and if $\psi(x) = \varphi(x)!$

$$\frac{\ell\beta}{\beta!}\prod_{k=0}^{\ell-1}\frac{\psi((\beta-k)m)}{\psi(-km)} \equiv 1 (\bmod^* p).$$

If $\ell = \ell_1 + uq$ with $\ell_1 > 0$ and $u \geq 0$ then $\ell^\beta \equiv \ell_1^\beta (\operatorname{mod}^* p)$. Moreover

$$\prod_{k=0}^{\ell-1} \frac{\psi((\beta-k)m)}{\psi(-km)} = \left\{\prod_{k=0}^{\ell_1-1} \frac{\psi((\beta-k)m)}{\psi(-km)}\right\} \left\{\prod_{k=\ell_1}^{\ell-1} \frac{\psi((\beta-k)m)}{\psi(-km)}\right\}$$

and

$$\prod_{k=\ell_1}^{\ell-1} \psi(-km) = \{\prod_{j=0}^{q-1} j!\}^u = \prod_{k=\ell_1}^{\ell-1} \psi((\beta-k)m).$$

Thus it is enough to prove the lemma with ℓ replaced by ℓ_1. In other words we may suppose that $0 < \ell < q$. The case $\ell = 1$ is trivial and we exclude it from the following discussion. Finally we suppose that $0 < m < q$.

Let $q-1 = r\ell + s$ with $0 < r$ and $0 \leq s < \ell$. Arrange the integers from 0 to $q-1$ into the following array.

$$\begin{array}{ccccccccccc}
0 & 1 & 2 & . & . & . & . & . & . & . & l-1 \\
l & l+1 & l+2 & . & . & . & . & . & . & . & 2l-1 \\
. & . & & & & & & & & & . \\
. & . & & & & & & & & & . \\
. & . & & & & \beta-l+1 & & & & & . \\
. & . & . & & \beta & & & & & & . \\
. & . & & & & & & & & & . \\
. & . & & & & & & & & & . \\
(r-1)l & (r-1)l+1 & & & & & & & q-l & . & rl-1 \\
rl & rl+1 & . & . & . & . & . & rl+s & & &
\end{array}$$

Since ℓ does not divide q, $r\ell + s = q - 1$ does not lie in the last column. Also $q - \ell$ lies in the column following that in which $r\ell + s$ lies.

We replace each number j in the above array by $\varphi(jm)$. The resulting array, which is written out below, has some special features which must be explained. The first column is explained by the observation $x\ell m \equiv x (\operatorname{mod} q)$. The other entries, apart from those at the foot of each column, are explained by the observation that, when $1 \leq j$ and $x\ell + j$ lies in the first array, $\varphi(x + mj) > r$ while $0 < \varphi(mj) + x < q + r$ so that $\varphi(x + mj) = \varphi(mj) + x$. The position of $q - 1$ is explained by the relation $m(q - \ell) \equiv -m\ell \equiv q - 1 (\operatorname{mod} q)$. The other entries at the feet of the columns are explained by the observation that if $1 \leq j \leq \ell - 1$ then $\varphi(jm) > r \geq 1$ while $m(q - k) = m(q - \ell) + m(\ell - k) \equiv \varphi((\ell - k)m) - 1 (\operatorname{mod} q)$ if $1 \leq k \leq \ell - 1$.

$$\begin{array}{cccccccccc}
0 & m & . & . & . & . & . & . & . & \varphi((l-1)m) \\
l & m+1 & . & . & . & . & . & . & . & \varphi((l-1)m)+1 \\
. & . & & & & & & & & . \\
. & . & & & & & & & & . \\
. & . & & & \varphi((\beta-l+1)m) & & & & & . \\
. & . & . & \varphi(\beta m) & & & & & & . \\
. & . & & & & & & & & . \\
. & . & & & & & & & & . \\
r-1 & m+r-1 & & & & & & q-1 & . & \varphi((l-2-s)m)-1 \\
r & m+r & . & . & . & . & \varphi((l-1)m)-1 & & &
\end{array}$$

Suppose first of all that $\beta < \ell - 1$. Then the numbers $\varphi((\beta - k)m),\ 0 \le k \le \ell - 1$ constitute the first $\beta + 1$ together with the last $\ell - \beta - 1$ numbers in the array. (The order of the numbers in the array is the order in which they appear when the array is read as though it were a printed page.) The numbers $\varphi(-km),\ 1 \le k \le \ell - 1$, are the last $\ell - 1$ numbers of the array, that is, the numbers after $q - 1$. Cancelling in the product of the lemma the terms in numerator and denominator corresponding to the last $\ell - \beta - 1$ terms of the array, we obtain

$$\prod_{j=1}^{\beta} \frac{\varphi(jm)!}{(\varphi(jm) - 1)!} = \prod_{j=1}^{\beta} \varphi(jm) \equiv m^{\beta}\beta!\ (\mathrm{mod}^* p)$$

as required.

Now take $\beta \ge \ell - 1$. Then the numbers $\beta, \beta - 1, \ldots, \beta - (\ell - 1)$ occur as indicated in the first array. In particular there is exactly one in each column. The numerator in the product of the lemma is the product of the factorials of the corresponding elements of the second array. The denominator is the product of the factorials of the elements appearing after $q - 1$. As indicated t is the element lying above $q - 1$. Thus t is larger than any element appearing in a column other than that of t. The product of the lemma is $t!$ times the product of the factorials of the other elements on the broken line divided by the factorials of the elements at the foot of the column in which they lie. Thus it equals $t!$ divided by the product of all the elements below the broken line except those which lie directly below t. But $t!$ is the product of all numbers in the second array except those which lie below t. Thus the quotient is the product of all numbers which lie above or on the broken line, that is,

$$\prod_{j=1}^{\beta} \varphi(jm) \equiv \prod_{j=1}^{\beta} jm = m^{\beta}\, \beta!\, (\mathrm{mod}^* p)$$

as required.

Lemma 7.6

Suppose that $q = p^f$ is a prime power, that ℓ is a positive integer dividing $q-1$, that $0 \le \alpha_1 < q-1$, that $(\ell, \alpha_1) = 1$, and that

$$\alpha_2 = \frac{\alpha_1}{\ell} \quad \frac{q^{\ell} - 1}{q - 1}.$$

Then α_2 is an integer and $0 \le \alpha_2 < q - 1$. Moreover if

$$\alpha_2 = \gamma_0 + \gamma_1 q + \ldots + \gamma_{\ell-1}\, q^{\ell-1}$$

with $0 \le \gamma_i \le q - 1$ for $0 \le i \le \ell - 1$ then

$$\sum_{j=0}^{\ell-1} \gamma_j = \alpha_1 + \sum_{j=1}^{\ell-1} \quad j \cdot \frac{q-1}{\ell}$$

and

$$\ell^{\alpha_1} \prod_{j=0}^{\ell-1} \gamma_j! \equiv \alpha_1! \prod_{j=1}^{\ell-1} \left(\frac{jq - 1!}{\ell}\right) \quad (\mathrm{mod}^* p).$$

Certainly $0 \le \alpha_2 < q^{\ell} - 1$; moreover

$$\frac{q^{\ell} - 1}{q - 1} = 1 + q + \ldots + q^{\ell-1} \equiv \ell \quad (\mathrm{mod}\, \ell)$$

so that α_2 is an integer. Let $\alpha_1 = m\ell + k$ with $m \geq 0$ and $0 \leq k < \ell$ and for $0 \leq j < \ell$ let

$$(\ell - 1 - j)k = i_j + \delta_j \ell$$

with $\delta_j \geq 0$ and $0 \leq i_j < \ell$. Clearly $i_{\ell-1} = \delta_{\ell-1} = 0$. Also $(\ell-1)k = \ell - k + \ell(k-1)$ so that $i_0 = \ell - k$ and $\delta_0 = k - 1$. If $j \geq 1$ then $(\delta_{j-1} - \delta_j)\ell = k + (i_j - i_{j-1})$. Since $-\ell < i_j - i_{j-1} < \ell$ and $0 < k < \ell$ the right-hand side is greater than $-\ell$ and less than 2ℓ so that $\delta_{j-1} - \delta_j$ is 0 or 1. If it is 1 then $k + i_j \geq \ell$ and $i_j \geq \ell - k$. If it is 0 then $i_j = i_{j-1} - k < \ell - k$. Recalling that $i_0 = \ell - k$ we see that

$$S = \{j | 1 \leq j \leq \ell - 1 \quad \text{and} \quad \delta_{j-1} - \delta_j = 1\} = \{j | 0 \leq j < \ell \quad \text{and} \quad i_j > \ell - k\}.$$

We shall prove that

$$\gamma_0 = m + i_0 \, \frac{(q-1)}{\ell} + k - \delta_0$$

and

$$\gamma_j = m + i_j \, \frac{(q-1)}{\ell} + \delta_{j-1} - \delta_j \quad 1 \leq j < \ell.$$

Since $(k, \ell) = 1$ the numbers i_j are distinct and it will follow immediately that

$$\sum\nolimits_{j=0}^{\ell-1} \gamma_j = (m\ell + k) + \sum\nolimits_{j=0}^{\ell-1} j \cdot \frac{q-1}{\ell} = \alpha_1 + \sum\nolimits_{j=1}^{\ell-1} \, j \cdot \frac{q-1}{\ell}.$$

Moreover we will have

$$\prod\nolimits_{j=0}^{\ell-1} \gamma_j! = \left\{ \prod\nolimits_{j=0}^{\ell-1} \, \left(m + j \, \frac{(q-1)}{\ell} \right)! \right\} \left\{ m + i_0 \, \frac{q-1}{\ell} + k - \delta_0 \right\} \left\{ \prod\nolimits_{j \in S} \left(m + 1 + i_j \, \frac{(q-1)}{\ell} \right) \right\}.$$

Recall that $k - \delta_0 = 1$. Dividing the first term by

$$\prod\nolimits_{j=0}^{\ell-1} \quad \left(j \cdot \frac{(q-1)}{\ell} \right)!$$

we obtain

$$\prod\nolimits_{j=0}^{\ell-1} \, \prod\nolimits_{n=1}^{m} \quad \left(n + j \, \frac{(q-1)}{\ell} \right).$$

The product of the last two terms is

$$\prod\nolimits_{j=\ell-k}^{\ell-1} \quad \left(m + 1 + j \, \frac{(q-1)}{\ell} \right).$$

If $1 \leq n \leq m$ and $0 \leq j \leq \ell - 1$ then $n\ell - j < \alpha_1 < q$ so that the product of ℓ^{mk} and the first of these two expressions is multiplicatively congruent to

$$\prod\nolimits_{j=0}^{\ell-1} \, \prod\nolimits_{n=1}^{m} \quad (n\ell - j) = (m\ell)!$$

Moreover, if $\ell-k \le j \le \ell-1$, then $0 \le (m+1)\ell-j \le (m+1)\ell-(\ell-k)=\alpha_1<q$ and the second of these expressions upon multiplication by ℓ^k becomes multiplicatively congruent to

$$\prod_{j=\ell-k}^{\ell-1}((m+1)\ell-j)=\prod_{j=1}^{k}(m\ell+j).$$

The relations together imply the second identity of the lemma.

To verify that the $\gamma_j,\ 0\le j<\ell$, have the form asserted, we start with the relation

$$\alpha_2=\frac{q^\ell-1}{q-1}\cdot\frac{m\ell+k}{\ell}=\sum_{j=0}^{\ell-1}q^jm+\sum_{j=0}^{\ell-1}\frac{q^jk}{\ell}.$$

The second term is equal to

$$\sum_{j=0}^{\ell-1}\left\{\left(\sum_{i=0}^{j-1}q^i\right)\ \frac{q-1}{\ell}\,k\right\}+k=k+\sum_{j=0}^{\ell-2}(\ell-1-j)q^j\cdot\frac{q-1}{\ell}\cdot k.$$

Thus

$$\begin{aligned}\alpha_2&=\left(m+(\ell-1)k\cdot\frac{q-1}{\ell}+k\right)+\sum_{j=1}^{\ell-1}\left(m+(\ell-1-j)k\cdot\frac{q-1}{\ell}\right)q^j\\&=\left(m+i_0\cdot\frac{q-1}{\ell}+k-\delta_0\right)+\sum_{j=1}^{\ell-1}\left(m+i_j\cdot\frac{q-1}{\ell}+\delta_{j-1}-\delta_j\right).\end{aligned}$$

Moreover $m<\frac{q-1}{\ell}$ so that

$$0\le m+i_0\cdot\frac{q-1}{\ell}+k-\delta_0<\ell\cdot\frac{q-1}{\ell}+1=q$$

and

$$0\le m+i_j\cdot\frac{q-1}{\ell}+\delta_{j-1}-\delta_j<\ell\cdot\frac{q-1}{\ell}+1=q.$$

The required relations follow immediately.

Now we can state and prove the promised identities for Gaussian sums. Each of these will amount to an assertion that a certain number in $\mathfrak{k}_{p(q-1)}$ is 1. To prove this we will show first that the number is invariant under all automorphisms of $\mathfrak{k}_{p(q-1)}$ over $\mathfrak{k}_{(q-1)}$ and thus lies in $\mathfrak{k}_{q-1}$. The only prime ideals occurring in the factorization of the number, which is not *a priori* an algebraic integer, into prime ideals will be divisors of p. We show that every conjugate of the number has absolute value 1 and that it is multiplicatively congruent to 1 modulo every divisor of p. It will follow that it is a root of unity in $\mathfrak{k}_{q-1}$ and hence a $(q-1)$th root of unity if q is odd and a $2(q-1)$th root of unity if q is even. If q is odd the multiplicative congruences imply that the number is 1. If q is even they imply that the number is ±1. To show that it is actually 1 some supplementary discussion will be necessary.

Stickelberger's result is directly applicable only to the normalized Gaussian sum $\tau(\chi_\kappa)$. We shall have to use the obvious relation $\tau(\chi_\kappa,\Psi_\kappa)=\chi_\kappa(\beta)\tau(\chi_\kappa)$ if $\psi_\kappa(\alpha)=\psi^0_\kappa(\beta\alpha)$. If κ is an extension of λ and ψ_λ is given, we set

$$\psi_{\kappa/\lambda}(\alpha)=\psi_\lambda(S_{\kappa/\lambda}(\alpha))$$

for α in κ. If χ_λ is given $\chi_{\kappa/\lambda}$ is the character defined by

$$\chi_{\kappa/\lambda}(\alpha) = \chi_\lambda(N_{\kappa/\lambda}(\alpha)).$$

Lemma 7.7

If κ is a finite extension of the finite field and χ_λ and ψ_λ are given then

$$\tau(\chi_{\kappa/\lambda}, \psi_{\kappa/\lambda}) = \{\tau(\chi_\lambda, \psi_\lambda)\}^{[\kappa:\lambda]}.$$

Since $\chi_{\kappa/\lambda}(\beta) = \chi_\lambda(\beta)^{[\kappa:\lambda]}$ it will be enough to show that

$$\tau(\chi_{\kappa/\lambda}) = \{\tau(\chi_\lambda)\}^{[\kappa:\lambda]}.$$

Set

$$\mu = \frac{\{\tau(\chi_\lambda)\}^{[\chi:\lambda]}}{\tau(\chi_{\kappa/\lambda})}.$$

Let λ have $q = p^\ell$ elements and let κ have $p^k = q^f$. It follows immediately from Lemma 7.1 that the absolute value of μ and all its conjugates is 1, that it lies in $\mathfrak{k}_{p(q^f-1)}$, that it is invariant under all automorphisms of $\mathfrak{k}_{p(q^f-1)}$ over $\mathfrak{k}_{q^f-1}$, and that its only prime factors are divisors of p. The mapping $\beta \longrightarrow N_{\kappa/\lambda}\beta$ sends β to $\beta^{\frac{q^f-1}{q-1}}$. Thus if $\alpha = \alpha(\chi_\lambda, \mathfrak{p})$ and $\mathfrak{P}$ divides $\mathfrak{p}$

$$\alpha(\chi_{\kappa/\lambda}, p) = \frac{q^f-1}{q-1}\,\alpha = \alpha + \alpha q + \ldots + \alpha q^{f-1}.$$

Applying Lemmas 7.1 and 7.2, we see that

$$\tau(\chi_\lambda) \equiv \frac{\varpi^\alpha}{\alpha!} \pmod{^*\mathfrak{P}}$$

and

$$\tau(\chi_{\kappa/\lambda}) \equiv \frac{\varpi^{f\alpha}}{(\alpha!)^f} \pmod{^*\mathfrak{P}}.$$

Consequently

$$\mu \equiv 1 \pmod{^*\mathfrak{P}}.$$

Thus $\mu = 1$ if q is odd and $\mu = \pm 1$ if q is even. If $\chi_\lambda = 1$ then $\chi_{\kappa/\lambda} = 1$ and, from part (b) of Lemma 7.1, μ is 1. If $q = 2$ then $\chi_\lambda = 1$. Suppose then q is even and greater than 2. If χ_λ is not identically 1 choose a prime r dividing the order of χ_λ. Set $\chi_\lambda = \chi'_\lambda\chi''_\lambda$ where the order of χ'_λ is a power of r and the order of χ''_λ is prime to r. The analogous decomposition of $\chi_{\kappa/\lambda}$ is $\chi'_{\kappa/\lambda}\chi''_{\kappa/\lambda}$. Of course χ_λ and $\chi_{\kappa/\lambda}$ have the same order. Define μ' and μ'' in the obvious way. According to part (f) of Lemma 7.1

$$\mu \equiv \mu'' \pmod r.$$

Since r does not divide 2 this implies that $\mu = \mu''$. Thus one can show by induction on the number of primes dividing the order of χ_λ that $\mu = 1$.

Lemma 7.8

Suppose λ is a finite field with q elements, κ is a finite extension of λ, and $[\kappa : \lambda] = f$. Suppose ℓ is a prime and the order of q modulo ℓ is f. Let T be a set of representatives for the orbits of the non-trivial characters of κ^* of order ℓ under the action of $\mathfrak{G}(\kappa/\lambda)$ and let χ_λ be a character of λ^*. If ψ_λ is any non-trivial character of λ

$$\chi_\lambda(\ell^\ell)\tau(\chi_\lambda^\ell, \psi_\lambda)\ \prod\nolimits_{\mu_\kappa \in T}\ \tau(\mu_\kappa, \psi_{\kappa/\lambda}) = \tau(\chi_\lambda, \psi_\lambda) \prod\nolimits_{\mu_\kappa \in T}\ \tau(\chi_{\kappa/\lambda}\ \mu_\kappa,\ \psi_{\kappa/\lambda}).$$

Since the isotropy group of each point in T is trivial

$$\chi_\lambda^\ell(\beta)\ \prod\nolimits_{\mu_\kappa \in T}\ \mu_\kappa(\beta) = \chi_\lambda(\beta)\ \prod\nolimits_{\mu_\kappa \in T}\ \chi_{\kappa/\lambda}(\beta)\,\mu_\kappa(\beta)$$

and we may content ourselves with showing that

$$\chi_\lambda(\ell^\ell)\,\tau(\chi_\lambda^\ell)\ \prod\nolimits_{\mu_\kappa \in T}\ \tau(\mu_\kappa) = \tau(\chi_\lambda)\ \prod\nolimits_{\mu_\kappa \in T}\ \tau(\chi_{\kappa/\lambda}\ \mu_\kappa).$$

Of course $\chi_\lambda(\ell^\ell)$ is the value of χ_λ at the element of the prime field corresponding to ℓ^ℓ. Let μ be the quotient of the right side by the left. The characters of κ^* of order ℓ are the characters $\mu_\kappa^k,\ 0 \le k < \ell$, defined by

$$\alpha(\mu_\kappa^k, \mathfrak{P}) = k \cdot \frac{q^f - 1}{\ell}.$$

Since the order of q modulo ℓ is f, if $T = \{\mu_\kappa^k | k \in A\}$ every non-trivial character of order ℓ is representable as $\mu_\kappa^{\eta(q^i k)}$ with $0 \le i < f$ and $k \in A$. $\eta(q^i k)$ is the remainder of $q^i k$ upon division by ℓ. Thus as we already saw, T has $\frac{\ell-1}{f}$ elements. Lemma 7.1 again shows that μ and all its conjugates have absolute value 1 and that μ is invariant under all automorphisms of $\mathfrak{k}_{p(q^f-1)}$ over $\mathfrak{k}_{q^f-1}$.

Let $\alpha = \alpha(\chi_\lambda, \mathfrak{p})$ and let $\beta = \alpha(\chi_\lambda^\ell, \mathfrak{p})$. Then $\ell\alpha = \beta + \nu(q-1)$ with $\nu \ge 0$. If $0 \le k < \ell$ let

$$\alpha(\mu_\kappa^k, \mathfrak{P}) = k \cdot \frac{q^f - 1}{\ell} = \sum\nolimits_{j=0}^{f-1} \gamma_j^k\ q^j$$

with $0 \le \gamma_j^k \le q-1$. In particular, γ_0^k is the residue of $k \cdot \frac{q^f-1}{\ell}$ modulo q. Moreover if $k_1 \equiv q^i k$ (modulo ℓ) then

$$\alpha(\mu_\kappa^k, \mathfrak{P}) = \sum\nolimits_{j=0}^{f-1} \gamma_{j+i}^{k_1}\ q^j.$$

It is understood that if $j + i \ge \ell$ then $\gamma_{j+i}^{k_1} = \gamma_{j+i-\ell}^{k_1}$. Thus if $\varphi(x)$ is the remainder of x upon division by q,

$$\{\gamma_j^k \,|\, k \in A,\ 0 \le j < f\} = \left\{\varphi\left(k \cdot \frac{q^f - 1}{\ell}\right)\,|\, 0 < k < \ell\right\}.$$

Certainly

$$\alpha(\chi_{\kappa/\lambda}\ \mu_\kappa^k, \mathfrak{P}) \equiv \frac{q^f - 1}{q - 1}\ \alpha + k \cdot \frac{q^f - 1}{\ell} \pmod{q^f - 1}.$$

Let $0 \le k' < \ell$ and let $\nu + k \equiv k' \pmod{\ell}$. Since, by definition, $\ell\alpha = \beta + \nu(q-1)$

$$\frac{q^f - 1}{q - 1}\ \alpha + k\ \frac{q^f - 1}{\ell} \equiv \frac{q^f - 1}{\ell} \cdot \frac{\beta}{q - 1} + k'\ \ \frac{q^f - 1}{\ell} \pmod{q^f - 1}.$$

Since $0 \le \beta < q-1$ the right side is non-negative and at most $q^f - 2$. Thus it is $\alpha(\chi_{\kappa/\lambda}\ \mu_\kappa^k, \mathfrak{P})$. Let

$$\alpha(\chi_{\kappa/\lambda}\ \mu_\kappa^k, \mathfrak{P}) = \sum\nolimits_{j=0}^{f-1}\ \delta_j^k\ q^j$$

with $0 \le \delta_j^k \le q-1$. Thus δ_0^k is the residue of

$$\frac{q^f-1}{\ell} \cdot \frac{\beta}{q-1} + k' \cdot \frac{q^f-1}{\ell}$$

modulo q. Since $\chi_{\kappa/\lambda}$ is invariant under automorphisms of κ/λ

$$\alpha(\chi_{\kappa/\lambda}\ \mu_\kappa^k, \mathfrak{P}) = \sum\nolimits_{j=0}^{f-1}\ \delta_{j+i}^{k_1}\ q^j$$

if $k_1 \equiv q^i k \pmod{\ell}$. Since the residue of $\frac{q^f-1}{q-1}\alpha$ modulo q is α,

$$\{\alpha\} \cup \{\delta_j^k \,|\, 0 \le j < \ell,\ k \in A\} = \left\{\varphi\left(\frac{q^f-1}{\ell} \cdot \frac{\beta}{q-1} + k\ \frac{q^f-1}{\ell}\right) \,|\, 0 \le k < \ell\right\}.$$

Since $\chi_\lambda(\ell^\ell) \equiv \ell^{\alpha\ell} \pmod{^*\mathfrak{P}}$ the number μ is multiplicatively congruent modulo $\mathfrak{P}$ to the quotient of

$$\frac{\varpi^\alpha \varpi^\varepsilon}{\alpha!\ \prod_{k\in A}\prod_{j=0}^{\ell-1}\delta_j^k!}, \quad \varepsilon = \sum\nolimits_{k\in A}\ \sum\nolimits_{j=0}^{f-1}\delta_j^k$$

by

$$\frac{\ell^\beta\ \varpi^\beta\ \varpi^{\varepsilon'}}{\beta!\ \prod_{k\in A}\ \prod_{j=0}^{\ell-1}\gamma_j^k!}, \quad \varepsilon' = \sum\nolimits_{k\in A}\ \sum\nolimits_{j-0}^{f-1}\gamma_j^k.$$

Since

$$\sum\nolimits_{j=0}^{f-1}\ \left(\alpha + \gamma_j^k\right)\ q^j \equiv \sum\nolimits_{j=0}^{f-1}\ \delta_j^k\ q^j,$$

we conclude from Lemma 7.4 that

$$f\alpha + \sum\nolimits_{j=0}^{f-1}\ \left(\gamma_j^k - \delta_j^k\right) = \rho(q-1),$$

if ρ is the number of $i,\ 0 \le i < f$, such that

$$\frac{q^f-1}{q-1}\alpha + \alpha\left(\mu_\kappa^{\eta(q^ik)}, \mathfrak{P}\right) \ge q^f.$$

Since

$$\frac{q^f-1}{q-1}\cdot\alpha + \alpha(\mu_\kappa^0, \mathfrak{P}) = \frac{q^f-1}{q-1}\alpha,$$

the number

$$(\ell-1)\alpha + \sum\nolimits_{k\in A}\sum\nolimits_{j=0}^{f-1}\ \left(\gamma_j^k - \delta_j^k\right)$$

is $(q-1)$ times the number of $k,\ 0 \le k < \ell$, such that

$$\frac{q^f-1}{q-1}\alpha + k\cdot\frac{q^f-1}{\ell} = \frac{q^f-1}{q-1}\ \frac{\beta}{\ell} + (k+\nu)\ \frac{q^f-1}{\ell} \ge q^f.$$

The number of such k is ν because $\nu < \ell$ and

$$\frac{q^f-1}{q-1}\ \frac{\beta}{\ell} + (\ell-\nu+\nu)\ \frac{q^f-1}{\ell} \ge 1 + q^f - 1 = q^f$$

while

$$\frac{q^f-1}{q-1}\ \frac{\beta}{\ell} + (\ell-1)\ \frac{q^f-1}{\ell} < \frac{q^f-1}{\ell} + (\ell-1)\ \frac{q^f-1}{\ell} = q^f-1.$$

Thus

$$\sum\nolimits_{k\in A}\sum\nolimits_{j=0}^{f-1}\ (\gamma_j^k - \delta_j^k) = \nu(q-1) - (\ell-1)\alpha = \alpha - \beta.$$

If $\ell m \equiv 1 \pmod q$

$$\varphi\left(k\cdot\frac{q^f-1}{\ell}\right) = \varphi(-km)$$

and

$$\varphi\left(\frac{q^f-1}{\ell}\cdot\frac{\beta}{q-1} + k\ \frac{q^f-1}{\ell}\right) = \varphi((\beta-k)m).$$

It follows immediately from Lemma 7.5 that

$$\ell^\beta\ \alpha!\ \prod\nolimits_{k\in A}\ \prod\nolimits_{j=0}^{f-1}\ \delta_j^k! \equiv \beta!\ \prod\nolimits_{k\in A}\ \prod\nolimits_{j=0}^{f-1}\ \gamma_j^k!$$

Thus $\mu = 1$ if q is odd and $\mu = \pm 1$ if q is even. If $\chi_\lambda = 1$ the number μ is clearly 1. This time too, one can apply part (f) of Lemma 7.1 and induction on the number of primes dividing the order of χ_λ to show that $\mu = 1$ if q is even.

Lemma 7.9

Let λ be a finite field with q elements and let κ be a finite extension of λ with $[\kappa:\lambda] = \ell$ where ℓ is a prime dividing $q-1$. Suppose χ_λ is a character of λ^* whose restriction to the ℓth roots of unity is not trivial and χ_κ is a character of κ^* such that $\chi_\kappa^\ell = \chi_{\kappa/\lambda}$. If T is the set of non-trivial characters of λ^* of order ℓ

$$\chi_\lambda(\ell)\tau(\chi_\lambda,\psi_\lambda)\ \prod\nolimits_{\mu_\lambda\in T}\ \tau(\mu_\lambda,\psi_\lambda) = \tau(\chi_\kappa,\psi_{\kappa/\lambda}).$$

If $\sigma \in \mathfrak{G}(\kappa/\lambda)$ define χ_κ^σ by $\chi_\kappa^\sigma(\alpha) = \chi_\kappa(\alpha^{\sigma^{-1}})$. Since $\chi_{\kappa/\lambda}^\sigma = \chi_{\kappa/\lambda},\ \chi_\kappa^{\sigma\ell} = \chi_{\kappa/\lambda}$ and $\chi_\kappa^{\sigma-1}$ is a character of order ℓ. If $\chi_\kappa^{\sigma-1} = 1$ for some $\sigma \ne 1$ then it is 1 for all σ and $\chi_\kappa(\alpha) = 1$ if α is a $(q-1)$th power, that is, if $N_{\kappa/\lambda}(\alpha) = 1$. Consequently there is a character ν_λ of λ^* such that $\chi_\kappa = \nu_{\kappa/\lambda}$. Then $\nu_\lambda^\ell = \chi_\lambda$ and χ_λ is trivial on the ℓth roots of unity, contrary to assumption. Thus

$$\{\chi_\kappa^{\sigma-1}\,|\,\sigma \ne 1\} = \{\mu_{\kappa/\lambda}\,|\,\mu_\lambda \in T\}.$$

If $\beta \in \lambda^*$ and $\beta = N_{\kappa/\lambda}(\gamma)$ then

$$\chi_\kappa(\beta) = \prod_\sigma \chi_\kappa(\gamma^{\sigma-1}) = \chi_\kappa(\gamma^\ell) \prod_{\sigma\neq 1} \chi_\kappa^{\sigma-1}(\gamma) = \chi_\lambda(\beta) \prod_{\sigma\neq 1} \mu_\lambda(\beta),$$

because $\mu_\lambda(\beta) = \mu_{\kappa/\lambda}(\gamma)$, and it will be enough to show that

$$\chi_\lambda(\ell)\ \tau(\chi_\lambda) \prod_{\mu_\lambda \in T} \tau(\mu_\lambda) = \tau(\chi_\kappa).$$

Let μ be the quotient of the left side by the right. Thus μ is a number in $\mathfrak{K}_{p(q-1)}$ and the only primes appearing in the factorization of μ are divisors of p. Since $\chi_{\kappa/\lambda}$ is not identically 1 neither is χ_κ. Thus the absolute value of μ and all its conjugates is 1. Let $\alpha = \alpha(\chi_\lambda, \mathfrak{p})$ and let $\beta = \alpha(\chi_\kappa, \mathfrak{P})$ where $\mathfrak{P}$ divides $\mathfrak{p}$. Then

$$\ell\beta \equiv \alpha \frac{q^\ell - 1}{q-1} \pmod{q^\ell - 1}.$$

Since ℓ divides $\frac{q^\ell-1}{q-1}$ we can write

$$\beta = \frac{q^\ell - 1}{q-1} \cdot \frac{\alpha}{\ell} - j \cdot \frac{q^\ell - 1}{\ell}.$$

Since the restriction of χ_λ to the ℓth roots of unity is not trivial, $\alpha \cdot \frac{q-1}{\ell} \not\equiv 0 \pmod{(q-1)}$. Thus ℓ does not divide α. For all $i \geq 0$

$$\tau\left(\chi_\kappa^{q^i}\right) = \tau(\chi_\kappa).$$

Moreover

$$\begin{aligned}\alpha\left(\chi_\kappa^{q^i}, \mathfrak{P}\right) &\equiv \frac{\alpha^\ell - 1}{q-1}\ \frac{\alpha}{\ell} - j\ \frac{\alpha^\ell - 1}{\ell} + (q^i - 1)\ \frac{q^\ell - 1}{q-1}\ \frac{\alpha}{\ell} - j(q^i - 1)\ \frac{q^\ell - 1}{\ell} \\ &\equiv \frac{q^\ell - 1}{q-1}\ \frac{\alpha}{\ell} + \left\{\frac{q^i - 1}{q-1}\ \alpha - j\right\}\ \frac{q^\ell - 1}{\ell}.\end{aligned}$$

Since $\frac{q^i-1}{q-1} \equiv i \pmod{\ell}$ we choose i so that $i\alpha \equiv j \pmod{\ell}$; then

$$\alpha(\chi_\kappa^{q^i}, \mathfrak{P}) \equiv \frac{q^\ell - 1}{q-1}\ \frac{\alpha}{\ell} \pmod{q^\ell - 1}.$$

Both sides of this congruence are non-negative and less than $q^\ell - 1$. Thus it is an equality and we can assume that $\beta = \frac{q^\ell-1}{q-1} \cdot \frac{\alpha}{\ell}$. The set T consists of the characters $\mu_\lambda^j,\ 1 \leq j \leq \ell - 1$, defined by

$$\alpha(\mu_\lambda^j, \mathfrak{P}) = \frac{j}{\ell}\ (q-1).$$

Under the automorphism $z \longrightarrow z^m$ of $k_{p(q^\ell-1)}$ over $k_{q^\ell-1}$ the number μ is multiplied by $\chi_\kappa^{-1}(m)\ \chi_\lambda(m) \prod_{\mu_\lambda\in T} \mu_\lambda(m)$ which is 1 because m belongs to λ. Let

$$\beta = \gamma_0 + \gamma_1 q + \ldots + \gamma_{\ell-1}\, q^{\ell-1}$$

with $0 \le \gamma_i \le q-1$. Then

$$\tau(\chi_\kappa) \equiv \frac{\varpi^\varepsilon}{\prod_{j=0}^{\ell-1} \gamma_j!} \pmod{^*\mathfrak{P}}, \quad \varepsilon = \sum_{j=0}^{\ell-1} \gamma_j,$$

and

$$\chi_\lambda(\ell)\tau(\chi_\lambda) \prod_{j=1}^{\ell-1} \tau(\mu_\lambda^j) \equiv \frac{\ell^\alpha \varpi^{\varepsilon'}}{\alpha! \prod_{j=1}^{\ell-1} \left(j \cdot \frac{q-1}{\ell}\right)!} \pmod{^*\mathfrak{P}}, \quad \varepsilon' = \alpha + \sum_{j=0}^{\ell-1} j \cdot \frac{q-1}{\ell}.$$

Lemma 7.6 implies immediately that $\mu \equiv 1 \pmod{^*\mathfrak{P}}$. Thus $\mu = 1$ if q is odd and $\mu = \pm 1$ if q is even. If ℓ' is a prime divisor of $q-1$ different from ℓ, we write χ_λ as $\chi'_\lambda \chi''_\lambda$ where the order of χ'_λ is a power of ℓ' and the order of χ''_λ is prime to ℓ. In a similar fashion we write χ_κ as $\chi'_\kappa \chi''_\kappa$. The pair χ''_λ and χ''_κ also satisfy the conditions of the lemma. The final assertion of Lemma 7.1 shows that, if μ'' is defined in the same way as $\mu, \mu = \mu''$. Arguing by induction we see that it is enough to verify that $\mu = 1$ when the order of χ_λ is a power of ℓ. Applying the last part of Lemma 7.1, again we see that there is a prime $\mathfrak{q}$ dividing ℓ such that

$$\tau(\chi_\lambda) \equiv \tau(\chi_\kappa) \equiv \tau(\mu_\lambda^j) \equiv 1 \pmod{\mathfrak{q}}.$$

Since $\chi_\lambda(\ell)$ is an ℓ^ωth root of unity for some ω,

$$\chi_\lambda(\ell) \equiv 1 \pmod{\mathfrak{q}}.$$

Thus $\mu \equiv 1 \pmod{\ell}$ and $\mu = 1$.

Chapter Eight.

A Lemma of Lamprecht

Let F be a non-archimedean local field and let ψ_F be a non-trivial character of F. $n = n(\psi_F)$ is the largest integer such that ψ_F is trivial on $\mathfrak{P}_F^{-n}$. If χ_F is a quasi-character of C_F, $m = m(\chi_F)$ is the smallest non-negative integer such that χ_F is trivial on U_F^m. If γ in C_F is such that $\gamma O_F = \mathfrak{P}_F^{m+n}$ set

$$\Delta_1(\chi_F, \psi_F; \gamma) = \frac{\int_{U_F} \psi_F\left(\frac{\alpha}{\gamma}\right) \chi_F^{-1}(\alpha) d\alpha}{|\int_{U_F} \psi_F\left(\frac{\alpha}{\gamma}\right) \chi_F^{-1}(\alpha) d\alpha|}.$$

Then

$$\Delta(\chi_F, \psi_F) = \chi_F(\gamma)\Delta_1(\chi_F, \psi_F, \gamma).$$

As suggested by Hasse [8], we shall, in the proofs, of the main lemmas, make extensive use of the following lemma which is central to the paper [10] of Lamprecht.

Lemma 8.1

(a) *If $m = m(\chi_F) = 2d$ with d integral and positive there is a unit β in O_F such that*

$$\psi_F\left(\frac{\beta x}{\gamma}\right) = \chi_F(1 + x)$$

for all x in $\mathfrak{P}_F^d$. For any such β

$$\Delta_1(\chi_F, \psi_F; \gamma) = \psi_F\left(\frac{\beta}{\gamma}\right) \chi_F^{-1}(\beta).$$

(b) *If $m = m(\chi_F) = 2d + 1$ with d integral and positive there is a unit β in O_F such that, for all x in $\mathfrak{P}_F^{d+1}$,*

$$\psi_F\left(\frac{\beta x}{\gamma}\right) = \chi_F(1 + x).$$

For any such β, $\Delta_1(\chi_F, \psi_F; \gamma)$ is equal to

$$\psi_F\left(\frac{\beta}{\gamma}\right) \chi_F^{-1}(\beta) \frac{\int_{O_F/\mathcal{P}_F} \psi_F\left(\frac{\delta\beta x}{\gamma}\right) \chi_F^{-1}(1 + \delta x) dx}{|\int_{O_F/\mathcal{P}_F} \psi_F\left(\frac{\delta\beta x}{\gamma}\right) \chi_F^{-1}(1 + \delta x) dx|}$$

if $\delta O_F = \mathfrak{P}_F^d$.

Let $m = 2d + \varepsilon$ with $\varepsilon = 0$ in case (a) and $\varepsilon = 1$ in case (b). The function $\psi_F\left(\frac{xy}{\gamma}\right)$, $x \in O_F$, $y \in \mathfrak{P}_F^{d+\varepsilon}$ can be regarded as a function on

$$O_F/\mathfrak{P}_F^d \times \mathfrak{P}_F^{d+\varepsilon}/\mathfrak{P}_F^m.$$

For fixed x it is a character of $\mathfrak{P}_F^{d+\varepsilon}/\mathfrak{P}_F^m$ which is trivial if and only if $x \in \mathfrak{P}_F^d$ and for fixed y it is a character of $O_F/\mathfrak{P}_F^d$ which is trivial if and only if $y \in \mathfrak{P}_F^m$. Thus it defines a duality of $O_F/\mathfrak{P}_F^d$ and $\mathfrak{P}_F^{d+\varepsilon}/\mathfrak{P}_F^m$. The existence of a β such that

$$\chi_F(1+x) = \psi_F\left(\frac{\beta x}{\gamma}\right)$$

for x in $\mathfrak{P}_F^{d+\varepsilon}$ follows immediately from the relation

$$\chi_F(1+x)\,\chi_F(1+y) = \chi_F(1+x+y)$$

which is valid for x in $\mathfrak{P}_F^{d+\varepsilon}$. The number β must be a unit because $\chi_F(1+x)$ is different from 1 for some x in $\mathfrak{P}_F^{m-1}$.

In case (a)

$$\int_{U_F} \psi_F\left(\frac{\alpha}{\gamma}\right)\chi_F^{-1}(\alpha)d\alpha$$

is equal to

$$\int_{U_F/U_F^d} \psi_F\left(\frac{\alpha}{\gamma}\right)\chi_F^{-1}(\alpha)\left\{\int_{\mathfrak{P}_F^d} \psi_F\left(\frac{(\alpha-\beta)x}{\gamma}\right)dx\right\}d\alpha.$$

The main integral is 1 or 0 according as $\alpha-\beta$ does or does not lie in $\mathfrak{P}_F^d$. Thus this expression is equal to

$$\psi_F\left(\frac{\beta}{\gamma}\right)\chi_F^{-1}(\beta)\;[U_F:U_F^d]^{-1}.$$

The first part of the lemma follows.

In case (b)

$$\int_{U_F} \psi_F\left(\frac{\alpha}{\gamma}\right)\chi_F^{-1}(\alpha)d\alpha$$

is equal to

$$\int_{U_F/U_F^{d+1}} \psi_F\left(\frac{\alpha}{\gamma}\right)\chi_F^{-1}(\alpha)\;\left\{\int_{\mathfrak{P}_F^{d+1}} \psi_F\left(\frac{(\alpha-\beta)x}{\gamma}\right)dx\right\}d\alpha.$$

The inner integral is 0 unless $\alpha-\beta$ lies in $\mathcal{P}_F^d$ when it is 1. Thus this expression is equal to

$$\psi_F\left(\frac{\beta}{\gamma}\right)\chi_F^{-1}(\beta)\;[U_F:U_F^d]^{-1}\int_{O_F/\mathfrak{P}_F} \psi_F\left(\frac{\delta\beta x}{\gamma}\right)\chi_F^{-1}(1+\delta x)dx.$$

The second part of the lemma follows.

The number β is only determined modulo $\mathfrak{P}_F^d$. When applying the lemma we shall, after choosing β, set

$$\Delta_2(\chi_F,\psi_F;\gamma) = \psi_F\left(\frac{\beta}{\gamma}\right)\chi_F^{-1}(\beta)$$

and then define $\Delta_3(\chi_F,\psi_F;\gamma)$, which will be 1 when m is even, by the equation,

$$\Delta_1(\chi_F,\psi_F;\gamma) = \Delta_2(\chi_F,\psi_F;\gamma)\,\Delta_3(\chi_F,\psi_F;\gamma).$$

When we need to make the relation between β and χ_F explicit we write β as $\beta(\chi_F)$. To be of any use to us this lemma must be supplemented by some other observations.

If K is a finite Galois extension of F any quasi-character χ_F of C_F determines a one-dimensional representation of $W_{K/F}$ whose restriction to C_K is a quasi-character $\chi_{K/F}$ of C_K. The character $\chi_{K/F}$ may be defined directly by

$$\chi_{K/F}(\alpha) = \chi_F(N_{K/F}\alpha).$$

More generally, if E is any finite separable extension of F we define $\chi_{E/F}$ by

$$\chi_{E/F}(\alpha) = \chi_F(N_{E/F}\alpha).$$

To apply the lemma of Lamprecht we shall need to know, in some special cases, the relation between $\beta(\chi_F)$ and $\beta(\chi_{E/F})$.

Suppose m is a positive integer and $m = 2d + \varepsilon$ where ε is 0 or 1 and d is a positive integer. Let $m' = \psi_{E/F}(m-1) + 1$ and let $m' = 2d' + \varepsilon'$ where ε' is 0 or 1 and d' is a positive integer.* Since $\psi_{E/F}$ is convex

$$\psi_{E/F}\left(\frac{m-1}{2}\right) \le \frac{1}{2}\,\psi_{E/F}(m-1) + \frac{1}{2}\,\psi_{E/F}(0) = \frac{1}{2}\,(m'-1) < d' + \varepsilon'$$

and

$$d' + \varepsilon' = \psi_{E/F}(u)$$

with $u > \frac{m-1}{2}$. Since the least integer greater than $\frac{m-1}{2}$ is $d + \varepsilon$, Lemma 6.6 implies that

$$N_{E/F}\left(U_E^{d'+\varepsilon'}\right) \le U_F^u \le U_F^{d+\varepsilon}.$$

In other words, if $x \in \mathfrak{P}_E^{d'+\varepsilon'}$ then

$$N_{E/F}(1+x) - 1 \in \mathfrak{P}_F^{d+\varepsilon}.$$

Lemma 6.6 also implies that

$$N_{E/F}(1+x) - 1 \in \mathfrak{P}_F^m$$

if $x \in \mathfrak{P}_E^{m'}$. If $x \in \mathfrak{P}_E^{d'+\varepsilon'}$ and $y \in \mathfrak{P}_E^{m'}$ then

$$N_{E/F}(1+x+y) - 1 = N_{E/F}(1+x)N_{E/F}\left(1 + \frac{y}{1+x}\right) - 1$$

is congruent to

$$N_{E/F}(1+x) - 1$$

modulo $\mathfrak{P}_F^m$. Thus if $x \in \mathfrak{P}_E^{d'+\varepsilon'}$ and $y \in \mathfrak{P}_E^{d'+\varepsilon"}$ so that $xy \in \mathfrak{P}_E^{m'}$, then

$$N_{E/F}(1+x+y) - 1 \equiv N_{E/F}(1+x+y+xy) - 1 \pmod{\mathfrak{P}_\mathrm{F}^\mathrm{m}}.$$

The right side is

$$N_{E/F}(1+x)N_{E/F}(1+y) - 1,$$

* We are here dealing not with an additive character, but with the function of Chapter 6!

which equals

$$\{N_{E/F}(1+x)-1\}+\{N_{E/F}(1+y)-1\}+\{(N_{E/F}(1+x)-1)\,(N_{E/F}(1+y)-1)\}$$

and this is congruent to

$$\{N_{E/F}(1+x)-1\}+\{N_{E/F}(1+y)-1\}$$

modulo $\mathfrak{P}_F^m$. Thus the map

$$P_{E/F}: x \longrightarrow N_{E/F}(1+x)-1$$

is a homomorphism from $\mathfrak{P}_E^{d'+\varepsilon'}/\mathfrak{P}_E^{m'}$ to $\mathfrak{P}_F^{d+\varepsilon}/\mathfrak{P}_F^{m}$. If $E\subseteq E'$ we can replace F by E, E by E', m by m', and m' by $\psi_{E'/E}(m'-1)+1$, and define $P_{E'/E}$. Since $\psi_{E'/F}=\psi_{E'/E}\circ\psi_{E/F}$ and

$$N_{E'/F}(1+x)-1=N_{E/F}(1+(N_{E'/E}(1+x)-1))-1,$$

the relation

$$P_{E'/F}=P_{E/F}\circ P_{E'/E}$$

is valid.

If $n=n(\psi_F)$ and $n'=n(\psi_{E/F})$, choose γ_F in C_F so that $\gamma_F O_F=\mathfrak{P}_F^{m+n}$ and γ_E in C_E so that $\gamma_E O_E=\mathfrak{P}_E^{m'+n'}$. I apologize again for the unfortunate conflict of notation. $\psi_{E/F}$ is on the one hand a function on $\{u\in\mathbb{R}\,|\,u\geq -1\}$ and on the other a character of E. However, warned one again, the reader should not be too inconvenienced by the conflict. Define

$$P^*_{E/F}: O_F/\mathfrak{P}_F^d \longrightarrow O_E/\mathfrak{P}_E^{d'}$$

by the relation

$$\psi_F\left(\frac{x\,P_{E/F}(y)}{\gamma_F}\right)=\psi_{E/F}\left(\frac{P^*_{E/F}(x)y}{\gamma_E}\right).$$

It will often be necessary to keep in mind the dependence of $P^*_{E/F}$ on γ_F and γ_E. Then we shall write

$$P^*_{E/F}(x)=P^*_{E/F}(x;\gamma_E,\gamma_F).$$

It is clear that

$$P^*_{E'/F}(x;\gamma_{E'},\gamma_F)=P^*_{E'/E}(P^*_{E/F}(x;\gamma_E,\gamma_F);\gamma_{E'},\gamma_E).$$

Lemma 8.2

Let K/F be abelian and let $G=\mathfrak{G}(K/F)$. Suppose there is an integer t such that $G=G_t$ while $G_{t+1}=\{1\}$. Suppose $m\geq t+1$ and $m>1$ and γ_F is chosen. If μ_F belongs to $S(K/F)$, the set of characters of $C_F/N_{K/F}C_K$, then $m\geq m(\mu_F)$ so that for some $\alpha(\mu_F)$ in O_F

$$\mu_F(1+x)=\psi_F\left(\frac{\alpha(\mu_F)x}{\gamma_F}\right)$$

for all x in $\mathfrak{P}_F^{d+\varepsilon}$. The element γ_K may be taken equal to γ_F and if $P^*_{K/F}(\beta)=P^*_{K/F}(\beta;\gamma_F,\gamma_F)$ then

$$N_{K/F}(P^*_{K/F}(\beta))\equiv\prod\nolimits_{\mu_F}(\beta+\alpha(\mu_F))\ (\mathrm{mod}\,\mathfrak{P}_{\mathrm{F}}^{\mathrm{d}})$$

for all β in O_F.

If $t=-1$ then $n(\psi_F)=n(\psi_{K/F})$ and $m'=m$ so that γ_K may be taken equal to γ_F. If $t\geq 0$ the extension is ramified. Let $\mathfrak{P}_K^{\delta_{K/F}}$ be the different of K/F. Then

$$n(\psi_{K/F})=[K:F]n(\psi_F)+\delta_{K/F}.$$

By definition
$$\psi_{K/F}(m-1)=t+[K:F](m-t-1).$$
By Proposition 4 of paragraph IV.2 of Serre's book $\delta_{K/F}=([K:F]-1)(t+1)$. Thus

$$m^*+n(\psi_{K/F})=[K:F]\,(m+n(\psi_F))$$

and we can again take $\gamma_K=\gamma_F$.

Since $m(\mu_F)=t+1$ we have $m\geq m(\mu_F)$ and

$$\mu_F(1+x+y)=\mu_F(1+x)\,\mu_F(1+y)$$

for x and y in $\mathfrak{P}_F^{d+\varepsilon}$. Thus the existence of $\alpha(\mu_F)$ is assured. The last assertion of the lemma will be proved by induction. We will need to know that if $x\equiv y(\operatorname{mod}\mathfrak{P}_{\mathrm{K}}^{\mathrm{d}'})$ then

$$N_{K/F}x\equiv N_{K/F}y(\operatorname{mod}\mathfrak{P}_{\mathrm{F}}^{\mathrm{d}}).$$

When proving this we may suppose that $xO_K=\mathfrak{P}_K^r$ with $r\leq d'$ and that $\frac{y}{x}$ belongs to O_K. Then

$$N_{K/F}x-N_{K/F}y=N_{K/F}x\left\{1-N_{K/F}\left(1+\frac{y-x}{x}\right)\right\}.$$

If $r\geq d$ there is nothing to prove. Suppose $r\leq d$. If $d'-r=\psi_{K/F}(u)$ and s is the smallest integer greater than or equal to u the right side belongs to $\mathfrak{P}_F^{s+r}$. Since the derivative of $\psi_{K/F}$ is at least one everywhere $\psi_{K/F}(u+r)\geq d'$. But

$$d'\geq\frac{m'-1}{2}=\frac{1}{2}\,\psi_{K/F}(m-1)+\frac{1}{2}\,\psi_{K/F}(0)\geq\psi_{K/F}\left(\frac{m-1}{2}\right).$$

Thus $u+r\geq\frac{m-1}{2}$ and $s+r\geq d$.

Suppose $F\subseteq L\subseteq K$ and L/F is cyclic of prime order. Let $H=\mathfrak{G}(K/L)$ and let $\overline{G}=\mathfrak{G}(L/F)$. Certainly $H=H_t$ while $H_{t+1}=\{1\}$. Since $\psi_{K/F}(t)=\psi_{K/L}(t)=t$, we have $\psi_{L/F}(t)=t$ and, by Herbrand's theorem,
$$\overline{G}_t=\overline{G}^t=HG^t/H=G/H=\overline{G}.$$
Moreover $t+1=\psi_{L/F}(t+\delta)$ with $\delta>0$ so that

$$\overline{G}_{t+1}=\overline{G}^{t+\delta}=HG^{t+\delta}/H=H/H=\{1\}.$$

Finally, $\psi_{L/F}(m-1)+1\geq t+1$ so that L/F and K/L, with m replaced by $\psi_{L/F}(m-1)+1$, satisfy the conditions of the lemma. $S(L/F)$ is a subgroup of $S(K/F)$. If μ_F and ν_F belong to $S(K/F)$ then

$\mu_{L/F} = \nu_{L/F}$ if and only if μ_F and ν_F belong to the same coset of $S(L/F)$. Take S to be a set of representatives for these cosets; then

$$S(K/L) = \{\mu_{L/F} \,|\, \mu_F \,|\, \mu_F \in S\}.$$

We take $\alpha(\mu_F\nu_F) = \alpha(\mu_F) + \alpha(\nu_F)$ if μ_F belongs to S and ν_F belongs to $S(L/F)$. If μ_F belongs to S we take $\alpha(\mu_{L/F})$ to be $P^*_{L/F}(\alpha(\mu_F))$. If the lemma is valid for K/L and L/F then

$$N_{K/F}(P^*_{K/F}(\beta)) = N_{L/F}(N_{K/L}(P^*_{K/L}(P^*_{L/F}(\beta)))$$

which is congruent modulo $\mathcal{P}_F^d$ to

$$N_{L/F}\left(\prod\nolimits_{\mu_F \in S} (P^*_{L/F}(\beta) + P^*_{L/F}(\alpha(\mu_F)))\right)$$

or

$$\prod\nolimits_{\mu_F \in S} \{N_{L/F}(P^*_{L/F}(\beta + \alpha(\mu_F)))\}.$$

This is congruent modulo $\mathcal{P}_F^d$ to

$$\prod\nolimits_{\mu_F \in S} \prod\nolimits_{\nu_F \in S(L/F)} \{\beta + \alpha(\mu_F) + \alpha(\nu_F)\}$$

which equals

$$\prod\nolimits_{\mu_F \in S(K/F)} \{\beta + \alpha(\mu_F)\}.$$

Thus it is enough to prove the lemma when K/F is cyclic of prime order. In this case more precise information is needed and the assertion of the lemma will follow immediately from it.

Lemma 8.3

If K/F is unramified and $m \geq 1$ we may take $P^*_{K/F}(\beta) = \beta$.

According to paragraph V.2 of Serre's book

$$N_{K/F}(1+y) - 1 \equiv S_{K/F}(y) \,(\mathrm{mod}\, \mathcal{P}_{\mathrm{F}}^{\mathrm{m}})$$

if $y \in \mathfrak{P}_K^{d'+\varepsilon'}$. Thus $P_{K/F}(y) = S_{K/F}(y)$ and

$$\psi_F\left(\frac{x\,P_{K/F}y}{\gamma_F}\right) = \psi_{K/F}\left(\frac{xy}{\gamma_F}\right).$$

Lemma 8.4

Suppose K/F is abelian, totally ramified, and $[K:F] = \ell$ is an odd prime. If $d \geq t+1$ we may take $P^*_{K/L}(\beta) = \beta$.

The relation

$$m' = t + 1 + \ell(m - 1 - t) = \ell m - (t+1)(\ell - 1)$$

implies that $m' \equiv m \,(\mathrm{mod}\,2),\ \varepsilon' = \varepsilon$, and

$$d' = \ell d + \frac{\ell-1}{2}(\varepsilon - t - 1) = d + \frac{\ell-1}{2}(m-t-1).$$

Since

$$\frac{\ell-1}{2}(m-t-1) \geq m-t-1 \geq d+\varepsilon$$

we have

$$d' + \varepsilon' \geq 2(d+\varepsilon) \geq m.$$

Moreover

$$\frac{2(d'+\varepsilon') + \delta_{K/F}}{\ell} \geq \frac{m' + \delta_{K/F}}{\ell} = m$$

so that by Lemma 5 of paragraph V.3 of Serre's book

$$N_{K/F}(1+x) - 1 \equiv S_{K/F}(x) \ (\mathrm{mod}\,\mathfrak{P}_{\mathrm{F}}^{\mathrm{m}})$$

if $x \in \mathfrak{P}_K^{d'+\varepsilon'}$. The lemma follows.

Let p be the characteristic of $O_F/\mathfrak{P}_F$.

Lemma 8.5

Suppose K/F is abelian, totally ramified, and $[K:F] = \ell$ is an odd prime. Suppose $t+1 \leq m \leq 2t+1$. Choose a non-trivial character μ_F in $S(K/F)$. We may choose $\alpha = \alpha(\mu_F)$ so that $\alpha O_F = \mathfrak{P}_F^v$, if $m = t+1+v$, so that $\alpha = N_{K/F}\alpha_1$ for some α_1 in O_K, and so that

$$\mu_F(1+x) = \psi_F\left(\frac{\alpha x}{\gamma_F}\right)$$

for x in $\mathfrak{P}_F^s$. Here s is the least integer greater than or equal to $\frac{t}{2}$. If ζ is a $(p-1)$th root of unity in F there is a unique integer j with $1 \leq j \leq p-1$ such that $\zeta - j$ lies in $\mathfrak{P}_F$. Set $\mu_F^\zeta = \mu_F^j$. We may take $\alpha(\mu_F^\zeta)$ to be $\zeta\alpha$. If β belongs to O_F we can find a β_1 in O_K such that $\beta \equiv N_{K/F}\beta_1 (\mathrm{mod}\,\mathfrak{P}_{\mathrm{F}}^{\mathrm{d}})$. Then

$$P^*_{K/F}(\beta) \equiv \beta - \beta_1\ \frac{\alpha}{\alpha_1}\ (\mathrm{mod}\,\mathfrak{P}_{\mathrm{K}}^{\mathrm{d}'}).$$

If

$$\mu_F(1+x) = \psi_F\ \left(\frac{\alpha x}{\gamma_F}\right)$$

for x in $\mathfrak{P}_F^s$ then, necessarily, $\alpha O_F = \mathfrak{P}_F^v$. Choose δ_1 in O_K such that $\delta_1 O_K = \mathfrak{P}_K^v$ and set $\delta = N_{K/F}\delta_1$. Set $\alpha = \omega\delta$ where ω is yet to be chosen. We must have

$$\mu_F(1+x) = \psi_F\ \left(\frac{\omega\delta x}{\gamma_F}\right)$$

if $x \in \mathfrak{P}_F^s$. This equation determines the unit w modulo $\mathfrak{P}_F^r$ if $r = t-s$. Since any unit is a norm modulo $\mathfrak{P}_F^t$ we may suppose $\omega = N_{K/F}\omega_1$. Take $\alpha_1 = \omega_2\delta_1$. β_1 exists for a similar reason.

The number $\zeta - j$ must lie in pO_F. But K/F is wildly ramified, because $2t+1 \geq m > 1$, $\ell = p$ and $p = S_{K/F}(1)$ so that, by paragraph V.3 of Serre's book, p belongs to $\mathfrak{P}_F^u$ if u is the greatest integer in

$$\frac{(\ell-1)}{\ell}\,(t+1) \geq \frac{t+1}{2}.$$

However $d+\varepsilon \geq s$ so that $d+\varepsilon+u \geq t+1$ and, if x belongs to $\mathfrak{P}_F^{d+\varepsilon}$, $(\zeta-j)x$ lies in $\mathfrak{P}_F^{t+1}$. Thus

$$\psi_F\left(\frac{\alpha(\zeta-j)x}{\gamma_F}\right) = \mu_F\left(1+(\zeta-j)x\right) = 1$$

and

$$\mu_F^j(1+x) = \mu_F^j(1+x) = \psi_F\,\left(\frac{j\alpha x}{\gamma_F}\right) = \psi_F\,\left(\frac{\zeta\alpha x}{\gamma_F}\right).$$

Since

$$\frac{2s+\delta_{K/F}}{\ell} \geq \frac{t+1+\delta_{K/F}}{\ell} = t+1.$$

The lemmas of paragraph V.3 of Serre's book imply that

$$N_{K/F}(1+x) \equiv 1 + S_{K/F}(x) + N_{K/F}(x)\,(\mathrm{mod}\,\mathfrak{P}_{\mathrm{F}}^{\mathrm{t}+1})$$

if x belongs to $\mathfrak{P}_K^s$ and then

$$1 = \mu_F(N_{K/F}(1+x)) = \mu_F(1+S_{K/F}(x)+N_{K/F}(x)).$$

As we observed $d+\varepsilon \geq s$. Moreover $d+\varepsilon \leq t+1$ so that

$$\frac{d+\varepsilon+\delta_{K/F}}{\ell} \geq d+\varepsilon$$

and $S_{K/F}(x)$ and $N_{K/F}(x)$ belong to $\mathfrak{P}_F^{d+\varepsilon}$ if x belongs to $\mathfrak{P}_K^{d+\varepsilon}$. Thus, for such x,

$$\psi_F\,\left(\frac{\alpha N_{K/F}(x)}{\gamma_F}\right) = \psi_F\,\left(\frac{-\alpha S_{K/F}(x)}{\gamma_F}\right).$$

Again

$$\frac{2(d'+\varepsilon')+\delta_{K/F}}{\ell} \geq m$$

so that

$$N_{K/F}(1+x) - 1 = S_{K/F}(x) + N_{K/F}(x)\ (\mathrm{mod}\,\mathfrak{P}_{\mathrm{F}}^{\mathrm{m}})$$

if $x \in \mathfrak{P}_K^{d'+\varepsilon'}$. Moreover

$$d'+\varepsilon' = d+\varepsilon+\frac{\ell-1}{2}\,(m-t-1) \geq d+\varepsilon$$

so that $N_{K/F}(x)$ and hence $S_{K/F}(x)$ belong to $\mathfrak{P}_F^{d+\varepsilon}$. Thus

$$\beta N_{K/F}x \equiv \alpha N_{K/F}\,\left(\frac{\beta_1 x}{\alpha_1}\right)\ (\mathrm{mod}\,\mathfrak{P}_{\mathrm{F}}^{\mathrm{m}}).$$

But $\beta_1 x/\alpha_1$ belongs to $\mathfrak{P}_K^{d'+\varepsilon'-v}$ and

$$d'+\varepsilon'-v = d+\varepsilon+\frac{\ell-1}{2}\,v-v \geq d+\varepsilon$$

so that

$$\psi_F\ \left(\frac{\beta\,P_{K/F}(x)}{\gamma_F}\right) = \psi_F\ \left(\frac{\beta\,S_{K/F}(x)+\beta\,N_{K/F}(x)}{\gamma_F}\right)$$

which equals

$$\psi_F\ \left(\frac{\beta\,S_{K/F}(x)-\alpha S_{K/F}\left(\frac{\beta_1 x}{\alpha_1}\right)}{\gamma_F}\right) = \psi_{K/F}\ \left(\left(\beta-\frac{\alpha\beta_1}{\alpha_1}\right)\ \frac{x}{\gamma_F}\right)$$

as required.

Lemma 8.6

Suppose K/F is a wildly ramified quadratic extension, $m \geq t+1$, and $m = t+1+v$. Let μ_F be the non-trivial character in $S(K/F)$. If β belongs to O_F there is a β_1 in O_K and a δ in U_F^t such that $\beta \equiv \delta N_{K/F}\beta_1 (\operatorname{mod}\mathfrak{P}_F^d)$. We can choose $\alpha = \alpha(\mu_F)$ so that

$$\mu_F(1+x) = \psi_F\ \left(\frac{\alpha\delta x}{\gamma_F}\right)$$

if x is in $\mathfrak{P}_F^s$ and so that $\alpha = N_{K/F}\alpha_1$ for some α_1 in O_K. Here s has the same meaning as before. Thus, if r is the integral part of $\frac{t+1}{2}$, $t+1 = r+s$. With these choices

$$P^*_{K/F}(\beta) \equiv \beta-\frac{\beta_1\alpha\delta}{\alpha_1}\ \left(\operatorname{mod}\mathcal{P}_{\mathrm{K}}^{\mathrm{d}'}\right).$$

If $\beta = 0$ the existence of δ and β_1 is clear. Otherwise we can find a β_1 such that $N_{K/F}\beta_1/\beta$ is in U_F^t. We choose δ accordingly. If $m = t+1+v$ and

$$\mu_F(1+x) = \psi_F\ \left(\frac{\alpha\delta x}{\gamma_F}\right)$$

for x in $\mathfrak{P}_F^s$ then $O_F\alpha = \mathfrak{P}_F^v$. Choose η_1 in O_K so that $O_K\eta_1 = \mathfrak{P}_K^v$ and set $\eta = N_{K/F}\eta_1$. Set $\alpha = \omega\eta$ where ω is yet to be chosen. We must have

$$\mu_F(1+x) = \psi_F\ \left(\frac{\omega\eta\delta x}{\gamma_F}\right)$$

if $x \in \mathfrak{P}_F^s$. This equation determines the unit ω modulo $\mathfrak{P}_F^r$. Since any unit is a norm modulo $\mathfrak{P}_F^t$ we may suppose $\omega = N_{K/F}\omega_1$. Take $\alpha_1 = \omega_1\eta_1$.

Since the extension is quadratic

$$N_{K/F}(1+x) = 1+S_{K/F}(x)+N_{K/F}(x).$$

Since

$$\frac{s+\delta_{K/F}}{2} = \frac{s+t+1}{2} \geq s$$

both $S_{K/F}(x)$ and $N_{K/F}(x)$ are in $\mathfrak{P}_F^s$ if x belongs to $\mathfrak{P}_K^s$ and

$$\psi_F\left(\frac{\alpha\delta N_{K/F}(x)}{\gamma_F}\right) = \psi_F\left(\frac{-\alpha\delta S_{K/F}(x)}{\gamma_F}\right).$$

We have $m' = 2m-(t+1)$ and $d' = m-s$, so that $d'+\varepsilon' = m-r$ and $d'+\varepsilon'-v = s$. Thus if x belongs to $\mathfrak{P}_K^{d'+\varepsilon'}$

$$\beta N_{K/F}(x) \equiv \alpha\delta N_{K/F}\left(\frac{\beta_1 x}{\alpha_1}\right) \qquad (\mathrm{mod}\, \mathfrak{P}_{\mathrm{F}}^{\mathrm{m}})$$

and $\beta_1 x/\alpha_1$ lies in $\mathfrak{P}_K^s$. Consequently

$$\psi_F\left(\frac{\beta\, P_{K/F} x}{\gamma_F}\right) = \psi_{K/F}\left(\left(\beta - \beta_1 \frac{\alpha\delta}{\alpha_1}\right)\frac{x}{\gamma_F}\right)$$

as required.

Lemma 8.7

If K/F is a tamely ramified quadratic extension and $m \geq 2$ we may take $P^*_{K/F}(\beta) = \beta$.

Notice that $t+1 = 1$ so that $m \geq t+1$. In this case $m' = 2m-1,\ d' = m-1$, and $d'+\varepsilon' = m$. If $x \in \mathfrak{P}_K^{d'+\varepsilon'}$

$$N_{K/F}(1+x) = 1 + S_{K/F}(x) + N_{K/F}(x)$$

is congruent to

$$1 + S_{K/F}(x)$$

modulo $\mathfrak{P}_F^m$. The lemma follows.

To complete the proof of Lemma 8.2 we have to show that if K/F is cyclic of prime order

$$N_{K/F}(P^*_{K/F}(\beta)) \equiv \prod\nolimits_{\mu_F \in S(K/F)} (\beta + \alpha(\mu_F)) \quad (\mathrm{mod}\, \mathfrak{P}_{\mathrm{F}}^{\mathrm{d}}).$$

We consider the cases discussed in the previous lemmas one by one. If the extension is unramified we may take all the numbers $\alpha(\mu_F)$ to be 0. The congruences then reduce to the identity $\beta^n = \beta^n$. The same is true if K/F is cyclic of odd order and $d \geq t+1$ or K/F is quadratic and $t = 0$. If K/F is cyclic of odd order ℓ and $t+1 \leq m \leq 2t+1$ the right side becomes

$$\beta^\ell - \beta\alpha^{\ell-1}.$$

If $\beta \equiv 0\, (\mathrm{mod}\, \mathfrak{P}_{\mathrm{F}}^{\mathrm{d}})$ both sides are congruent to 0 modulo $\mathfrak{P}_F^d$. Suppose β does not belong to $\mathfrak{P}_F^d$ and $\beta O_F = \mathfrak{P}_F^u$. Then $\beta_1 O_K = \mathfrak{P}_K^u$ and

$$N_{K/F}\left(\beta - \beta_1 \frac{\alpha}{\alpha_2}\right)$$

is congruent to

$$\beta^\ell - \beta\alpha^{\ell-1} + \sum\nolimits_{i=1}^{\ell-1} (-1)^i \beta^\ell E^i \left(\frac{\beta_1\alpha}{\beta\alpha_1}\right)$$

modulo $\mathfrak{P}_F^d$. If $x \in K$ then $E^i(x)$ is the ith elementary symmetric function of x and its conjugates. Moreover $\beta_1\alpha/\beta\alpha_1$ belongs to $\mathfrak{P}_K^{(\ell-1)\,(v-u)}$. If $\ell-1 \geq i \geq 1$

$$\frac{i(\ell-1)\,(v-u)+(\ell-1)\,(t+1)}{\ell} \geq \frac{(\ell-1)\,(v+t+1)}{\ell} - \ell u.$$

The right side is

$$\frac{(\ell-1)}{\ell}m - pu \geq d - \ell u.$$

The argument of paragraph V.3 of Serre's book shows that

$$N_{K/F}\left(\beta - \beta_1\,\frac{\alpha}{\alpha_1}\right) \equiv \beta^\ell - \beta\alpha^{\ell-1} \pmod{\mathfrak{P}_{\mathrm{F}}^{\mathrm{d}}}.$$

For a wildly ramified quadratic extension we use the notation of Lemma 8.6. The right side of the congruence may be taken to be $\beta^2+\beta\alpha\delta$. The identity is again non-trivial only if $\beta O_F = \mathfrak{P}_F^u$ with $u<d$. Then the left side may be taken to be

$$\beta^2 - \beta^2\delta S_{K/F}\left(\frac{\beta_1\alpha}{\beta\alpha_1}\right) + \delta^2\alpha N_{K/F}\beta_1$$

which is congruent to

$$\beta^2 + \alpha\beta\delta - \beta^2\delta S_{K/F}\left(\frac{\beta_1\alpha}{\beta\alpha_1}\right)$$

modulo $\mathcal{P}_F^d$. Since

$$\frac{v-u+t+1}{2} \geq \frac{m}{2} - u \geq d-u$$

we have

$$\beta^2 S_{K/F}\left(\frac{\beta_1\alpha}{\beta\alpha_1}\right) \equiv 0 \pmod{\mathfrak{P}_{\mathrm{F}}^{\mathrm{d}}}.$$

Suppose χ_F is a quasi-character of C_F, $m=m(\chi_F)$, and $\beta=\beta(\chi_F)$. If, as sometimes happens, $m' = m(\chi_{K/F})$ we can take $\beta(\chi_{K/F}) = P^*_{K/F}(\beta)$.

Lemma 8.8

Suppose K/F is Galois and $G=\mathfrak{G}(K/F)$. Suppose $s \geq 0$ is an integer and $G^s=\{1\}$. If $m=m(\chi_F)$ and $m>s$ then

$$m' = \psi_{K/F}(m-1)+1 = m(\psi_{K/F}).$$

It follows from paragraph V.6 of Serre's book that

$$N_{K/F}(U_K^{\psi_{K/F}(v)}) = U_F^v$$

if $v \geq s$. Thus $\chi_{K/F}$ is trivial on U_K^u if $u > \psi_{K/F}(m-1)$ but is not trivial on U_K^i if $u = \psi_{K/F}(m-1)$.

We can now collect together, with one or two additional comments, the previous results in a form which will be useful in the proof of the first main lemma. We use the same notation.

Lemma 8.9

Suppose K/F is a cyclic extension of prime order ℓ, χ_F is a quasi-character of C_F, $m(\chi_F) \geq t+1$, $m(\chi_F) > 1$, and $m(\chi_{K/F}) - 1 = \psi_{K/F}(m(\chi_F) - 1)$.

(a) *If K/F is unramified we may take $\beta(\chi_{K/F}) = \beta(\chi_F)$ and $\beta(\mu_F \chi_F) = \beta(\chi_F)$ for all μ_F in $S(K/F)$.*

(b) *If ℓ is odd and $d \geq t+1$ we may take $\beta(\chi_{K/F}) = \beta(\chi_F)$ and $\beta(\mu_F \chi_F) = \beta(\chi_F)$ for all μ_F in $S(K/F)$.*

(c) *If ℓ is odd and $t+1 \leq m \leq 2t+1$ and μ_F is a given non-trivial character in $S(K/F)$ we may choose $\alpha = \alpha(\mu_F) = N_{K/F}\alpha_1$ as in Lemma 8.5 and $\beta = \beta(\chi_F) = N_{K/F}\beta_1$ for some β_1 in U_K. Then we may choose*

$$\beta(\chi_{K/F}) = \beta - \beta_1 \, \frac{\alpha}{\alpha_1}$$

and

$$\beta(\mu_F^\zeta \chi_F) = N_{K/F}(\beta_1 + \zeta\alpha_1).$$

(d) *If ℓ is 2 and K/F is wildly ramified we choose $\alpha = \alpha(\mu_F)$ as in Lemma 8.6. We may choose $\beta = \beta(\chi_F)$ in the form $\delta N_{K/F}\beta_1$ with δ in U_F^t. Then we may choose*

$$\beta(\chi_{K/F}) = \beta - \beta_1 \, \frac{\alpha\delta}{\alpha_1}$$

and

$$\beta(\mu_F \chi_F) = \beta + \alpha\delta.$$

(e) *If ℓ is 2 and K/F is tamely ramified we may take $\beta(\chi_{K/F}) = \beta(\mu_F \chi_F) = \beta(\chi_F)$.*

Only part (c) requires any further verification. It must be shown that

$$N_{K/F}(\beta_1 + \zeta\alpha_1) \equiv \beta + \zeta\alpha \pmod{\mathfrak{P}_{\mathrm{F}}^{\mathrm{d}}}.$$

The left side is congruent to

$$\beta N_{K/F}\left(1 + \frac{\zeta\alpha_1}{\beta_1}\right).$$

All we need do is show that

$$N_{K/F}\left(1 + \frac{\zeta\alpha_1}{\beta_1}\right) \equiv 1 + \frac{\zeta\alpha}{\beta} \pmod{\mathfrak{P}_{\mathrm{F}}^{\mathrm{d}}}.$$

The right side is

$$1 + N_{K/F}\left(\frac{\zeta\alpha_1}{\beta_1}\right).$$

According to paragraph V.3 of Serre's book the congruence will be satisfied if

$$\frac{v + (\ell - 1)\,(t+1)}{\ell} \geq d.$$

But $t+1=d+x$ with $x\geq 0$ so that $d+x+v=2d+\varepsilon$ and $v=d+\varepsilon-x$. Thus

$$\frac{v+(\ell-1)\,(t+1)}{\ell}=\frac{d+\varepsilon-x+(\ell-1)\,(d+x)}{\ell}=d+\frac{\varepsilon+(\ell-2)x}{\ell}\geq d.$$

The preceding discussion has now to be repeated with different hypotheses and different, but similar, conclusions.

Lemma 8.10

Suppose K/F is abelian and $G=\mathfrak{G}(K/F)$. Suppose there is a $t\geq 0$ such that $G=G_t$ while $G_{t+1}=\{1\}$. If $2\leq m\leq t+1$ then $m'=\psi_{K/F}(m-1)+1$ is just m. Let $t+1=m+v$, let δ be such that $\delta O_F=\mathfrak{P}_F^{t+1+n(\psi_F)}$, let ε_1 in O_K be such that $\varepsilon_1 O_K=\mathfrak{P}_K^v$, and let $\varepsilon=N_{K/F}\varepsilon_1$. We may choose $\gamma_F=\delta/\varepsilon$ and $\gamma_K=\delta/\varepsilon_1$. Let r be the greatest integer in $\frac{t+1}{2}$ and let $s=t+1-r$. If μ_F is a non-trivial character in $S(K/F)$ then $m(\mu_F)=t+1$. Let

$$\mu_F(1+x)=\psi_F\,\left(\frac{\beta(\mu_F)x}{\delta}\right)$$

for x in $\mathfrak{P}_F^s$. Then

$$\beta\prod\nolimits_{\mu_F\neq 1}(\beta\varepsilon+\beta(\mu_F))\equiv N_{K/F}(P^*_{K/F}(\beta))\pmod{\mathfrak{P}_{\mathrm{F}}^{\mathrm{d}}}.$$

The relation $m'=\psi_{K/F}(m-1)+1=m$ is an immediate consequence of the definitions. Since the extension is totally ramified

$$n(\psi_{K/F})=[K:F]n+([K:F]-1)(t+1)$$

if $n=n(\psi_F)$. Thus

$$m+n=(t+1+n)-v$$

and

$$m'+n(\psi_{K/F})=[K:F](t+1+n)+(m-t-1)=[K:F](t+1+n)-v.$$

Consequently γ_F and γ_K can be chosen as asserted. The results of chapter V of Serre's book imply that $m(\mu_F)=t+1$ if μ_F is not trivial.

We saw when proving Lemma 8.2 that if $x\equiv y\pmod{\mathfrak{P}_{\mathrm{K}}^{\mathrm{d}'}}$ then $N_{K/F}x\equiv N_{K/F}y\pmod{\mathfrak{P}_{\mathrm{F}}^{\mathrm{d}}}$ and that if $F\subseteq L\subseteq K$ both L/F and K/L satisfy the conditions of the lemma. For L/F, ε_1 is replaced by $N_{K/L}\varepsilon_1$ and, for K/L, ε is replaced by $N_{K/L}\varepsilon_1$. Take $Q^*_{L/F}$ to be $P^*_{L/F}$ in the special case that $m=t+1$ and $\varepsilon_1=1$. Then

$$\psi_{L/F}\,\left(\frac{N_{K/L}(\varepsilon_1)x\,P^*_{L/F}(\beta)}{\delta}\right)=\psi_F\,\left(\frac{\varepsilon P_{L/F}(x)\beta}{\delta}\right)$$

by definition. The right side is equal to

$$\psi_{L/F}\,\left(\frac{x\,Q^*_{L/F}(\varepsilon\beta)}{\delta}\right).$$

Thus

$$Q^*_{L/F}(\varepsilon\beta) \equiv N_{K/L}(\varepsilon_1) P^*_{L/F}(\beta) \pmod{\mathfrak{P}_{\mathrm{L}}^{\mathrm{s}}}.$$

If μ_F belongs to $S(K/F)$ but not to $S(L/F)$ then $m(\mu_{L/F}) = m(\mu_F)$ and $\beta(\mu_{L/F})$ may be taken to be $Q^*_{L/F}(\beta(\mu_F))$. Let S' be a set of representatives for the cosets of $S(L/F)$ in $S(K/F) - S(L/F)$ and suppose the lemma is true for K/L and L/F. Then

$$N_{K/F}(P^*_{K/F}(\beta)) = N_{L/F}(N_{K/L}(P^*_{K/L}(P^*_{L/F}(\beta))))$$

is congruent to

$$N_{L/F}(P^*_{L/F}(\beta) \prod\nolimits_{\mu_F \in S'} \{N_{K/L}(\varepsilon_1) P^*_{L/F}(\beta) + Q^*_{L/F}(\beta(\mu_F))\})$$

modulo $\mathfrak{P}_F^d$. This in turn is congruent to

$$N_{L/F}(P^*_{L/F}(\beta)) \prod\nolimits_{\mu_F \in S'} N_{L/F}(Q^*_{L/F}(\varepsilon\beta + \beta(\mu_F))).$$

Applying the induction hypothesis to the first part and Lemma 8.2 to the second, we see that the whole expression is congruent to

$$\beta \left\{ \prod\nolimits_{\substack{\nu_F \in S(L/F) \\ \nu_F \neq 1}} (\varepsilon\beta + \beta(\nu_F)) \right\} \left\{ \prod\nolimits_{\substack{\mu_F \in S' \\ \nu_F \in S(L/F)}} (\varepsilon\beta + \beta(\mu_F) + \beta(\nu_F)) \right\}$$

modulo $\mathfrak{P}_F^d$ as required.

Once again we devote a lemma to cyclic extensions of prime order.

Lemma 8.11

Suppose K/F is cyclic of prime order ℓ and $2 \leq m \leq t+1$. Choose a non-trivial character μ_F in $S(K/F)$. There is an α_1 in U_K such that if $\alpha = N_{K/F}\alpha_1$

$$\mu_F(1+x) = \psi_F \left(\frac{\alpha x}{\delta}\right)$$

for x in $\mathcal{P}_F^s$. If β belongs to O_F there is a β_1 in O_K such that $\beta \equiv N_{K/F}(\beta_1) \pmod{\mathfrak{P}_{\mathrm{F}}^{\mathrm{t}}}$. Then

$$P^*_{K/F}(\beta) \equiv \beta \, \frac{\varepsilon}{\varepsilon_1} - \beta_1 \, \frac{\alpha}{\alpha_1} \pmod{\mathfrak{P}_{\mathrm{K}}^{\mathrm{d}'}}.$$

Since $\beta(\mu_F)$ is determined only modulo $\mathfrak{P}_F^s$ and $s \leq t$ we can take $\beta(\mu_F) = N_{K/F}\alpha_1$ for some α_1 in U_K. The existence of β_1 also follows as before. Since $t+1 \geq m$

$$\frac{2(d' + \varepsilon') + (\ell - 1)(t+1)}{\ell} \geq \frac{m + (\ell-1)(t+1)}{\ell} \geq m$$

and

$$N_{K/F}(1+x) \equiv 1 + S_{K/F}(x) + N_{K/F}(x) \pmod{\mathfrak{P}_{\mathrm{F}}^{\mathrm{m}}}$$

if x belongs to $\mathfrak{P}_K^{d'+\varepsilon'}$. Thus

$$\psi_F\left(\frac{\varepsilon P_{K/F}(x)\beta}{\delta}\right) = \psi_{K/F}\left(\frac{\varepsilon x\beta}{\delta}\right)\ \psi_F\left(\frac{N_{K/F}(\varepsilon_1 x)\beta}{\delta}\right).$$

But $d' + \varepsilon' + t \geq t+1$ so that

$$N_{K/F}(\varepsilon_1 x)\beta \equiv \alpha N_{K/F}\left(\frac{\varepsilon_1\beta_1}{\alpha_1}\cdot x\right) \pmod{\mathfrak{P}_{\mathrm{F}}^{\mathrm{t}+1}}$$

Since $t+1 = m+v,\ d'+\varepsilon'+v \geq s$ and if $y = \frac{\varepsilon_1\beta_1}{\alpha_1}\cdot x$ then y which lies in $\mathfrak{P}_K^{d'+\varepsilon'+v}$ also lies in $\mathfrak{P}_K^s$. But

$$\frac{2s+(t+1)(\ell-1)}{\ell} \geq t+1$$

so that

$$N_{K/F}(1+y) \equiv 1 + S_{K/F}(y) + N_{K/F}(y) \pmod{\mathfrak{P}_{\mathrm{F}}^{\mathrm{t}+1}}.$$

Consequently

$$\psi_F\left(\frac{-\alpha N_{K/F}(y)}{\delta}\right) = \psi_F\left(\frac{\alpha S_{K/F}(y)}{\delta}\right).$$

In conclusion

$$\psi_F\left(\frac{\varepsilon\, P_{K/F}(x)\beta}{\delta}\right) = \psi_{K/F}\left(\frac{\varepsilon_1}{\delta}\left(\frac{\varepsilon}{\varepsilon_1}\cdot\beta - \frac{\alpha}{\alpha_1}\cdot\beta_1\right)x\right)$$

as required.

To complete the proof of Lemma 8.10 we have to show that when K/F is cyclic of prime order, ℓ

$$\beta\prod\nolimits_{\mu_F\neq 1}(\beta\varepsilon + \beta(\mu_F)) \equiv N_{K/F}(P^*_{K/F}(\beta)) \pmod{\mathfrak{P}_{\mathrm{F}}^{\mathrm{d}}}$$

Since $2 \leq m \leq t+1$ the extension is wildly ramified, $\ell = p$, and once the character μ_F is chosen as in the previous lemma we can define μ_F^ζ as in Lemma 8.5. The left side is congruent to

$$\beta\left(\beta^{\ell-1}\varepsilon^{\ell-1} + (-1)^\ell\alpha^{\ell-1}\right).$$

If $\beta \in \mathfrak{P}_F^d$ this is congruent to 0 and so is the right side. Suppose $\beta O_F = \mathfrak{P}_F^u$ with $u < d$. The right side is congruent to

$$N_{K/F}\left(\beta\,\frac{\varepsilon}{\varepsilon_1} - \beta_1\,\frac{\alpha}{\alpha_1}\right) \equiv \beta\alpha^{\ell-1}N_{K/F}\left(\frac{\beta}{\beta_1}\ \frac{\alpha_1}{\alpha}\ \frac{\varepsilon}{\varepsilon_1} - 1\right).$$

Since

$$\frac{(\ell-1)(u+v)+(\ell-1)(t+1)}{\ell} \geq \frac{\ell-1}{\ell}\cdot(t+1) \geq \frac{t+1}{2} \geq d$$

this is congruent to

$$\beta\alpha^{\ell-1}\left\{N_{K/F}\left(\frac{\beta}{\beta_1}\ \frac{\alpha_1}{\alpha}\ \frac{\varepsilon}{\varepsilon_1}\right) + (-1)^\ell\right\}. \tag{8.1}$$

Since

$$\beta N_{K/F}\left(\beta_1^{-1}\right) \equiv 1 \pmod{\mathfrak{P}_F^{t-u}}.$$

We see that

$$\beta^{\ell+1} N_{K/F}\beta_1^{-1} \equiv \beta^{\ell} \pmod{\mathfrak{P}_F^{t}}$$

and that the expression (8.1) is congruent to

$$\beta^{\ell}\varepsilon^{\ell-1} + (-1)^{\ell}\beta\alpha^{\ell-1}$$

modulo $\mathfrak{P}_F^d$.

Lemma 8.12

Suppose K/F is abelian and $G = \mathfrak{G}(K/F)$. Suppose there is an integer t such that $G = G_t$ while $G_{t+1} = \{1\}$. Let χ_F be a quasi-character of C_F and suppose $2 \le m(\chi_F) \le t+1$. If $m(\chi_F) < t+1$ then $m(\chi_{K/F}) = m(\chi_F)$. If $m(\chi_F) = t+1$ then $m(\mu_F\chi_F) < t+1$ for some μ_F in $S(K/F)$ if and only if $m(\chi_{K/F}) < m(\chi_F)$.

It follows immediately from Lemma 6.7 that if χ_F is any quasi-character of C_F and E any finite separable extension of F then

$$m(\chi_{E/F}) - 1 \le \psi_{E/F}(m(\chi_F) - 1).$$

In the particular case under consideration Lemma 6.10 shows that if $m = m(\chi_F) \le t$ then

$$N_{K/F} : U_K^{m-1}/U_K^t \longrightarrow U_F^{m-1}/U_F^t$$

is an isomorphism. Thus $\chi_{K/F}(\alpha)$ will be different from 1 for some α in U_K^{m-1} and $m(\chi_{K/F})$ will be at least m. If $m(\chi_F) = t+1$ then $m(\mu_F\chi_F)$ is less than $t+1$ for some μ_F in $S(K/F)$ if and only if χ_F is trivial on the image of U_K^t/U_K^{t+1} in U_F^t/U_F^{t+1}. This is so if and only if $m(\chi_{K/F}) \le t$.

We shall need the following lemma in the proof of the first main lemma.

Lemma 8.13

Suppose K/F is cyclic of prime order, χ_F is a quasi-character of C_F with $m(\chi_F) \le t+1$, and $m(\chi_{K/F}) = m(\chi_F)$. Choose $\alpha, \alpha_1, \varepsilon, \varepsilon_1$ in Lemma 8.11. We may choose $\beta = \beta(\chi_F) = N_{K/F}\beta_1$ with β_1 in U_K and we may choose

$$\beta(\chi_{K/F}) = \beta\,\frac{\varepsilon}{\varepsilon_1} - \beta_1\,\frac{\alpha}{\alpha_1}.$$

Moreover $m(\mu_F^{\zeta}\chi_F) = t+1$ and we may take

$$\beta(\mu_F^{\zeta}\chi_F) = N_{K/F}(\zeta\alpha_1 + \varepsilon_1\beta_1).$$

Since $\beta(\chi_F)$ is determined only modulo $\mathfrak{P}_F^d$ and $d \le t$ the existence of β_1 is clear. It is also clear that $m(\mu_F^{\zeta}\chi_F) = t+1$. The elements $\beta(\chi_F)$, $\beta(\chi_{K/F})$, and $\beta(\mu_F^{\zeta}\chi_F)$ are to satisfy the following conditions:

(i) If x is in $\mathfrak{P}_F^d$

$$\chi_F(1+x) = \psi_F\left(\frac{\varepsilon\beta(\chi_F)x}{\delta}\right).$$

(ii) If x is in $\mathfrak{P}_K^{d'}$

$$\chi_{K/F}(1+x) = \psi_{K/F}\left(\frac{\varepsilon_1\beta(\chi_{K/F})x}{\delta}\right).$$

(iii) If x is in $\mathfrak{P}_F^s$

$$\mu_F^\zeta(1+x)\chi_F(1+x) = \psi_F\left(\frac{\beta(\mu_F^\zeta\chi_F)x}{\delta}\right).$$

We have already shown that $\beta(\chi_{K/F})$ may be taken to be

$$\beta\ \frac{\varepsilon}{\varepsilon_1} - \beta_1\ \frac{\alpha}{\alpha_1}$$

$\beta(\mu_F^\zeta\chi_F)$ must be congruent to $\zeta\alpha+\varepsilon\beta$ modulo $\mathfrak{P}_F^r$

$$N_{K/F}(\zeta\alpha_1+\varepsilon_1\beta_1) = \zeta\alpha N_{K/F}\left(1+\frac{\varepsilon_1\beta_1}{\zeta\alpha_1}\right).$$

Since

$$\frac{\nu+(\ell-1)(t+1)}{\ell} \geq \frac{\ell-1}{\ell}(t+1) \geq r.$$

The right side is congruent to

$$\zeta\alpha\left\{1+N_{K/F}\left(\frac{\varepsilon_1\beta_1}{\zeta\alpha_1}\right)\right\} = \zeta\alpha+\varepsilon\beta$$

modulo $\mathfrak{P}_F^r$.*

∗(1998) The manuscript of Chapter 8 ends here.

Chapter Nine.

A Lemma of Hasse

Let $\lambda \subseteq \kappa$ be two finite fields and let $G = \mathfrak{G}(\kappa/\lambda)$. If $x \in \kappa$ set

$$\omega_{\kappa/\lambda}(x) = \sum x^{\sigma_1} x^{\sigma_2}$$

where the sum is taken over all unordered pairs of distinct elements of G. It is clear that

$$\omega_{\kappa/\lambda}(x+y) = \omega_{\kappa/\lambda}(x) + \omega_{\kappa/\lambda}(y) + S_{\kappa/\lambda}(x)S_{\kappa/\lambda}(y) - S_{\kappa/\lambda}(xy).$$

One readily verifies also that if $\lambda \le \eta \le \kappa$ then

$$\omega_{\kappa/\lambda}(x) = \omega_{\eta/\lambda}(S_{\kappa/\eta}(x)) + S_{\eta/\lambda}\,(\omega_{\kappa/\eta}(x)).$$

Suppose ψ_λ is a non-trivial character of λ and φ_λ is a nowhere vanishing function on λ satisfying the identity

$$\varphi_\lambda(x+y) = \varphi_\lambda(x)\varphi_\lambda(y)\,\psi_\lambda(xy).$$

Define $\varphi_{\kappa/\lambda}$ on κ by

$$\varphi_{\kappa/\lambda}(x) = \varphi_\lambda(S_{\kappa/\lambda}(x))\,\psi_\lambda(-\omega_{\kappa/\lambda}(x)).$$

Then $\varphi_{\kappa/\lambda}(x+y)$ is equal to

$$\varphi_\lambda(S_{\kappa/\lambda}(x+y))\,\psi_\lambda\left(-\omega_{\kappa/\lambda}(x) - \omega_{\kappa/\lambda}(y) - S_{\kappa/\lambda}(x)S_{\kappa/\lambda}(y) + S_{\kappa/\lambda}(xy)\right)$$

which is

$$\varphi_{\kappa/\lambda}(x)\varphi_{\kappa/\lambda}(y)\psi_{\kappa/\lambda}(xy).$$

If the fields have odd characteristic the following lemma is, basically, a special case of Lemma 7.7. That lemma has been proven in a simple and direct manner by Weil [14]. We shall use his method to prove the following lemma which in characteristic two, when it cannot be reduced to the previous lemma, is due to Hasse [8].

Lemma 9.1

Let

$$\sigma(\varphi_\lambda) = -\sum\nolimits_{x\in\lambda} \varphi_\lambda(x)$$

and let

$$\sigma(\varphi_{\kappa/\lambda}) = -\sum\nolimits_{x\in\kappa} \varphi_{\kappa/\lambda}(x).$$

Then

$$\sigma(\varphi_{\kappa/\lambda}) = \sigma(\varphi_\lambda)^{[\kappa:\lambda]}.$$

If

$$P(X) = X^m - aX^{m-1} + bX^{m-2} - + \dots$$

is any monic polynomial with coefficients in λ set $m(P)=m$ and

$$\chi_\lambda(P)=\varphi_\lambda(a)\ \psi_\lambda(-b).$$

If the degree of the polynomial is 1, b is taken to be 0; if the degree is 0 both a and b are taken to be 0. If

$$P'(X)=X^{m'}-a'\ X^{m'-1}+b'\,X^{m'-2}-+\dots$$

then

$$PP'(X)=X^{m+m'}-(a+a')\,X^{m+m'-1}+(b+b'+aa')X^{m+m'-2}-+\dots$$

and

$$\chi_\lambda(PP')=\varphi_\lambda(a+a')\,\psi_\lambda(-b-b'-aa')=\chi_\lambda(P)\chi_\lambda(P').$$

If t is an indeterminate we introduce the formal series

$$F_\lambda(t)=\sum\ \chi_\lambda(P)t^{m(P)}=\prod(1-\chi_\lambda(P)t^{m(P)})^{-1}.$$

The sum is overall monic polynomials with coefficients in λ and the product is overall irreducible polynomials of positive degree with coefficients in λ. If $r\geq 2$

$$\sum\nolimits_{m(P)=r}\chi_\lambda(P)=0$$

so that

$$F_\lambda(t)=1-\sigma(\varphi_\lambda)t.$$

If we replace λ by κ, φ_λ by $\varphi_{\kappa/\lambda}$, and ψ_λ by $\psi_{\kappa/\lambda}$, we can define $F_{\kappa/\lambda}(t)$ in a similar way. If $k=[\kappa:\lambda]$ and T is the set of kth roots of unity the problem is to show that

$$\prod\nolimits_{\zeta\in T}\ F_\lambda(\zeta t)=F_{\kappa/\lambda}(t^k).$$

Suppose P is an irreducible monic polynomial with coefficients in λ and P' is one of its monic irreducible factors over κ. Let $m=m(P)$ and let r be the greatest common divisor of m and k. The field obtained by adjoining the roots of P to κ has degree $\frac{mk}{r}$ over λ and is the same as the field obtained by adjoining the roots of P' to κ. Thus $m(P')=\frac{m}{r}$ and P splits into r irreducible factors over κ. We shall show that

$$\chi_{\kappa/\lambda}(P')=\{\chi_\lambda(P)\}^{\frac{k}{r}}.$$

Thus if $P'_1,\dots,P'_r$ are the factors of P and $\ell=\frac{k}{r}$

$$\prod\nolimits_{i=1}^{r}\{1-\chi_{\kappa/\lambda}(P'_i)t^{km(P'_i)}\}=\{1-\chi_\lambda(P)^\ell t^{\ell m}\}^r$$

which equals

$$\prod\nolimits_{\zeta\in T}\ \{1-\chi_\lambda(P)\zeta^m t^m\}.$$

The necessary identity follows.

Let ν be the field obtained by adjoining a root x of P' to κ and let μ be the field obtained by adjoining x to λ. If

$$P(X) = X^m - aX^{m-1} + bX^{m-2} \dots$$

then

$$a = S_{\mu/\lambda}(x)$$

and

$$b = \omega_{\mu/\lambda}(x).$$

Thus

$$\chi_\lambda(P) = \varphi_\lambda(S_{\mu/\lambda}(x))\,\psi_\lambda(-\omega_{\mu/\lambda}(x)) = \varphi_{\mu/\lambda}(x).$$

Since $\varphi_{\nu/\lambda}(x)$ is equal to

$$\varphi_\lambda(S_{\kappa/\lambda}(S_{\nu/\kappa}(x)))\,\psi_\lambda(-\omega_{\kappa/\lambda}(S_{\nu/\kappa}(x)) + S_{\kappa/\lambda}(\omega_{\nu/\kappa}(x)))$$

which in turn equals

$$\varphi_{\kappa/\lambda}(S_{\nu/\kappa}(x))\,\psi_{\kappa/\lambda}(-\omega_{\nu/\kappa}(x)).$$

We conclude that

$$\chi_{\kappa/\lambda}(P') = \varphi_{\nu/\lambda}(x).$$

Replacing κ by μ we see that $\varphi_{\nu/\lambda}(x)$ equals

$$\varphi_{\mu/\lambda}(S_{\nu/\mu}(x))\,\psi_{\mu/\lambda}(-\omega_{\nu/\mu}(x)) = \varphi_{\mu/\lambda}(\ell x)\,\psi_{\mu/\lambda}\left(-\ell\,\frac{(\ell-1)}{2}\,x^2\right).$$

One easily shows by induction that for every integer ℓ

$$\{\varphi_{\mu/\lambda}(x)\}^\ell = \varphi_{\mu/\lambda}(\ell x)\,\Psi_{\mu/\lambda}\left(-\ell\,\frac{(\ell-1)}{2}\,x^2\right). \tag{9.1}$$

The relation

$$\chi_{\kappa/\lambda}(P') = \{\chi_\lambda(P)\}^\ell$$

follows.

Taking $\mu = \lambda$ in the identity (9.1) we see that

$$\{\varphi_\lambda(x)\}^\ell = \varphi_\lambda(\ell x)\,\psi_\lambda\left(-\ell\,\frac{(\ell-1)}{2}\,x^2\right)$$

for every integer ℓ. Moreover $\{\varphi_\lambda(0)\}^2 = \varphi_\lambda(0)$ so that $\varphi_\lambda(0) = 1$. If the characteristic p of λ is odd take $\ell = p$ to see that $\{\varphi_\lambda(x)\}^p = 1$. If the characteristic is 2, take $\ell = 4$ to see that $\{\varphi_\lambda(x)\}^4 = 1$. Suppose φ'_λ is another function on λ which vanishes nowhere and satisfies

$$\varphi'_\lambda(x+y) = \varphi'_\lambda(x)\,\varphi'_\lambda(y)\,\psi_\lambda(xy).$$

Then $\varphi'_\lambda\varphi_\lambda^{-1}$ is a character and for some α in λ

$$\varphi'_\lambda(x) \equiv \varphi_\lambda(x)\,\psi_\lambda(\alpha x).$$

Of course
$$\varphi_\lambda(x)\psi_\lambda(\alpha x)=\varphi_\lambda(x+\alpha)\varphi_\lambda^{-1}(\alpha).$$
Thus
$$\sigma(\varphi'_\lambda)=\varphi_\lambda^{-1}(\alpha)\,\sigma(\varphi_\lambda).$$
If a and b are two non-zero complex numbers and m is a positive integer we write $a\sim_m b$ if, for some integer $r\geq 0$, $\left(\frac{a}{b}\right)^{m^r}=1$.

Lemma 9.2

If $\alpha\in\lambda^\times$, the multiplicative group of λ, let $\nu(\alpha)$ be 1 or -1 according as α is or is not a square in λ. Suppose $\psi'_\lambda(x)=\psi_\lambda(\alpha x),\ \varphi_\lambda$ and φ'_λ are nowhere vanishing, and

$$\varphi_\lambda(x+y)=\varphi_\lambda(x)\varphi_\lambda(y)\psi_\lambda(xy)$$

while
$$\varphi'_\lambda(x+y)=\varphi'_\lambda(x)\varphi'_\lambda(y)\psi'_\lambda(xy).$$
Then
$$\sigma(\varphi'_\lambda)\sim_p\nu(\alpha)\sigma(\varphi_\lambda).$$
Moreover
$$\sigma(\varphi_\lambda)\sim_{2p}\ |\sigma(\varphi_\lambda)|.$$

Suppose first that p is odd. By the remarks preceding the statement of the lemma it is enough to prove the assertions for one choice of φ_λ and φ'_λ. For example we could take $\varphi_\lambda(x)=\Psi_\lambda\ \left(\frac{(x^2)}{2}\right)$ and if $\alpha=\beta^2$ we could take $\varphi'_\lambda(x)=\psi_\lambda\ \left(\frac{(\beta x)^2}{2}\right)$. In this case it is clear that $\sigma(\varphi_\lambda)=\sigma(\varphi'_\lambda)$. However if α is not a square, we take $\varphi'_\lambda(x)=\psi_\lambda\ \left(\frac{\alpha x^2}{2}\right)$. Then

$$\sigma(\varphi_\lambda)+\sigma(\varphi'_\lambda)=2\ \sum\nolimits_{x\in\lambda}\ \psi_\lambda\ \left(\frac{x}{2}\right)=0.$$

With this choice of φ_λ,
$$\overline{\varphi_\lambda(x)}=\psi_\lambda\ \left(-\frac{x^2}{2}\right)$$
so that $\overline{\sigma(\varphi_\lambda)}=\nu(-1)\ \sigma(\varphi_\lambda)$. Moreover it is well known and easily verified that $\sigma(\varphi_\lambda)\neq 0$. Since
$$\{\sigma(\varphi_\lambda)\}^4=\{\nu(-1)\}^2\ |\sigma(\varphi_\lambda)|^4=|\sigma(\varphi_\lambda)|^4$$
we have
$$\sigma(\varphi_\lambda)\sim_{2p}\ |\sigma(\varphi_\lambda)|.$$
The absolute value on the right is of course the ordinary absolute value.

Suppose p is 2. Again any choice of φ_λ and φ'_λ will do. In this case α is necessarily a square. Let $\alpha=\beta^2$. We can take $\varphi'_\lambda(x)=\varphi_\lambda(\beta x)$. Then $\sigma(\varphi'_\lambda)=\sigma(\varphi_\lambda)$. It is enough to prove the second assertion for any ψ_λ and any φ_λ. Let ϕ be the prime field and let ψ_ϕ be the unique non-trivial additive character of ϕ. Take $\psi_\lambda=\psi_{\lambda/\phi}$. Let $\varphi_\phi(0)=1,\ \ \varphi_\phi(1)=i$. One verifies by inspection that

$$\varphi_\phi(x+y)=\varphi_\phi(x)\varphi_\phi(y)\psi_\phi(xy).$$

Take $\varphi_\lambda = \varphi_{\lambda/\phi}$. Since

$$\sigma(\varphi_{\lambda/\phi}) = \{\sigma(\varphi_\phi)\}^{[\lambda:\phi]},$$

it is enough to verify that

$$\sigma(\varphi_\phi) \sim_2 \ |\sigma(\varphi_\phi)|.$$

Since $\sigma(\varphi_\phi) = -1 + i$, this is no problem.

If a is a non-zero complex number set

$$A\,[a] = \frac{a}{|a|}.$$

The following lemma explains our interest in the numbers $\sigma(\varphi_\lambda)$.

Lemma 9.3

Suppose L is a non-archimedean local field and χ_L is a quasi-character of C_L with $m = m(\chi_L) = 2d+1$, where d is a positive integer. Let ψ_L be a non-trivial additive character of L and let $n = n(\psi_L)$. Let γ be such that $\gamma O_L = \mathcal{P}_L^{m+n}$ and let β be a unit such that

$$\chi_L(1+x) = \psi_L\ \left(\frac{\beta x}{\gamma}\right)$$

for x in $\mathfrak{P}_L^{d+1}$. Choose δ so that $\delta O_L = \mathfrak{P}_L^d$ and let ψ_λ be the character of $\lambda = O_L/\mathfrak{P}_L$ defined by

$$\psi_\lambda(x) = \psi_L\ \left(\frac{\beta\delta^2 x}{\gamma}\right).$$

If φ_λ is defined by

$$\varphi_\lambda(x) = \psi_L\ \left(\frac{\beta\delta x}{\gamma}\right)\ \chi_L^{-1}(1+\delta x)$$

then

$$\varphi_\lambda(x+y) = \varphi_\lambda(x)\varphi_\lambda(y)\psi_\lambda(xy)$$

and

$$\Delta_3(\chi_L,\, \psi_L,\, \gamma) = A\,[-\sigma(\varphi_\lambda)].$$

In the statement of this lemma we have not distinguished, in the notation, between an element of O_L and its image in λ. This is convenient and not too ambiguous. It will be done again. The only questionable part of the lemma is the relation

$$\varphi_\lambda(x+y) = \varphi_\lambda(x)\varphi_\lambda(y)\psi_\lambda(xy).$$

Since

$$(1+\delta x)\ (1+\delta y) \equiv (1+\delta x+\delta y)\ (1+\delta^2 xy) \pmod{\mathfrak{P}_L^m}$$

we have

$$\chi_L^{-1}(1+\delta x)\,\chi_L^{-1}(1+\delta y) = \chi_L^{-1}(1+\delta x+\delta y)\,\psi_L\left(-\frac{\beta\delta^2 xy}{\gamma}\right).$$

The required relation follows immediately.

There are a few remarks which we shall need later. It is convenient to formulate them explicitly now. We retain the notation of the previous lemma.

Lemma 9.4

If $m(\mu_L) < m(\chi_L)$ then

$$\Delta_3(\mu_L\,\chi_L,\ \Psi_L;\gamma) \sim_p\ \Delta_3\,(\chi_L, \Psi_L;\gamma)$$

and if $m(\mu_L) \le d$ we may take $\beta(\mu_L\chi_L) = \beta(\chi_L)$ and then

$$\Delta_3(\mu_L\chi_L, \psi_L;\gamma) = \Delta_3(\chi_L, \psi_L;\gamma).$$

In both cases $m(\mu_L\chi_L) = m(\chi_L)$. Moreover if $x \in \mathfrak{P}_L^{2d}$

$$\psi_L\ \left(\frac{\beta(\mu_L\chi_L)x}{\gamma}\right) = \mu_L(1+x)\,\chi_L(1+x) = \chi_L(1+x)$$

which in turn equals

$$\psi_L\ \left(\frac{\beta(\chi_L)x}{\gamma}\right).$$

Thus

$$\beta(\mu_L\chi_L) \equiv \beta(\chi_L) \pmod{\mathfrak{P}_L}$$

and if

$$\psi_\lambda(x) = \psi_L\ \left(\frac{\beta(\chi_L)\delta^2 x}{\gamma}\right)$$

while

$$\psi'_\lambda(x) = \psi_L\ \left(\frac{\beta(\mu_L\chi_L)\delta^2 x}{\gamma}\right)$$

then $\psi_\lambda = \psi'_\lambda$. The first assertion of the lemma now follows from the previous two lemmas. It is clear that we can take $\beta(\mu_L\chi_L) = \beta(\chi_L)$ if $m(\mu_L) \le d$. Let the common value of the two numbers be β. Then

$$\psi_L\ \left(\frac{\beta\delta x}{\gamma}\right)\ \mu_L^{-1}(1+\delta x)\chi_L^{-1}(1+\delta x)$$

is equal to

$$\psi_L\ \left(\frac{\beta\delta x}{\gamma}\right)\ \chi_L^{-1}(1+\delta x).$$

We see now that the second assertion is completely trivial.

There is a corollary of this lemma which it is convenient to observe.

Lemma 9.5

Suppose $m(\chi_L) = 2d + \varepsilon$ where d is a positive integer and ε is 0 or 1. If $m(\mu_L) \le d$ and μ_L is of order r then

$$\Delta(\mu_L\chi_L, \psi_L) \sim_r \Delta(\chi_L, \psi_L).$$

Choose γ in the usual way so that

$$\Delta(\chi_L, \psi_L) = \chi_L(\gamma)\ \Delta_1(\chi_L, \psi_L; \gamma)$$

and

$$\Delta(\mu_L \chi_L, \psi_L) = \chi_L(\gamma)\mu_L(\gamma)\ \Delta_1(\mu_L\chi_L, \psi_L; \gamma).$$

It is clear that

$$\mu_L(\gamma) \sim_r 1.$$

If we take

$$\beta(\mu_L \chi_L) = \beta(\chi_L)$$

then, clearly,

$$\Delta_2(\mu_L\chi_L, \psi_L; \gamma) \sim_r\ \Delta_2(\chi_L, \psi_L, \gamma).$$

To complete the proof of Lemma 9.5 we have only to appeal to Lemma 9.4.

Lemma 9.6

Suppose K is an unramified extension of L and χ_L is a quasi-character of C_L with

$$m = m(\chi_L) = 2d + 1$$

where d is a positive integer. Let ψ_L be a non-trivial additive character of F and let $n = n(\psi_L)$. Suppose

$$\chi_L(1 + x) = \psi_L\ \left(\frac{\beta x}{\varpi_L^{m+n}}\right)$$

for x in $\mathfrak{P}_L^{d+1}$. Take

$$\beta(\chi_L) = \beta(\chi_{K/L}) = \beta.$$

If

$$\varphi_\lambda(x) = \psi_L\ \left(\frac{\beta\varpi_L^d x}{\varpi_L^{m+n}}\right)\ \chi_L^{-1}(1 + \varpi_L^d x)$$

and if

$$\varphi_\kappa(x) = \psi_{K/L}\ \left(\frac{\beta\varpi_L^d x}{\varpi_L^{m+n}}\right)\ \chi_{K/L}^{-1}(1 + \varpi_L^d x)$$

for x in $\kappa = 0_K/\mathfrak{P}_K$ then $\varphi_\kappa = \varphi_{\kappa/\lambda}$. Moreover if $[K : L] = \ell$ then

$$\Delta_3(\chi_{K/L}, \psi_{K/L}, \varpi_L^{m+n}) = (-1)^{\ell-1}\{\Delta_3(\chi_L, \psi_L, \varpi_L^{m+n})\}^\ell.$$

Once we prove that $\varphi_\kappa = \varphi_{\kappa/\lambda}$ this lemma will follow from Lemmas 9.1 and 9.3. If x belongs to K let $E^2(x)$ be the second elementary symmetric function of x and its conjugates over L. If x belongs to O_K

$$N_{K/F}(1 + \varpi_L^d x) \equiv (1 + \varpi_L^d S_{K/L} x)\,(1 + \varpi_L^{2d} E^2(x)) \pmod{\mathfrak{P}_L^m}.$$

Since

$$E^2(x) \equiv \omega_{\kappa/\lambda}(x) \pmod{\mathfrak{P}_F}$$

we have

$$\varphi_\kappa(x) = \varphi_\lambda(S_{K/L}x)\psi_\lambda(-\omega_{\kappa/\lambda}(x)) = \varphi_{\kappa/\lambda}(x).$$

Now suppose K is a ramified abelian extension of L and $[K : L] = \ell$ is an odd prime. Let $G = \mathfrak{G}(K/L)$ and suppose $G = G_t$ while $G_{t+1} = \{1\}$. Suppose

$$m = m(\chi_L) = 2d + 1$$

is greater than or equal to $t + 1$ and

$$\chi_L(1 + x) = \psi_L \left(\frac{\beta x}{\varpi_L^{m+n}}\right)$$

for x in $\mathcal{P}_L^{d+1}$. Let

$$d' = \ell d - \left(\frac{\ell - 1}{2}\right) t$$

and if x belongs to O_K set

$$\varphi'_\lambda(x) = \psi_{K/L} \left(\frac{\beta\varpi_K^{d'}x}{\varpi_L^{m+n}}\right) \chi_L^{-1}(1 + S_{K/L}(\varpi_K^{d'}x) + E^2(\varpi_K^{d'}x)).$$

Suppose also that

$$\varpi_L = N_{K/L}\varpi_K.$$

The assumptions listed, we may now state the next lemma.

Lemma 9.7

If

$$\varepsilon = S_{K/L} \left(\frac{\varpi_K^{2d'}}{\varpi_L^{2d}}\right)$$

then ε is a unit. Moreover φ'_λ is a function on $\lambda = O_L/\mathcal{P}_L + O_K/\mathcal{P}_K$ which satisfies

$$\varphi'_\lambda(x + y) = \varphi'_\lambda(x)\varphi'_\lambda(y)\psi_\lambda(\varepsilon xy)$$

if

$$\psi_\lambda(u) = \psi_L \left(\frac{\beta u}{\varpi_L^{1+n}}\right).$$

If

$$\varphi_\lambda(x) = \psi_L \left(\frac{\beta x}{\varpi_L^{d+1+n}}\right) \chi_L^{-1} (1 + \varpi_L^d x)$$

then

$$A[\sigma(\varphi_\lambda)]^\ell = A[\sigma(\varphi'_\lambda)].$$

Since

$$\frac{d' + (\ell - 1)(t + 1)}{\ell} \geq d$$

the number

$$S_{K/L}\ (\varpi_K^{d'} x)$$

lies in $\mathfrak{P}_L^d$. Moreover $E^2(\varpi_K^{d'} x)$ is a sum of traces of elements in $\mathfrak{P}_K^{2d'}$. Since

$$\frac{2d' + (\ell - 1)\,(t+1)}{\ell} = 2d + \frac{\ell - 1}{\ell} \geq 2d$$

it lies in $\mathfrak{P}_L^{2d}$. If x lies in $\mathfrak{P}_K$ it lies in $\mathfrak{P}_L^m$ and

$$S_{K/L}(\varpi_K^{d'} x)$$

lies in $\mathfrak{P}_L^{d+1}$ because

$$\frac{d' + 1 + (\ell - 1)\,(t+1)}{\ell} = d + 1 + \frac{t(\ell - 1)}{2\ell} \geq d + 1.$$

Thus if x belongs to $\mathcal{P}_K$

$$\varphi'_\lambda(x) = \psi_L\ \left(\frac{\beta}{\varpi_L^{m+n}}\ S_{K/L}\,(\varpi_K^{d'} x)\right)\,\chi_L^{-1}\,(1 + S_{K/L}(\varpi_K^{d'} x)) = 1.$$

Since

$$E^2(\varpi_K^{d'}(x+y))$$

is equal to

$$E^2(\varpi_K^{d'} x) + E^2(\varpi_K^{d'} y) + S_{K/L}(\varpi_K^{d'} x)\,S_{K/L}(\varpi_K^{d'} y) - S_{K/L}(\varpi_K^{2d'} xy),$$

the expression

$$1 + S_{K/L}(\varpi_K^{d'}(x+y)) + E^2(\varpi_K^{d'}(x+y))$$

is congruent modulo $\mathfrak{P}_L^m$ to the product of

$$1 + S_{K/L}(\varpi_K^{d'} x) + E^2(\varpi_K^{d'} x)$$

and

$$1 + S_{K/L}(\varpi_K^{d'} y) + E^2(\varpi_K^{d'} y)$$

and

$$1 - S_{K/L}(\varpi_K^{2d'} xy).$$

Thus

$$\varphi'_\lambda(x+y) = \varphi'_\lambda(x)\varphi'_\lambda(y)\psi_\lambda(\varepsilon xy).$$

Since

$$\frac{2d' + (\ell - 1)\,(t+1)}{\ell} \geq 2d$$

the number ε is in O_L. We conclude in particular that if y belongs to $\mathfrak{P}_K$ then

$$\varphi'_\lambda(x+y) = \varphi'_\lambda(x).$$

If $t = 0$ let σ be a generator of G and let $\varpi_K^{1-\sigma} = \nu$. In this case $2d' = 2d\ell$ and

$$\frac{\varpi_K^{2d'}}{\varpi_L^{2d}} = \left\{\prod\nolimits_{\tau\in G} \varpi_K^{1-\tau}\right\}^{2d} \equiv \nu^{d\ell(\ell-1)} \pmod{\mathfrak{P}_L}$$

and

$$\varepsilon \equiv \ell\nu^{d\ell(\ell-1)} \pmod{\mathfrak{P}_L}$$

is a unit. If $t > 0$

$$\varpi_K^{2d'} \equiv \varpi_L^{2d-t}\varpi_K^t \pmod{\mathfrak{P}_K}$$

so that

$$\varepsilon \equiv S_{K/L}\left(\frac{\varpi_K^t}{\varpi_L^t}\right) \pmod{\mathfrak{P}_L}.$$

It is shown in paragraph V.3 of Serre's book that the right side of this congruence is a unit.

First take p odd and let

$$\varphi_\lambda(x) = \psi_\lambda\left(\frac{x^2}{2} + \alpha x\right) = \psi_\lambda\left(\frac{(x+\alpha)^2}{2}\right)\psi_\lambda\left(\frac{-\alpha^2}{2}\right).$$

Then

$$\sigma(\varphi_\lambda) = -\psi_\lambda\left(\frac{-\alpha^2}{2}\right)\sum\psi_\lambda\left(\frac{(x+\alpha)^2}{2}\right) = -\psi_\lambda\left(\frac{-\alpha^2}{2}\right)\sum\psi_\lambda\left(\frac{x^2}{2}\right).$$

Making use of the calculations in the proof of Lemma 9.2 we see that

$$A[\sigma(\varphi_\lambda)]^\ell = \nu_\lambda(-1)^{\frac{\ell-1}{2}}\psi_\lambda\left(\frac{-\ell\alpha^2}{2}\right) A\left[-\sum\nolimits_\lambda \psi_\lambda\left(\frac{x^2}{2}\right)\right]$$

of ν_λ is the non-trivial quadratic character of $\lambda^\times$.

Since

$$1 + S_{K/L}\left(\varpi_K^{d'}x\right) + E^2(\varpi_K^{d'}x)$$

is congruent to

$$\{1 + S_{K/L}(\varpi_K^{d'}x)\}\ \{1 + E^2(\varpi_K^{d'}x)\}$$

modulo $\mathfrak{P}_L^m$ the value of $\varphi'_\lambda(x)$ is

$$\psi_\lambda\left(\frac{(S_{K/L}y)^2 + 2\alpha\, S_{K/L}y - 2E^2(y)}{2}\right)$$

if

$$y = \frac{\varpi_K^{d'}}{\varpi_L^d}x.$$

Thus

$$\varphi'_\lambda(x) = \psi_\lambda\left(\frac{(S_{K/L}(y+\alpha)^2) - \ell\alpha^2}{2}\right).$$

Replacing x by

$$x-\frac{\varpi_L^d}{\varpi_K^{d'}}\alpha$$

and summing we find that

$$\sigma(\varphi'_\lambda)=\psi_\lambda\,\left(\frac{-\ell\alpha^2}{2}\right)\,\left\{-\sum\nolimits_x\psi_\lambda\,\left(\frac{\varepsilon x^2}{2}\right)\right\}.$$

Collecting this information together we see that to prove the lemma when the residual characteristic p is odd we must show that

$$\nu_\lambda(-1)^{\frac{\ell-1}{2}}=\nu_\lambda(\varepsilon).$$

Since $\nu^{d\ell(\ell-1)}$ is certainly a square we have to show that

$$\nu_\lambda(-1)^{\frac{\ell-1}{2}}=\nu_\lambda(\ell)$$

when $t=0$. If the field λ is of even degree over the prime field both sides are 1. If not, an odd power of p is congruent to 1 modulo ℓ and the relation follows from the law of quadratic reciprocity. If $t>0$ then

$$\varepsilon\equiv S_{K/L}\,\left(\frac{\varpi_K^t}{\varpi_L^t}\right)\pmod{\mathfrak{P}_L}$$

and we can appeal to paragraph V.3 for a proof that

$$\varepsilon+u^{p-1}\equiv 0$$

has a solution in λ. Thus $\nu_\lambda(\varepsilon)=\nu_\lambda(-1)$ and we have to show that

$$\nu_\lambda(-1)^{\frac{p-3}{2}}=1.$$

If $p\equiv 1\pmod 4$ then $\nu_\lambda(-1)=1$ and if $p\equiv 3\pmod 4$ the exponent is even.

Before considering the case $p=2$, we remark a simple consequence of the preceding discussion.

Lemma 9.8

If p is odd let

$$\varphi_\lambda(x) = \psi_\lambda \left(\frac{x^2}{2} + \alpha x\right).$$

If $t = 0$ and

$$\mu = \nu^{d\ell\frac{(\ell-1)}{2}}$$

then

$$\varphi'_\lambda \left(\frac{x}{\mu}\right) = \psi_\lambda \left(\ell \left(\frac{x^2}{2} + \alpha x\right)\right)$$

and if $t > 0$

$$\varphi'_\lambda(x) = \psi_\lambda \left(\frac{\varepsilon x^2}{x}\right).$$

In both cases

$$\varphi'_\lambda(x) = \psi_\lambda \left(\frac{(S_{K/L}\,(y+\alpha)^2) - \ell\alpha^2}{2}\right)$$

with

$$y = \frac{\varpi_K^{d'}}{\varpi_L^d} x.$$

If $t = 0$ then $y = \mu x$. Thus if x belongs to O_L, as we may assume,

$$\varphi'_\lambda \left(\frac{x}{\mu}\right) = \psi_\lambda \left(\frac{\ell(x+\alpha)^2 - \ell\alpha^2}{2}\right) = \psi_\lambda \left(\ell \left(\frac{x^2}{2} + \alpha x\right)\right).$$

If $t > 0$ then $\ell = p$ is odd and

$$\frac{d'\ell d + (\ell-1)\,(t+1)}{\ell} = \frac{1}{\ell} \left\{(\ell-1)\,(t-1) - \frac{(\ell-1)}{2}\,t\right\} = \frac{1}{\ell} \left\{(\ell-1) + \frac{(\ell-1)}{2}\,t\right\} \geq 1$$

so that, if $x \in O_F$,

$$S_{K/L}(y+\alpha)^2 \equiv \varepsilon x^2 \pmod{\mathcal{P}_L}.$$

Now take $p = 2$ so that t is necessarily 0 and again let

$$\mu = \nu^{d\ell\frac{(\ell-1)}{2}}$$

so that

$$\frac{\varpi_K^{d'}}{\varpi_L^d} \equiv \mu \pmod{\mathcal{P}_K}.$$

If x is in O_L and $y = \frac{x}{\mu}$ then

$$\varphi'_\lambda \left(\frac{x}{\mu}\right) = \varphi'_\lambda(y)$$

is equal to

$$\psi_L \left(\frac{\ell\, x}{\varpi_L^{d+1+n}}\right) \chi_L^{-1} \left(1 + \ell\, \varpi_L^d x + \frac{\ell(\ell-1)}{2}\, \varpi_L^{2d} x^2\right).$$

Since
$$1+\ell\varpi_L^d x+\frac{\ell(\ell-1)}{2}\,\varpi_L^{2d}x^2\equiv(1+\ell\varpi_L^d x)\left(1+\frac{\ell(\ell-1)}{2}\,\varpi_L^{2d}x^2\right)$$
modulo $\mathfrak{P}_L^m$ we have
$$\varphi'_\lambda\left(\frac{x}{\mu}\right)=\varphi_\lambda(\ell\,x)\,\psi_\lambda\left(\frac{-\ell(\ell-1)}{2}\,x^2\right)$$
which equals
$$\{\varphi_\lambda(x)\}^\ell.$$
Moreover
$$\{\varphi_\lambda(x)\}^2=\varphi_\lambda(2x)\,\psi_\lambda(-x^2)=\psi_\lambda(-x^2).$$
Since the characteristic is 2 there is an $\alpha\neq 0$ such that
$$\psi_\lambda(x^2)=\psi_\lambda(\alpha x).$$
Then the complex conjugate of $\varphi_\lambda(x)$ is
$$\varphi_\lambda(x)\psi_\lambda(\alpha x)$$
and
$$\sigma(\varphi_\lambda)=-\sum\nolimits_x\varphi_\lambda(x+\alpha)$$
which equals
$$-\sum\nolimits_x\varphi_\lambda(x)\varphi_\lambda(\alpha)\psi_\lambda(\alpha x)$$
is equal to
$$\varphi_\lambda(\alpha)\;\overline{\sigma(\varphi_\lambda)}.$$
Consequently
$$A[\sigma(\varphi_\lambda)]^\ell=\varphi_\lambda(\alpha)^{\frac{\ell-1}{2}}\;A[\sigma(\varphi_\lambda)].$$
Since
$$\{\varphi_\lambda(x)\}^4=1$$
we have
$$A[\sigma(\varphi'_\lambda)]=A[\sigma(\varphi_\lambda)]$$
if $\ell\equiv 1\,(\mathrm{mod}\,4)$ and
$$A[\sigma(\varphi'_\lambda)]=A[\overline{\sigma(\varphi_\lambda)}]=\varphi_\lambda^{-1}(\alpha)\;A[\sigma(\varphi_\lambda)]$$
if $\ell\equiv 3\pmod 4$.

We have to show that
$$\varphi_\lambda(\alpha)^{\frac{\ell-1}{2}}=1$$
if $\ell\equiv 1\pmod 4$ and that
$$\varphi_\lambda(\alpha)^{\frac{\ell+1}{2}}=1$$
if $\ell\equiv 3\pmod 4$. These relations are clear if ℓ is congruent to 1 or 7 modulo 8. In general if $\ell\equiv 1\pmod 4$
$$\varphi_\lambda(\alpha)^{\frac{\ell-1}{2}}=\psi_\lambda\left(-\frac{(\ell-1)\,(\ell-3)}{8}\alpha^2\right)$$

and if $\ell \equiv 3 \pmod 4$

$$\varphi_\lambda(\alpha)^{\frac{\ell+1}{2}} = \psi_\lambda \left(-\frac{(\ell+1)(\ell-1)}{8}\alpha^2\right).$$

Let ϕ be the prime field and let ψ_ϕ be its non-trivial additive character. Choose α_1 such that

$$\psi_{\lambda/\phi}(x) = \psi_\lambda(\alpha_1^2 x).$$

Then

$$\psi_\lambda(x^2) = \psi_{\lambda/\phi}\left(\frac{x^2}{\alpha_1^2}\right) = \psi_{\lambda/\phi}\left(\frac{x}{\alpha_1}\right) = \psi_\lambda(\alpha_1 x)$$

and $\alpha = \alpha_1$. Thus

$$\psi_\lambda(\alpha^2) = \psi_{\lambda/\phi}(1).$$

The right side is +1 or –1 according as $f = [\lambda : \phi]$ is even or odd. But ℓ divides $2^f - 1$ so that, by the second supplement to the law of quadratic reciprocity, f is even if ℓ is congruent to 3 or 5 modulo 8.

There is a complement to Lemma 9.7.

Lemma 9.9

If $m(\chi_L) \geq 2(t+1)$ choose $\beta(\chi_{K/L}) = \beta(\chi_L) = \beta$ in O_L. If $t+1 < m(\chi_L) < 2(t+1)$ choose $\beta(\chi_L) = \beta$ and

$$\beta(\chi_{K/L}) = \beta - \beta_1 \frac{\alpha}{\alpha_1}$$

as in Lemma 8.9. Then $m(\chi_{K/L}) = 2d' + 1$ and

$$\psi_{K/L}\left(\frac{\beta(\chi_{K/L})\,\varpi_K^{d'} x}{\varpi_L^{m+n}}\right) \chi_{K/L}^{-1}(1 + \varpi_K^{d'} x)$$

is equal to

$$\psi_{K/L}\left(\frac{\beta\,\varpi_K^{d'} x}{\varpi_L^{m+n}}\right) \chi_L^{-1}(1 + S_{K/L}(\varpi_K^{d'} x) + E^2(\varpi_K^{d'} x)).$$

From Lemma 8.8 we have

$$m(\chi_{K/L}) = 1 + t + \ell(m - 1 - t) = 2\left(\ell\, d - \frac{(\ell-1)}{2}\, t\right) + 1$$

as required. If $d \geq t+1$ then

$$d' \geq \frac{(\ell+1)}{2}\, d + \frac{(\ell-1)}{2}\,(d-t) \geq m$$

because ℓ is odd. Moreover,

$$\frac{3d' + (\ell-1)(t+1)}{\ell} \geq \frac{m' + (\ell-1)(t+1)}{\ell} = m.$$

Consequently
$$N_{K/L}(1+\varpi_K^{d'}x) \equiv 1 + S_{K/L}(\varpi_K^{d'}x) + E^2(\varpi_K^{d'}x) \pmod{\mathfrak{P}_L^m}$$
and the lemma is valid if $m \geq 2(t+1)$.

If $t+1 < m < 2(t+1)$ we still have
$$\frac{3d' + (\ell-1)\,(t+1)}{\ell} \geq m$$
so that
$$N_{K/L}(1+\varpi_K^{d'}x)$$
is congruent to
$$1 + S_{K/L}(\varpi_K^{d'}x) + E^2(\varpi_K^{d'}x) + N_{K/L}(\varpi_K^{d'}x)$$
modulo $\mathfrak{P}_L^m$. Since $d' \geq d+1$ this is congruent to
$$\{1 + S_{K/L}(\varpi_K^{d'}x) + E^2(\varpi_K^{d'}x)\}\;\{1 + N_{K/L}(\varpi_K^{d'}x)\}$$
modulo $\mathfrak{P}_L^m$. Certainly
$$\chi_L(1 + N_{K/L}(\varpi_K^{d'}x)) = \psi_L\;\left(\frac{\beta\, N_{K/L}(\varpi_K^{d'}x)}{\varpi_L^{m+n}}\right).$$
Moreover, if $m = t+1+v$
$$d' - v = d + \frac{\ell-3}{2}\;v \geq d \geq s$$
if s is the least integer greater than or equal to $\frac{t}{2}$. Thus, just as in the proof of Lemma 8.5,
$$\psi_L\;\left(\frac{\beta\, N_{K/L}(\varpi_K^{d'}x)}{\varpi_L^{m+n}}\right) = \psi_L\;\left(\frac{\alpha\, N_{K/L}\;\left(\frac{\beta_1}{\alpha_1}\;\varpi_K^{d'}x\right)}{\varpi_L^{m+n}}\right)$$
is equal to
$$\psi_L\;\left(\frac{-S_{K/L}\;\left(\frac{\alpha\beta_1}{\alpha_1}\;\varpi_K^{d'}x\right)}{\varpi_L^{m+n}}\right).$$
Multiplying the inverse of this with
$$\psi_{K/L}\;\left(\left(\beta - \frac{\alpha\beta_1}{\alpha_1}\right)\;\frac{\varpi_K^{d'}x}{\varpi_L^{m+n}}\right)$$
we obtain
$$\psi_{K/L}\;\left(\frac{\beta\,\varpi_K^{d'}x}{\varpi_L^{m+n}}\right).$$
The lemma follows.

If $m = t + 1$ we may still choose

$$\beta(\chi_{K/L}) = \beta - \beta_1 \; \frac{\alpha}{\alpha_1}$$

as in Lemma 8.9. However the relation between $\varphi_\lambda(x)$ and

$$\varphi_K(x) = \psi_{K/L} \; \left(\frac{\beta(\chi_{K/L})\, \varpi_K^{d'} x}{\varpi_L^{m+n}} \right) \chi_{K/L}^{-1} \, (1 + \varpi_K^{d'} x)$$

will be more complicated. Here $x = O_K/\mathfrak{P}_K$ is the same field as $\lambda = O_L/\mathfrak{P}_L$. We introduce it only for notational purposes.

Because $m = t + 1$ the number t is at least 2 and

$$d = d' = \frac{t}{2}.$$

Since

$$\frac{3d + (p-1)\,(t+1)}{p} \geq t + 1$$

and

$$\frac{d + (p-1)\,(t+1)}{p} \geq d + 1$$

the expression

$$N_{K/L}(1 + \varpi_K^d x)$$

is congruent to

$$\{1 + S_{K/L}(\varpi_K^d x) + E^2(\varpi_K^d x)\} \; \{1 + \varpi_L^d \, N_{K/L} x\}$$

modulo $\mathfrak{P}_L^m$ and

$$\chi_L(1 + S_{K/L}(\varpi_K^d x) + E^2(\varpi_K^d x))$$

is equal to

$$\Psi_L \; \left(\frac{\beta\, S_{K/L}(\varpi_K^d x) + \beta\, E^2(\varpi_K^d x)}{\varpi_F^{m+n}} \right).$$

According to Newton's formulae

$$S_{K/L}(\varpi_K^{2d} x^2) - S_{K/L}(\varpi_K^d x)^2 + 2E^2(\varpi_K^d x) = 0.$$

Thus

$$E^2(\varpi_K^d x) \equiv -\, \frac{1}{2} \; S_{K/L}(\varpi_K^{2d} x^2) \pmod{\mathcal{P}_L^m}.$$

Observe that p is equal to ℓ and therefore, in the present circumstances, odd.

Let μ_L be a character in $S(K/L)$ as in Lemma 8.9(c) and let

$$\psi_L \; \left(\frac{\alpha\, x}{\varpi_L^{d+1+n}} \right) \; \mu_L^{-1}(1 + \varpi_L^d x) = \psi_\lambda \; \left(\rho \; \frac{x^2}{2} + \tau\, x \right)$$

with

$$\rho = \frac{\alpha}{\beta}.$$

Certainly

$$\mu_L(N_{K/L}(1+\varpi_K^d x)) = 1$$

if x belongs to O_K. Replacing x by $\frac{\beta_1}{\alpha_1}\,x$ we see that

$$\psi_L\ \left(\frac{1}{\varpi_L^{m+n}}\left\{\alpha\, S_{K/L}\left(\frac{\beta_1}{\alpha_1}\,\varpi_K^d x\right) -\ \frac{\alpha}{2}\ S_{K/L}\ \left(\frac{\beta_1^2}{\alpha_1^2}\,\varpi_K^{2d}x^2\right) + N_{K/L}\ \left(\beta_1\,\varpi_K^d x\right)\right\}\right)$$

is equal to

$$\psi_\lambda\ \left(\rho\,\frac{z^2}{2} + \tau\, z\right)$$

if

$$z = \frac{1}{\varpi_L^d}\ \left\{S_{K/L}\ \left(\frac{\beta_1}{\alpha_1}\ \varpi_K^d x\right) - \frac{1}{2}\ S_{K/L}\ \left(\frac{\beta_1^2}{\alpha_1^2}\,\varpi_K^{2d}x^2\right) + N_{K/L}\ \left(\frac{\beta_1}{\alpha_1}\,\varpi_K^d x\right)\right\}$$

which is congruent to

$$\frac{\beta}{\alpha}\ N_{K/L}x \equiv \frac{\beta}{\alpha}\,x^p$$

modulo $\mathfrak{P}_L$.

Let

$$\varphi_\lambda(x) = \psi_L\ \left(\frac{\beta\, x}{\varpi_L^{d+1+n}}\right)\ \chi_L^{-1}\,(1+\varpi_L^d x)$$

equal

$$\psi_\lambda\ \left(\frac{x^2}{2} + \sigma\, x\right).$$

If x belongs to O_K

$$\chi_L^{-1}\ \left(1+\varpi_L^d\, N_{K/L}x\right) = \psi_\lambda\ \left(\frac{x^{2p}}{2} + \sigma\, x^p\right)\ \psi_L\ \left(\frac{-\beta\, N_{K/L}x}{\varpi_L^{d+1+n}}\right).$$

We now put these facts together to find a suitable expression for $\varphi_\kappa(x)$. We may as well take x in O_L. Then $\varphi_\kappa(x)$ is the product of

$$\psi_{K/L}\ \left(\frac{\beta\,\varpi_K^{d'}x}{\varpi_L^{m+n}}\right)$$

and

$$\psi_{K/L}\ \left(-\ \frac{\beta_1\alpha}{\alpha_1}\ \frac{\varpi_K^d x}{\varpi_L^{m+n}}\right)\ \chi_L^{-1}\,(1+\varpi_L^d\, N_{K/L}x)$$

and

$$\psi_L\ \left(-\ \frac{\beta}{\varpi_L^{m+n}}\ \left\{S_{K/L}(\varpi_K^d x) - \frac{1}{2}\ S_{K/L}(\varpi_K^{2d}x^2)\right\}\right).$$

The second of these three expressions is equal to the product of

$$\psi_\lambda\ \left(\frac{x^{2p}}{2}+\sigma\, x^p\right)\ \psi_\lambda\ \left(-\rho^{-1}\ \frac{x^{2p}}{2}-\rho^{-1}\tau\, x^p\right)$$

and

$$\psi_{K/L}\ \left(-\ \frac{\alpha\beta_1^2\,\varpi_K^{2d}x^2}{2\alpha_1^2\,\varpi_L^{m+n}}\right)=\psi_\lambda\ \left(-\ \frac{\varepsilon\rho\beta_1^2}{2\alpha_1^2}\,x^2\right)$$

if

$$\varepsilon=S_{K/L}\ \left(\frac{\varpi_K^{2d}}{\varpi_L^{2d}}\right).$$

The product of the first and third is equal to

$$\psi_\lambda\ \left(\frac{\varepsilon\, x^2}{2}\right).$$

As proven in paragraph V.3 of Serre's book the elements of U_L congruent to

$$1+(\varepsilon\, x+x^p)\,\varpi_L^t$$

modulo $\mathfrak{P}_L^{t+1}$ are all norms, so that

$$\psi_\lambda(\rho\, x^p)=\psi_\lambda(-\rho\varepsilon\, x).$$

In particular

$$\psi_\lambda\ \left(-\ \frac{\varepsilon\rho\beta_1^2}{2\alpha_1^2}x^2\right)=\psi_\lambda\ \left(\rho^{-1}\ \frac{x^{2p}}{2}\right).^*$$

*(1998) The manuscript of Chapter 9 ends with this formula.

Chapter Eleven.

Artin–Schreier Equations

The theory of Artin–Schreier equations is central to Dwork's proof of the second main lemma. We first review the basic theory, which we take from Mackenzie and Whaples [11], and then review Dwork's rather amazing calculations. These we take from Lakkis [9].

We start with an exercise from Serre's book [12]. Suppose F is a non-archimedean local field and K/F is Galois. Let p be the residual characteristic. With the convention $(0) = \mathfrak{P}_F^\infty$ we let

$$p\,O_F = \mathfrak{P}_F^e.$$

Suppose $G = \mathfrak{G}(K/F)$ and $\sigma \in G_i$ with $i \geq 1$. Let

$$\varpi_K^\sigma = \varpi_K(1+a)$$

with a in $\mathfrak{P}_K^i$. Let

$$\varphi(x) = x^\sigma - x.$$

φ is an F-linear operator on K. If $x = \alpha\varpi_K^j$ belongs to $\mathfrak{P}_K^j$ then

$$\varphi(x) = x^\sigma - x = (\alpha^\sigma - \alpha)\,\varpi_K^{j\sigma} + \alpha(\varpi_K^{j\sigma} - \varpi_K)$$

is congruent to

$$\alpha\varpi_K^j\,\left(\varpi_K^{j(\sigma-1)} - 1\right) = \alpha\varpi_K^j\,\{(1+a)^j - 1\}$$

modulo $\mathfrak{P}_K^{i+j+1}$. This in turn is congruent to

$$(\alpha\,\varpi_K^j)\,(ja) = jax$$

modulo $\mathfrak{P}_K^{i+j+1}$.

If*

$$\psi(x) = x^{\sigma^p} - 1$$

then, as an operator,

$$\psi = (1+\varphi)^p - 1 = \sum\nolimits_{k=1}^{p} \binom{p}{k}\,\varphi^k.$$

If x belongs to $\mathfrak{P}_K^j$ then

$$\varphi^k(x) \equiv j(j+i)\ldots(j+(k-1)i)a^k x \pmod{\mathfrak{P}_K^{j+ki+1}}$$

and $\psi(x)$ is congruent to

$$pjax + j(j+i)\ldots(j+(p-1)i)a^p x$$

* We seem to be dealing with yet another use of the symbol ψ!

or to

$$pjax + j(j^{p-1} - i^{p-1})a^p x$$

modulo $\mathfrak{P}_K^{i+j+e'+1}$ if $pO_K = \mathfrak{P}_K^{e'}$.
We deduce the following congruences:

(i) If $(p-1)i > e'$ then
$$\psi(x) \equiv pjax \pmod{\mathfrak{P}_K^{i+j+e'+1}}.$$

(ii) If $(p-1)i = e'$ then

$$\psi(x) \equiv pjax + j(1 - i^{p-1})a^p x \pmod{\mathfrak{P}_K^{i+j+e'+1}}.$$

(iii) If $(p-1)i < e'$ then
$$\psi(x) \equiv j(1 - i^{p-1})a^p x \pmod{\mathfrak{P}_K^{pi+j+1}}.$$

Observe that if $(j,p) = 1$ and σ belongs to G_i, with $i \geq 1$, then

$$\varphi(x) \equiv 0 \pmod{\mathfrak{P}_K^{i+j+1}}$$

for all x in $\mathfrak{P}_K^j$ if and only if σ belongs to G_{i+1}. It follows immediately that if σ belongs to G_1 and $i \geq 1$ then
$$\varphi(x) \equiv 0 \pmod{\mathfrak{P}_K^{i+j}}$$

for all x in $\mathfrak{P}_K^j$ only if σ belongs to G_i.

If σ is replaced by σP then φ is replaced by ψ. If $k > \frac{e'}{p-1}$ and $G_k \neq \{1\}$ then, for some $i \geq k$, $G_i \neq \{1\}$ and $G_{i+1} = \{1\}$. Taking $(j,p) = 1$ we infer from (i) that if σ belongs to G_i but not to G_{i+1} then σ^p is in $G_{i+e'}$ but not in $G_{i+e'+1}$. This is impossible. Thus $G_k = \{1\}$ if $k > \frac{e'}{p-1}$. If $G_1 \neq \{1\}$ then p divides e' so that if $(p-1)i = e'$ the number i is also divisible by p. The congruence (ii) reduces to
$$\psi(x) \equiv j\,(pa + a^p) \pmod{\mathfrak{P}_K^{i+j+e'+1}}.$$

Thus if σ belongs to G_i its pth power σ^p lies in G_{i+e} and is therefore 1. Consequently

$$pa + a^p \equiv 0 \pmod{\mathfrak{P}_K^{pi+1}}.$$

Letting $a = \alpha\varpi_K^i$ and $p = \beta\varpi_K^e$ we find that

$$\alpha^p + \beta\alpha \equiv 0 \pmod{\mathfrak{P}_K}.$$

Since this congruence has only p roots the image of Θ_i lies in a subset of U_K^i/U_K^{i+1} with p elements and G_i is either $\{1\}$ or cyclic of order p.

If $(p-1) < e'$ and $(i,p) = 1$ the congruence (iii) implies that σ^p belongs to G_{pi+1} if σ belongs to G_i. However if $(p-1)i < e'$ and p divides i it shows that σ^p belongs to G_{pi} but not to G_{pi+1} if σ belongs to G_i but not to G_{i+1}. Thus $\sigma \longrightarrow \sigma^p$ defines an injection of G_i/G_{i+1} into G_{pi}/G_{pi+1}. If G_i/G_{i+1} is not trivial neither is G_{pi}/G_{pi+1} and $(p-1)pi \leq e'$. If $(p-1)pi < e'$ we can repeat the process. Thus, for some positive integer h, $(p-1)p^h i = e'$ and $G_{p^h i}$ is not trivial. It is then cyclic of order p. According to Proposition IV.10 of Serre's book those $k \geq 1$ for which $G_k/G_{k+1} \neq \{1\}$ are all congruent modulo p. In particular if G_k/G_{k+1} is not trivial for some $k \geq 1$ divisible by p it is not trivial only when k is divisible by p. The preceding discussion shows that if i is the smallest value of $k \geq 1$ for which G_k/G_{k+1} is non-trivial then any σ in G_i but not in G_{i+1} generates $G_i = G_1$. In other words:

Lemma 11.1

If G_1 is not cyclic then $(i,p) = 1$ if $i \geq 1$ and $G_i/G_{i+1} \neq \{1\}$.

Lemma 11.2

Suppose K/L is cyclic of prime degree and $G = \mathfrak{G}(K/L)$ is equal to G_L with $t \geq 1$ and $(t,p) = 1$. Then there is a Δ in K and an a in L such that $aO_L = \mathfrak{P}_L^{-t}$ and

$$\Delta^p - \Delta = a.$$

We observe first of all that $[K : L]$ must be p and that if $pO_K = \mathcal{P}_K^{e'}$ then $(p-1)t < e'$. If x belongs to K the symbol $O(x)$ will stand for an element in xO_K and the symbol $o(x)$ will stand for an element in $x\mathfrak{P}_K$. If

$$x = \sum_{i=0}^{p-1} a_i \,\varpi_K^i$$

with a_i in F then

$$|x| = \max_{0 \leq i < p} |a_i| \, |\varpi_K^i|.$$

Moreover if σ is a generator of G

$$x^\sigma - 1 = \sum_{i=1}^{p-1} a_i \,\varpi_K^i \,(\varpi_K^{i(\sigma-1)} - 1)$$

and if $\varpi_K^{\sigma-1} = (1 + a\varpi_K^t)$

$$|\varpi_K^{i(\sigma-1)} - 1| = |\,(1 + a\varpi_K^t)^i - 1| = |\varpi_K^t|$$

for $1 \leq i < p$. Thus

$$|x^\sigma - x| = |\varpi_K^t| \left\{ \max_{1 \leq i < p} \; |a_i| \; |\varpi_K^i| \right\} \leq |\varpi_K^t| \; |x|.$$

There is equality if $a_0 = 0$. In particular if

$$y = \sum_{i=1}^{p-1} a_i \,\varpi_K^i$$

then

$$x^\sigma - 1 = y^\sigma - 1$$

and

$$|y^\sigma - x| = |\varpi_K^t| \; |y|.$$

If x belongs to K let

$$\mathfrak{p}(x) = x^p - x.$$

Then

$$\mathfrak{p}(x+y) - \mathfrak{p}(x) - \mathfrak{p}(y) = \sum_{i=1}^{p-1} \binom{p}{i} \; x^i y^{p-i} \tag{11.1}$$

Since $e' - (p-1)t > 0$ the right side is $o(y)$ if

$$v_K(x) \geq -t$$

and

$$v_K(y) \geq -t.$$

We define $v_K(x)$ by the equation

$$|x| = |\varpi_K|^{v_K(x)}.$$

To prove the lemma we construct a sequence $\Lambda_0,\ \Lambda_1,\ \Lambda_2, \ldots$ and a sequence $\Theta_0,\ \Theta_1, \ldots$ with the following properties:

(i) $v_K(\Lambda_n) = -t$ for all $n \geq 0$.

(ii) If σ is a given generator of G and ζ is a given $(p-1)$th root of unity

$$\Lambda_n^\sigma - \Lambda_n = \zeta + o(1).$$

(iii)

$$\mathfrak{p}(\Lambda_n^\sigma) - \mathfrak{p}(\Lambda_n) = \Theta_n^\sigma - \Theta_n$$

and

$$|\Theta_n^\sigma - \Theta_n| = |\varpi_K^t|\ |\Theta_n|.$$

(iv)

$$\Lambda_{n+1} = \Lambda_n + \Theta_n.$$

(v)

$$\mathfrak{p}(\Lambda_{n+1}^\sigma) - \mathfrak{p}(\Lambda_{n+1}) = o(\mathfrak{p}(\Lambda_n^\sigma) - \mathfrak{p}(\Lambda_n)).$$

It will follow from (iii) and (v) that $\{\Theta_n\}$ is converging to 0. Then (iv) implies that $\{\Lambda_n\}$ has a limit Δ. (i) implies that $v_K(\Delta) = -t$ and (v) implies that $\Delta^p - \Delta = a$ belongs to F. From (ii)

$$\Delta^\sigma - \Delta = \zeta + o(1).$$

To construct Λ_0 let α belong to U_K^i and consider

$$\frac{\alpha^\sigma}{\varpi_K^{\sigma\,t}} - \frac{\alpha}{\varpi_K^t} = \frac{\alpha^\sigma - \alpha}{\varpi_K^{\sigma\,t}} + \frac{\alpha}{\varpi_K^t}\ \left(\varpi_K^{t(1-\sigma)} - 1\right) = -ta\alpha + o(1)$$

if

$$\varpi_K^\sigma = \varpi_K(1 + a\varpi_K^t).$$

We can choose α so that

$$-ta\alpha = \zeta + o(1).$$

Then we set

$$\Lambda_0 = \frac{\alpha}{\varpi_K^t}.$$

We observe in passing that conditions (i) and (ii) determine Λ_n modulo $\mathfrak{P}_K^{-t+1}$.

Suppose $\Lambda_0, \ldots, \Lambda_n$ have been defined. Then

$$\mathfrak{p}(\Lambda_n^\sigma) = \mathfrak{p}(\Lambda_n) + \mathfrak{p}(\zeta + o(1)) + o(1)$$

which equals

$$\mathfrak{p}(\Lambda_n) + \mathfrak{p}(\zeta) + o(1) = \mathfrak{p}(\Lambda_n) + o(1).$$

Choose Θ_n so that

$$\Theta_n^\sigma - \Theta_n = \mathfrak{p}(\Lambda_n^\sigma) - \mathfrak{p}(\Lambda_n)$$

and

$$|\Theta_n^\sigma - \Theta_n| = |\varpi_K^t|\ |\Theta_n|.$$

Then $v_K(\Theta_n) > -t$ and if

$$\Lambda_{n+1} = \Lambda_n + \Theta_n$$

$v_K(\Lambda_{n+1}) = -t$. Moreover

$$\Lambda_{n+1}^\sigma - \Lambda_{n+1} = \Lambda_n^\sigma - \Lambda_n + o(1) = \zeta + o(1).$$

and

$$\mathfrak{p}(\Lambda_{n+1}) = \mathfrak{p}(\Lambda_n) + \mathfrak{p}(\Theta_n) + x$$

with $x = o(\Theta_n)$. Then

$$x^\sigma - x = o(\Theta_n^\sigma - \Theta_n) = o(\mathfrak{p}(\Lambda_n^\sigma) - \mathfrak{p}(\Lambda_n)).$$

Also

$$\mathfrak{p}(\Theta_n^\sigma) - \mathfrak{p}(\Theta_n) = \mathfrak{p}(\Theta_n^\sigma - \Theta_n) + o(\Theta_n^\sigma - \Theta_n).$$

Since $v_K(\Theta_n^\sigma - \Theta_n)$ is positive the right side is

$$-(\Theta_n^\sigma - \Theta_n) + o(\Theta_n^\sigma - \Theta_n).$$

Thus

$$\mathfrak{p}(\Lambda_{n+1}^\sigma) - \mathfrak{p}(\Lambda_{n+1})$$

which equals

$$\mathfrak{p}(\Lambda_n^\sigma) - \mathfrak{p}(\Lambda_n) - (\Theta_n^\sigma - \Theta_n) + o(\mathfrak{p}(\Lambda_n^\sigma) - \mathfrak{p}(\Lambda_n))$$

is

$$o(\mathfrak{p}(\Lambda_n^\sigma) - \mathfrak{p}(\Lambda_n)).$$

Lemma 11.3

Supposer Δ_1 belongs to K, a belongs to L, $v_L(a) = -t$ and

$$\Delta_1^p - \Delta_1 = a + O(\varpi_K^r)$$

with $r \geq 1$. Define Δ_n inductively by

$$\Delta_{n+1} = \Delta_n^p - a.$$

Then

$$\Delta_{n+1} - \Delta_n = o(\Delta_n - \Delta_{n-1})$$

if $n \geq 2$ *and if* $r \geq (e' - (p-1)t)$

$$\Delta_{n+1} - \Delta_n = O(\varpi_K^{r+(n-1)\,(e'-(p-1)t)}).$$

Moreover

$$\lim_{n\to\infty} \Delta_n = \Delta$$

exists and $\Delta^p - \Delta = a$*.*

The last assertion is a consequence of the first. It is clear that

$$\Delta_2 - \Delta_1 = O(\varpi_K^r).$$

Suppose $n \geq 2$, and

$$\Delta_n - \Delta_{n-1} = x = o(1).$$

Then

$$\Delta_{n+1} - \Delta_n = \Delta_n^p - \Delta_{n-1}^p = (\Delta_{n-1} + x)^p - \Delta_{n-1}$$

is equal to

$$\left\{\sum\nolimits_{k=1}^{p-1} \binom{p}{k} \Delta_{n-1}^k\, x^{p-k}\right\} + x^p$$

which is $o(x)$ because $e' - (p-1)t > 0$. If

$$x = O(\varpi_K^{r+(n-2)\,(e'-(p-1)t)})$$

and $r \geq e' - (p-1)t$ it is

$$O(\varpi_K^{r+(n-1)\,(e'-(p-1)t)}).$$

The lemma has a couple of corollaries which should be remarked.

Lemma 11.4

If a *is in* L, $v_L(a) = -t$, $\Delta^p - \Delta = a$*, and* ξ *is a* $(p-1)$*th root of unity there is a number* Δ_ξ *such that*

$$\Delta_\xi = \Delta + \xi + O(\varpi_K^{e'-(p-1)t})$$

and

$$\Delta_\xi^p - \Delta_\xi = a.$$

Relation (11.1) shows that $\Delta+\xi$ satisfies the conditions of the previous lemma with $r = e' - (p-1)t$.

Lemma 11.5

Suppose Δ *belongs to* K*,* b *belongs to* L, $v_L(b) = -t$ *and*

$$\Delta^p - \Delta = b.$$

Then for any u *in* U_L^{t+1} *the equation*

$$\Lambda^p - \Lambda = bu$$

has a solution in K*.*

Take, in Lemma 11.3, $a = bu$ and $\Delta_1 = \Delta$. Lemma 11.5 shows that if S is the set of all in L with $v_L(a) = -t$ for which the equation

$$\Delta^p - \Delta = a$$

has a solution in K then $S = SU_L^{t+1}$.

Lemma 11.6

If ℓ is the integral part of $\frac{t}{p}$ the number of cosets of U_L^{t+1} in S is

$$\frac{p-1}{p}\,[O_L : \mathfrak{P}_L]^{1+\ell}.$$

Fix a generator σ of $G = \mathfrak{G}(K/L)$. If a belongs to S, $\Delta^p - \Delta = a$, and ξ is a $(p-1)$th root of unity

$$(\xi\Delta)^p - \xi\Delta = \xi\, a.$$

By Lemma 11.4 there is a $(p-1)$th root of unity ζ such that

$$\Delta^\sigma = \Delta + \zeta + o(1).$$

Then

$$(\xi\Delta)^\sigma = \xi\Delta + \xi\zeta + o(1).$$

Thus if S' is the set of a in L with $v_L(a) = -t$ for which

$$a = \Delta^p - \Delta$$

with

$$\Delta^\sigma = \Delta + 1 + o(1)$$

the number of cosets if U_L^{t+1} in S is $p-1$ times the number of cosets of U_L^{t+1} in S'.

Choose Δ_0, with $v_K(\Delta_0) = -t$, for which $\Delta_0^p - \Delta_0 = a_0$ is in F and

$$\Delta_0^\sigma = \Delta_0 + 1 + o(1).$$

If $v_K(\Delta) = -t, \quad \Delta^p - \Delta$ is in F, and

$$\Delta^\sigma = \Delta + 1 + o(1)$$

then, according to an earlier remark,

$$\Delta = \Delta_0 + \Omega_0$$

with $\Omega_0 = o(\Delta_0)$.

Choose any $\Omega_0 = o(\Delta_0)$ and set $\Lambda_0 = \Delta_0 + \Omega_0$. According to the relation (A)

$$\mathfrak{p}(\Lambda_0) = \mathfrak{p}(\Delta_0) + \mathfrak{p}(\Omega_0) + o(\Omega_0).$$

Since

$$\Omega_0^\sigma - \Omega_0 = O(\varpi_K^t \Omega_0) = o(1)$$

we have
$$\Omega_0^{\sigma\,p} - \Omega_0^p = \sum\nolimits_{i=1}^{p-1} \binom{p}{i} \Omega_0^{p-i}(\Omega_0^\sigma - \Omega_0)^i = o(\Omega_0^\sigma - \Omega_0).$$
Thus
$$\mathfrak{p}(\Lambda_0)^\sigma - \mathfrak{p}(\Lambda_0) = \Omega_0^\sigma - \Omega_0 + o(\varpi_K^t \Omega_0)$$
and $\mathfrak{p}(\Lambda_0)$ is in L only if
$$\Omega_0^\sigma - \Omega_0 = o(\varpi_K^t \Omega_0),$$
that is, only if $\Omega_0 = \alpha_0 + o(\Omega_0)$ with α_0 in L. On the other hand if
$$\Omega_0^\sigma - \Omega_0 = o(\varpi_K^t \Omega_0)$$
and we construct the sequence $\Lambda_0,\ \Lambda_1,\ \Lambda_2, \ldots$ as before and let
$$\Delta = \lim_{n\to\infty} \Lambda_n$$
then
$$\Delta = \Lambda_0 + o(\Omega_0).$$
We conclude that the number of cosets in $\mathfrak{P}_K^s/\mathfrak{P}_K^{s+1},\ s > -t$, containing an Ω_0 such that
$$(\Delta_0 + \Omega_0)^p - (\Delta_0 + \Omega_0)$$
is in L is 1 if p does not divide s and is $[O_L : \mathfrak{P}_L]$ if it does.

Choose Δ so that
$$\Delta^p - \Delta = a$$
is in S'. If Ω belongs to $\mathfrak{P}_K^s,\ s > -t$, but not to $\mathfrak{P}_K^{s+1}$ and
$$(\Delta + \Omega)^p - \Delta - \Omega = b$$
is also in S' then a and b belong to the same coset of U_L^{t+1} if and only if
$$b = a + o(1).$$
If $s > 0$
$$\mathfrak{p}(\Delta + \Omega) = \mathfrak{p}(\Delta) + o(1)$$
but if $s \le 0$
$$\mathfrak{p}(\Delta + \Omega) = \mathfrak{p}(\Delta) + \Omega^p - \Omega + o(\Omega)$$
and
$$\Omega^p - \Omega + o(\Omega) = o(1)$$
if and only if $s = 0$ and
$$\Omega = \xi + o(1)$$
where ξ is some $(p-1)$th root of unity. The lemma follows.

If $x = \{x_1, \dots, x_n\}$ let $E^i(x)$ be the ith elementary symmetric function of $x_1, \dots, x_n$ and let

$$S^i(x) = \sum\nolimits_{k=1}^{n} x_k^i.$$

If Z is an indeterminate and

$$Q(Z) = \sum\nolimits_{i=0}^{n} (-1)^i \, E^i(x) Z^i = \prod\nolimits_{i=1}^{n} (1 - x_i Z)$$

then

$$\sum\nolimits_{i=1}^{\infty} S^i(x) Z^i$$

is clearly $-Z$ times the logarithmic derivative of $Q(Z)$. Thus

$$\left(\sum\nolimits_{i=1}^{\infty} S^i(x)\, Z^i\right) \left(\sum\nolimits_{i=0}^{n} (-1)^i E^i(x) Z^i\right) = -\sum\nolimits_{i=0}^{n} (-1)^i \, i E^i(x) Z^i.$$

This identity which we refer to as Newton's identity is equivalent to the formulae of Newton. It implies in particular that

$$\sum\nolimits_{j=0}^{i-1} (-1)^j \, S^{i-j}(x) \, E^j(x) = (-1)^{i+1} \, i E^i(x) \tag{11.2}$$

if $1 \le i \le n$. We may divide Newton's identity by $Q(Z)$ and then expand the right-hand side to obtain expressions for the $S^i(x)$ as polynominals in $E^1(x), \dots, E^n(x)$. The coefficients are necessarily integers. To calculate them we suppose that $x_1, \dots, x_n$ lie in a field of characteristic zero. Let

$$Q(Z) = 1 + P(Z).$$

Then

$$\log Q(Z) = -\sum\nolimits_{k=1}^{\infty} \frac{(-1)^k}{k} \, (P(Z))^k.$$

The coefficient of Z^{i-1} in the derivative of the right side is

$$-\sum\nolimits_k \sum\nolimits_{\substack{\alpha_1 + \dots + \alpha_n = k \\ \alpha_1 + 2\alpha_2 + \dots + n\alpha_n = i}} \frac{i(k-1)!}{\alpha_1! \dots \alpha_n!} \prod\nolimits_{j=1}^{n} \{E^j(x)\}^{\alpha_j}.$$

This expression is therefore equal to $-S^i(x)$.

Suppose K/L is a ramified cyclic extension of degree p and $G = \mathfrak{G}(K/L)$. Let $G = G_t$ and $G_{t+1} = \{1\}$. Suppose $u \le t$, Λ is in K, and

$$\Lambda O_K = \mathfrak{P}_K^{-u}.$$

We take $\{x_1, \dots, x_n\}$ to be Λ and its conjugates under G. In this case we write

$$E^i(x) = E^i_{K/L}(\Lambda)$$

and

$$S^i(x) = S^i_{K/L}(\Lambda).$$

If $1 \leq i \leq p-1$ and γ_i is any integer less than or equal to

$$\frac{-iu + (p-1)\,(t+1)}{p}$$

we have

$$E^i_{K/L}(\Lambda) \equiv 0 \,(\mathrm{mod}\, \mathcal{P}_L^{\gamma_i}).$$

We may take

$$\gamma_i \geq -\frac{iu}{p} + \frac{(p-1)t}{p}.$$

If $iu + t$ is not divisible by p this inequality may be supposed strict.

Suppose $\alpha_1, \ldots, \alpha_p$ are non-negative integers,

$$\sum\nolimits_{i=1}^{p} \alpha_i = k$$

and

$$\sum\nolimits_{i=1}^{p} i\alpha_i = \ell.$$

If

$$\gamma = \left\{\sum\nolimits_{i=1}^{p-1} \gamma_i \alpha_i\right\} - u\alpha_p.$$

Then

$$\prod\nolimits_{i=1}^{p} \{E^i(\Lambda)\}^{\alpha_i} \equiv O\,(\varpi_K^{\gamma}). \tag{11.3}$$

We have

$$\gamma \geq -\frac{\ell\, u}{p} + \frac{(p-1)}{p}kt - \frac{(p-1)}{p}\alpha_p t.$$

The inequality is strict if α_i is non-zero for some i such that $iu + t$ is not divisible by p.

We record now some inequalities that γ satisfies in various special cases. They will be needed later. We observe first of all that, if $1 \leq i < p$, γ_i is non-negative and is positive unless p divides $iu + t$.

(i) If $\ell = p$ and $k = 2$ then

$$1 + u + \gamma \geq 1 + t.$$

In this case $\alpha_p = 0$ and the left side is at least

$$1 + \frac{2(p-1)}{p}\,t \geq 1 + t.$$

If p is odd the inequality is strict.

(ii) If $\ell = p$ and $k = 2$ then

$$\gamma \geq 0.$$

Moreover the inequality is strict if p is odd. This statement is of course weaker than that of (i).

(iii) If $\ell = p$, $k \geq 3$, and p is odd, then

$$\gamma \geq u + \frac{t-u}{p}$$

α_p is again 0. The left side is at least

$$-u+\frac{3(p-1)}{p}\,t=u+\frac{t-u}{p}+\frac{1}{p}\,\{(3p-4)t-(2p-1)u\}.$$

The final term is non-negative. The inequality is strict if $u \neq t$. If $u = t$ and p does not divide u it is again strict for then $\alpha_i \neq 0$ for some $i < p-1$ and for such an i the number $iu+t$ is not divisible by p.

(iv) If $k \leq p$ then

$$(p-1)u+\gamma \geq u+\frac{t-u}{p}$$

except when $\alpha_p = k$ or $\alpha_p = p-1$. We have to show that

$$(p-2)u+\gamma+\frac{u-t}{p} \geq 0.$$

The left side is at least

$$\left\{p-2-\frac{\ell}{p}+\frac{1}{p}\right\}u+\left\{\frac{p-1}{p}\ \left(\sum\nolimits_{i=1}^{p-1}\alpha_i\right)-\frac{1}{p}\right\}t.$$

If $\alpha_p \neq k$ the coefficient of t is positive and we need only show that it is at least as great as the negative of the coefficient of u or in other words that

$$(p-1)\ \left(\sum\nolimits_{i=1}^{p-1}\alpha_i\right)+(p-2)p \geq \ell.$$

This follows from the assumption that $\alpha_p \leq p-2$.

(v) If $k \leq p-2$ and $\alpha_p = k$ then

$$(p-1)u+\gamma \geq u.$$

In this case

$$\gamma \geq -ku.$$

There are circumstances in which the estimates for γ_i and therefore those for γ can be substantially improved. We will discuss them shortly.

Suppose now that K/F is a totally ramified Galois extension and $G = \mathfrak{G}(K/F)$ is the direct product of two cyclic groups of order p. By Lemma 11.1 the sequence of ramification groups is of the form

$$G=G_{-1}=G_0=G_1=\ldots=G_u \neq G_{u+1}=\ldots=G_t \neq G_{t+1}=\{1\}$$

with $(u,p)=1$ and $u \equiv t \,(\mathrm{mod}\, p)$ or of the form

$$G=G_{-1}=G_0=G_1=\ldots=G_t \neq G_{t+1}=\{1\}$$

with $(t,p)=1$. In the second case we take $u=t$. In the first case let L_1 be the fixed field of G_t and in the second let L_1 be any subfield of K of degree p over F. Let L_2 be any subfield of K different from L_1 which is also of degree p over F. Let $G^i = \mathfrak{G}(K/L_i)$ and let

$$G^i = G^i_{s_i} \neq G^i_{s_i+1} = \{1\}.$$

Then $s_1 = t$ and $s_2 = u$. According to Proposition IV.4 of Serre's book

$$\delta_{K/F} = (p^2 - p)\,(u+1) + (p-1)\,(t+1)$$

and

$$\delta_{K/L_1} = (p-1)\,(t+1)$$

and

$$\delta_{K/L_2} = (p-1)\,(u+1).$$

Thus

$$\delta_{L_1/F} = \frac{1}{p}\,\left(\delta_{K/F} - \delta_{K/L_1}\right) = (p-1)\,(u+1)$$

and

$$\delta_{L_2/F} = \frac{1}{p}\,\left(\delta_{K/F} - \delta_{K/L_2}\right) = \frac{(p-1)}{p}\,\left((p-1)\,(u+1) + t + 1\right).$$

If $\overline{G}^i = \mathfrak{G}(L_i/F)$ and

$$\overline{G}^i = \overline{G}^i_{t_i} \neq \overline{G}^i_{t_i+1} = \{1\}$$

then $t_1 = u$ and

$$t_2 = u + \frac{t-u}{p}.$$

Lemma 11.7

Suppose Δ belongs to K, $v_K(\Delta) = -u$, and

$$\Delta^p - \Delta = a$$

belongs to L_2. If Y belongs to L_2 then

$$v_{L_1}\left(S_{K/L_1}(Y\Delta^i)\right) \geq (p-1)t_2 - it_1 + v_{L_2}(Y)$$

and

$$v_{L_1}(E^i_{K/L_1}(Y\Delta)) \geq (p-1)t_2 + i(v_{L_2}(Y) - t_1)$$

for $1 \leq i \leq p-1$.

We show first that if θ belongs to L_1 and

$$\theta = \sum_{i=0}^{p-1} Y_i\Delta^i$$

with Y_i in L_2 then

$$v_{L_2}(Y_i) \geq it_1 + v_{L_1}(\theta)$$

for $0 \leq i \leq p-1$. Since $t_1 = u$ and

$$v_K(\theta) = \min_{0\leq i\leq p-1} \{v_K(Y_i) - iu\}$$

the inequality is clear for $i = 0$. To prove it in general, we use induction one i. Suppose $0 < j \leq p-1$ and the inequality is valid for $i < j$.

Let

$$pO_F = \mathfrak{P}_F^e.$$

Applying the exercise at the beginning of the paragraph to the extension L_2/F we see that

$$pe \geq (p-1)t_2 = (p-1)\left(u + \frac{t-u}{p}\right).$$

If ξ is any $(p-1)$th root of unity then, by Lemmas 11.3 and 11.4, there is a σ in $\overline{G}^2$ such that

$$\Delta^\sigma = \Delta + \xi + O(\varpi_K^{p^2e-(p-1)u}).$$

We may write

$$\theta^\sigma - \theta = \sum_{i=1}^{p-1} Y_i(\Delta^{i\sigma} - \Delta^i)$$

as a linear combination

$$\sum_{i=0}^{p-1} X_i\Delta^i$$

with coefficients from L_2. Since

$$v_{L_2}(\theta^\sigma - \theta) \geq v_{L_1}(\theta) + t_1$$

we may apply the induction assumption to see that

$$v_{L_2}(X_{j-1}) \geq (j-1))t_1 + v_{L_1}(\theta^\sigma - \theta) \geq jt_1 + v_{L_1}(\theta).$$

On the other hand

$$\Delta^{i\sigma} - \Delta^i = (\Delta+\xi)^i - \Delta^i + O(\varpi_K^{p^2e-(p-1)u-(i-1)u})$$

so that $\theta^\sigma - \theta$ is equal to

$$\sum_{i=1}^{p-1} Y_i \sum_{k=0}^{i-1} \binom{i}{k} \Delta^k\xi^{i-k} + \eta$$

with

$$\eta = O(\theta\varpi_K^{p^2e-(p-2)u}).$$

Thus if

$$\eta = \sum_{i=0}^{p-1} Z_i\Delta^i$$

with the Z_i in L_2 we have

$$v_K(Z_{j-1}) \geq (j-1)u + v_K(\Theta) + p^2e - (p-2)u.$$

But

$$p^2e - (p-2)u + (j-1)u \geq p(p-1)u - (p-2)u + (j-1)u$$

which equals

$$((p-1)^2 + j)u \geq pju.$$

Since

$$X_{j-1} = \left(\sum_{i=j}^{p-1} Y_i \binom{i}{j} \xi^{i-j}\right) + Z_{j-1}$$

we have

$$v_{L_2}\left(\sum_{i=j}^{p-1} Y_i \binom{i}{j} \xi^{i-j}\right) \geq ju + v_{L_1}(\theta)$$

for all ξ. We obtain the required estimate for $v_{L_2}(Y_j)$ by summing over ξ.

We now show that

$$v_{L_1}(S_{K/L_1}(Y\Delta^i)) \geq (p-1)t_2 - it_1 + v_{L_2}(Y)$$

for Y in L_2 and $1 \leq i \leq p-1$. All we need do is show that for any θ in the inverse different of L_1/F

$$S_{L_1/F}(\theta\varpi_{L_1}^{-v_{L_2}(Y)+it_1-(p-1)t_2}\ S_{K/L_1}(Y\Delta^i)) \in O_F$$

or that if θ is in L_1 and

$$v_{L_1}(\theta) \geq -(p-1)\,(t_1+1) + it_1 - (p-1)t_2 - v_{L_2}(Y)$$

then

$$S_{L_1/F}(\theta\, S_{K/L_1}(Y\Delta^i)) = S_{K/L}(\theta\, Y\Delta^i) \tag{11.4}$$

is in O_F.

Let

$$\theta = \sum_{j=0}^{p-1} Y_j\Delta^j$$

with Y_j in L_2 for $0 \leq j \leq p-1$. Then

$$\theta\, Y\Delta^i = \sum_{j=0}^{p-1-i} YY_j\Delta^{j+i} + (a+\Delta)\sum_{j=p-i}^{p-1} YY_j\Delta^{j+i-p}.$$

Since

$$\Delta^p - \Delta = a$$

we have

$$E^i_{K/L_2}(\Delta) = 0$$

for $1 \leq i < p-1$ and

$$E^{p-1}_{K/L_2}(\Delta) = (-1)^p.$$

The relations (11.2) imply that

$$S_{K/L_2}(\Delta^i) = 0$$

for $1 \leq i < p-1$ and that

$$S_{K/L_2}(\Delta^{p-1}) = p-1.$$

Thus (11.4) is equal to

$$(p-1)\, S_{L_2/F}(YY_{p-1-i}) + S_{L_2/F}(paYY_{p-i})$$

if $i < p-1$ and to the sum of this and

$$S_{L_2/F}(YY_{p-1})$$

if $i = p-1$.

We know that

$$v_{L_2}(Y_j) \geq jt_1 + v_{L_1}(\theta)$$

for each j. Thus

$$v_{L_2}(YY_{p-1-i}) \geq (p-1-i)t_1 - (p-1)\,(t_1+1) + it_1 - (p-1)t_2$$

which is at least $-(p-1)\,(t_2+1)$. So is

$$v_{L_2}(paYY_{p-1}) \geq (p-1)t_2 - t_1 - (p-1)\,(t_1+1) + it_1 + (p-i)t_1 - (p-1)t_2.$$

If $i = p-1$

$$v_{L_2}(YY_{p-1}) \geq (p-1)t_1 - (p-1)\,(t_1+1) + (p-1)t_1 - (p-1)t_2$$

is also at least $-(p-1)\,(t_2+1)$. All we need do now is observe that

$$S_{L_2/F}(\mathfrak{P}_{L_2}^{-(p-1)\,(t_2+1)}) \subseteq O_F.$$

To complete the proof of the lemma we have to show that

$$v_{L_1}(E^i_{K/L_1}(Y\Delta)) \geq (p-1)t_2 + i(v_{L_2}(Y) - t_1)$$

for $1 \leq i \leq p-1$. This has been done for $i = 1$; so we proceed by induction. Applying the relations (11.2) we see that

$$(-1)^{i+1}\, iE^i_{K/L_1}(Y\Delta) = \sum\nolimits_{j=0}^{i-1} (-1)^j\, S^{i-j}_{K/L_1}\,(Y\Delta)\, E^j_{K/L_1}(Y\Delta).$$

According to the induction assumption and the first part of the lemma, with Y replaced by Y^{i-j}, a typical term in the sum on the right is $O(\varpi^v_{L_1})$ with

$$v = (p-1)t_2 - (i-j)t_1 + (i-j)v_{L_2}(Y) + (p-1)t_2 + j(v_{L_2}(Y) - t_1)$$

if $j > 0$ and

$$v = (p-1)t_2 - it_1 + iv_{L_2}(Y)$$

if $j = 0$. The lemma follows.

We apply the second estimate with $Y = 1$ to improve, when $\Lambda = \Delta,\ L = L_1$, and certain auxiliary conditions are satisfied, our estimates on the number γ appearing in (11.3).

(vi) Suppose p is odd and

$$\ell = (p-1)\nu + j + 1.$$

If $k \geq \nu + 2$ and $\alpha_p \leq k-2$ then

$$jt_1 + \gamma \geq pt_2.$$

If $k \geq \nu + 2$ and $\alpha_p \leq k-1$ then

$$jt_1 + \gamma \geq (p-1)t_2 + t_1$$

and if $k \geq \nu + 1$ and $\alpha_p \leq k - 1$

$$jt_1 + \gamma \geq (p-1)t_2 - t_1.$$

In the present circumstances

$$\gamma_i \geq (p-1)t_2 - it_1$$

for $1 \leq i \leq p-1$. Thus

$$jt_1 + \gamma \geq jt_1 + \sum\nolimits_{i=1}^{p-1} \alpha_i((p-1)t_2 - it_1) - \alpha_p t_1$$

which equals

$$jt_1 + (p-1)kt_2 - \ell t_1 - (p-1)\alpha_p(t_2 - t_1)$$

or

$$(p-1)kt_2 - (p-1)\nu t_1 - t_1 - (p-1)\alpha_p(t_2 - t_1).$$

If $\alpha_p \leq k-2$, this is at least

$$2(p-1)t_2 + (p-1)\,(k-2-\nu)t_1 - t_1$$

which in turn is at least pt_2 if $p \geq 3$ and $k \geq \nu + 2$. If $\alpha_p \leq k-1$

$$\gamma \geq (p-1)t_2 + (p-1)\,(k-1-\nu)t_1 - t_1.$$

The required inequalities follow.

We shall use all these estimates for γ in the next sequence of lemmas.

Lemma 11.8

If Δ is as in Lemma 11.7 and p is odd then

$$S_{L_1/F} N_{K/L_1} \Delta \equiv S_{L_2/F} N_{K/L_2} \Delta \pmod{\mathfrak{P}_F^{1+t_2}}.$$

The assertion of the lemma may be reformulated as

$$S_{K/L_2} N_{K/L_1} \Delta \equiv S_{K/L_1} N_{K/L_2} \Delta \pmod{\mathfrak{P}_{L_1}^{1+pt_2}}.$$

Notice that

$$pt_2 = t + (p-1)u.$$

Earlier we applied Newton's identity to express $S^p_{K/L_1}(\Delta)$ in terms of the elementary symmetric functions of Δ and its conjugates. Since

$$pe \geq (p-1)t_2$$

we can apply the estimates (iii) for γ to see that

$$S^p_{K/L_1}(\Delta)$$

is congruent to

$$pN_{K/L_1}\Delta + \frac{p}{2}\ \sum\nolimits_{j=1}^{p-1}\ E^j_{K/L_1}(\Delta)\, E^{p-j}_{K/L_1}(\Delta) + \{S_{K/L_1}(\Delta)\}^p. \tag{11.5}$$

Since

$$\Delta^p - \Delta = a$$

we have

$$S_{K/L_1}(\Delta) = S^p_{K/L_1}(\Delta) - S_{L_2/F}(a).$$

According to Lemma 11.7 the left side belongs to $\mathfrak{P}_{L_1}^{(p-1)t_2-t_1}$. In particular it belongs to $\mathfrak{P}_{L_1}$. We need to know that it belongs to $\mathfrak{P}_{L_1}^{1+t_2}$. This is clear if $p > 3$ or $t_2 > t_1$. To prove it in general we first observe that all terms but the last in (11.5) are congruent to 0 modulo $\mathfrak{P}_{L_1}^{1+t_2}$. The middle terms are taken care of by the estimates (ii) for γ. To take care of the first we have to show that

$$pe - u \geq 1 + t_2.$$

We know that $pe \geq (p-1)t_2$ and that if $t = u$ the inequality is strict. We need only show that

$$(p-1)t_2 - u \geq t_2$$

with a strict inequality if $t \neq u$. This is clear since $t_2 \geq u$ and $t_2 > u$ if $t \neq u$. Thus

$$S_{K/L_1}\Delta \equiv (S_{K/L_1}\Delta)^p - S_{L_2/F}(a) \pmod{\mathfrak{P}_{L_1}^{1+t_2}}.$$

We now need only show that

$$S_{L_2/F}(a) \equiv 0 \pmod{\mathfrak{P}_{L_1}^{1+t_2}}.$$

The left side belongs to $\mathfrak{P}_{L_1}^{pb}$ if b is any integer less than or equal to

$$\frac{-u + (p-1)(t_2+1)}{p}.$$

We may take

$$b \geq \frac{-u + (p-1)t_2}{p}$$

which is greater than or equal to $\frac{1+t_2}{p}$ except when $p = 3$ and $t = u$. In this case, which is the one to worry about, $t_2 = u$ is prime to p and

$$\frac{-u + (p-1)(t_2+1)}{p} = \frac{u+2}{3}$$

has integral part at least $\frac{u+1}{3}$.

We apply (11.5) again to see that

$$S_{K/L_1}N_{K/L_2}\Delta = S_{K/L_1}a = S^p_{K/L_1}(\Delta) - S_{K/L_1}(\Delta)$$

is congruent to

$$-S_{K/L_1}\Delta + p\,N_{K/L_1}\Delta + \frac{p}{2}\ \sum\nolimits_{j=2}^{p-2}\ E^j_{K/L_1}(\Delta)\, E^{p-j}_{K/L_1}(\Delta).$$

We have still to consider
$$S_{K/L_2}\ N_{K/L_1}\,\Delta. \tag{11.6}$$
There are some general remarks to be made first. Suppose Λ belongs to K and
$$v_K(\Lambda) = -u.$$
If x and z also belong to K and
$$x\Lambda^j \in O_K$$
and
$$z \in \mathfrak{P}_K^{1+t+(p^2-1)u}$$
then
$$N_{K/L_1}(x(\Lambda+z)^{j+1}) \equiv N_{K/L_1}(x\Lambda^{j+1}) \pmod{\mathfrak{P}_{L_1}^{1+pt_2}}.$$
It is enough to show that
$$N_{K/L_1}\left(1+\frac{z}{\Lambda}\right)^{j+1} \equiv 1 \pmod{\mathfrak{P}_{L_1}^{1+t+pu}}.$$
This follows from Lemma V.5 of Serre's book and the relations
$$1+t+p^2u \geq 1+t+pu$$
and
$$\frac{1+t+p^2u+(p-1)\,(t+1)}{p} = 1+t+pu.$$

According to Lemmas 11.3 and 11.4 there is for each $\sigma \neq 1$ in G^2 a $(p-1)$th root of unity $\xi = \xi(\sigma)$ such that
$$\Delta^\sigma = (\Delta+\xi)^p - a + O\,(\varpi_K^{2(p^2e-(p-1)u)}).$$
We have
$$p^2e-(p-1)u \geq (p-1)\,\{(p-1)u+t\} - (p-1)u$$
which equals
$$(p-1)t + (p-2)\,(p-1)u \geq t + p(p-2)u.$$
If $t = u$ the first of these inequalities is strict and if $t > u$ the last is. Thus
$$p^2e-(p-1)u \geq 1+t+p(p-2)u$$
and
$$2(p^2e-(p-1)u) \geq \{1+t+(p^2-1)u\} + \{1+t+((p-1)^2-2p)u\}.$$
The second term is positive unless $p = 3$.

The expression
$$(\Delta+\xi)^p - a$$
is equal to
$$\Delta + \xi + \sum\nolimits_{i=1}^{p-1} \binom{p}{i}\ \xi^i\Delta^{p-i}.$$

But

$$\binom{p}{i} = \frac{p(p-1)\dots(p-i+1)}{i!} \equiv (-1)^{i+1}\ \frac{p}{i} \pmod{p^2}$$

and

$$2p^2e-(p-1)u \geq 2(p^2e-(p-1)u)$$

which is, as we have just seen, at least $1+t+(p^2-1)u$. Thus if $p>3$

$$\Delta^\sigma \equiv (\Delta+\xi)\,(1-Z(\xi)) \pmod{\mathfrak{P}_K^{1+t+(p^2-1)u}}$$

if

$$Z(\xi) = \frac{p\Delta^{p-1}}{1+\xi/\Delta}\ \sum\nolimits_{i=1}^{p-1}\ \frac{(-1)^i}{i}\ \left(\frac{\xi}{\Delta}\right)^i.$$

Expanding the denominator we obtain

$$Z(\xi) = p\Delta^{p-1}\ \sum\nolimits_{i=1}^{\infty}\ a_i\ \left(\frac{\xi}{\Delta}\right)^i.$$

If $i \geq p-1$

$$a_i = (-1)^i\ \sum\nolimits_{j=1}^{p-1}\ \frac{1}{j} \equiv 0 \pmod{p}.$$

Clearly

$$Z(\xi) = O(p\Delta^{p-2}) = O(\varpi_K^{p^2e-(p-2)u}).$$

If $p=3$

$$3(p^2e-(p-1)u) \geq \{1+t+(p^2-1)u\} + \{2(1+t)+(2p^2-6p+1)u\}.$$

The second term is at least $3u$ and in particular, is positive. Lemmas 11.3 and 11.4 show that

$$\Delta^\sigma \equiv ((\Delta+\xi)^3-a)^3-a \pmod{\mathfrak{P}_K^{1+t+(p^2-1)u}}.$$

The right side equals

$$(\Delta+\xi+3\xi\Delta^2+3\xi^2\Delta)^3-a.$$

Expanding the cube and ignoring all terms in $\mathfrak{P}_K^{1+t+(p^2-1)u}$ we obtain

$$\Delta+\xi+3\Delta^3\left\{\frac{\xi}{\Delta}+\frac{\xi^2}{\Delta^2}\right\}+9\Delta^4\xi$$

which we write as

$$(\Delta+\xi)\,(1-Z(\xi))$$

with

$$Z(\xi) = 3\Delta^2\sum\nolimits_{i=1}^{\infty}\ a_i\ \left(\frac{\xi}{\Delta}\right)^i + 9\Delta^4\sum\nolimits_{i=1}^{\infty}\ \left(\frac{-\xi}{\Delta}\right)^i.$$

Since

$$2(p^2e-(p-2)u) \geq 2(p^2e-(p-1)u)+2u \geq 1+t+p^2u$$

and

$$p^2e-(p-2)u \geq 1+t+(p-1)^2u \geq 1+t+pu$$

for all odd p, lemma V.5 of Serre's book shows that

$$N_{K/L_1}(x(\Delta+\xi)^{j+1}(1-Z(\xi))^{j+1}) \equiv \{N_{K/L_1}(x(\Delta+\xi)^{j+1})\}\,\{1-S_{K/L_1}Z(\xi)\}^{j+1}$$

modulo $\mathfrak{P}_{L_1}^{1+t+(p-1)u}$ if $x\Delta^j$ lies in O_K.

The expression (11.6) is equal to

$$N_{K/L_1}\Delta + \sum\nolimits_{\substack{\sigma\in G^2\\ \sigma\neq 1}} N_{K/L_1}\Delta^{\sigma}.$$

The preceding remarks show that, if $p>3$, this is congruent to

$$N_{K/L_1}\Delta + \sum\nolimits_{\xi} N_{K/L_1}(\Delta+\xi)\,\{1-S_{K/L_1}Z(\xi)\}$$

modulo $\mathfrak{P}_{L_1}^{1+t+(p-1)u}$. Since

$$\frac{2p^2e+u+(p-1)t}{p} \geq 2(p-1)\left(u+\frac{t-u}{p}\right)tu > t+pu$$

we have

$$N_{K/L_1}(\Delta+\xi)\,S_{K/L_1}(a_ip\,\Delta^{p-1-i}\xi^i) \in \mathfrak{P}_{L_1}^{1+pt_2}$$

if $i \geq p$ and we may replace $S_{K/L_1}Z(\xi)$ by

$$\sum\nolimits_{i=1}^{p-1} p\xi^i\,S_{K/L_1}(a_i\Delta^{p-1-i})$$

if $p>3.$ Of course

$$N_{K/L_1}(\Delta+\xi) = \sum\nolimits_{i=0}^{p} \xi^{1-i}\,E^i_{K/L_1}(\Delta).$$

Putting these observations together we see that, if $p>3$, (11.6) is congruent modulo $\mathfrak{P}_{L_1}^{1+pt_2}$ to the sum of

$$N_{K/L_1}\Delta + (p-1)\,\{S_{K/L_1}\Delta + N_{K/L_1}\Delta\}$$

and

$$-p(p-1)\,\sum\nolimits_{i=1}^{p-1} a_i\,S_{K/L_1}(\Delta^{p-1-i})\,E^{1+i}_{K/L_1}(\Delta)$$

and

$$-p(p-1)\,\{pa_{p-1}\,S_{K/L_1}(\Delta) + a_{p-2}\,S_{K/L_1}(\Delta)\}.$$

Since

$$pS_{K/L_1}(\Delta) \in \mathfrak{P}_{L_1}^{1+pt_2}$$

the last expression may be ignored as may the term in the second corresponding to $i = p-2$. Since

$$a_{p-1} = \sum_{j=1}^{p-1} \frac{1}{j} \equiv 0 \pmod p$$

and

$$S_{K/L_1}(\Delta^0) = p$$

and

$$3p^2e - t_2 \geq 1 + pt_2$$

the sum in the second expression need only be taken from 1 to $p-3$. The relation (11.2) implies that

$$pS_{K/L_1}^{p-1-i}(\Delta)\, E_{K/L_1}^{1+i}(\Delta) \equiv (-1)^i p(p-1-i)\, E_{K/L_1}^{p-1-i}(\Delta)\, E_{K/L_1}^{1+i}(\Delta)$$

modulo $\mathfrak{P}_{L_1}^{1+pt_2}$. To complete the proof of Lemma 11.8, for $p > 3$, we need only show that

$$ia_{i-1} + (p-i)\, a_{p-i-1} \equiv (-1)^i \pmod p$$

for $p-2 \geq p-i \geq i \geq 2$. This amounts to showing that

$$i \sum_{j=1}^{i-1} \frac{1}{j} + (p-i) \sum_{j=1}^{p-i-1} \frac{1}{j} \equiv -1 \pmod p.$$

We may replace the $p-i$ in front of the second sum by $-i$. Making the obvious cancellations we obtain

$$-i \sum_{j=i}^{p-i-1} \frac{1}{j} \equiv -1 - i \sum_{j=i}^{p-i} \frac{1}{j}.$$

If $\frac{1}{j}$ occurs in the sum on the right so does $\frac{1}{p-j}$.

The proof for $p = 3$ can proceed in exactly the same way provided we show that

$$9 \sum \{N_{K/L_1}(\Delta + \xi)\} \, \{S_{K/L_1}(\xi^i \Delta^{4-i})\} \tag{11.7}$$

lies in $\mathfrak{P}_{L_1}^{1+3t_2}$ for $i \geq 1$. Since

$$2p^2e - u \geq 2(p-1)t_2 - u \geq 3t_2$$

and one of the inequalities is strict

$$9N_{K/L_1}(\Delta + \xi) \in \mathfrak{P}_{L_1}^{1+3t_2}.$$

The expression

$$\xi^i \, S_{K/L_1}(\Delta^{4-i})$$

is clearly integral for $i \geq 4$. By, for example, Lemma 11.7 it is also integral if i is 2 or 3. Thus $i = 1$ is the only case to cause a problem. If $i = 1$ we sum over ξ to see that (11.7) equals

$$18\{E_{K/L_1}^2(\Delta)\, S_{K/L_1}(\Delta^3) + S_{K/L_1}(\Delta^3)\}.$$

The terms appearing in the expression in brackets have been shown to lie in O_{L_1}.

There is one more lemma to be proved before we come to the basic fact of this paragraph. If x is in K we set

$$g(x) = S_{L_1/F}(N_{K/L_1}\Delta\, S_{K/L_1}(x)) - S_{L_2/F}(N_{K/L_2}\Delta\, S_{K/L_2}(x))$$

and

$$h(x) = S_{L_1/F}(N_{K/L_1}(x\Delta)) - S_{L_2/F}(N_{K/L_2}(x\Delta)).$$

In the following lemma p is supposed odd.

Lemma 11.9

(a) *Suppose x is in L_2, $0 \le j \le p-1$, and $x\Delta^j$ lies in $\mathfrak{P}_K^{1+t_2-t_1}$. If $j \ne p-2$ then*

$$g(x\Delta^j) \equiv 0 \qquad (\operatorname{mod} \mathfrak{P}_F^{1+t_2})$$

but if $j = p-2$, there is an ω in L_2 such that

$$\omega x \equiv -x\, E^{p-1}_{K/L_1}(\Delta) \qquad (\operatorname{mod} \mathfrak{P}_K^{1+pt_2})$$

and

$$g(x\Delta^j) \equiv -\{S_{L_2/F}x - S_{L_2/F}(x\omega)\} \quad (\operatorname{mod} \mathfrak{P}_F^{1+t_2}).$$

(b) *Suppose x is in L_2, $0 \le j \le p-1$, and $x\Delta^j$ lies in $\mathfrak{P}_K$. If $j \ne p-2$*

$$h(x\Delta^j) \equiv 0 \qquad (\operatorname{mod} \mathfrak{P}_F^{1+t_2})$$

but if $j = p-2$

$$h(x\Delta^j) \equiv (p-1)\,(1 - \{E^{p-1}_{K/L_1}(\Delta)\}^p) N_{K/L_1} x$$

modulo $\mathfrak{P}_{L_1}^{1+pt_2}$.

The congruences modulo $\mathfrak{P}_F^{1+t_2}$ are of course equivalent to congruences modulo $\mathfrak{P}_{L_1}^{1+pt_2}$. We start with part (a). If x belongs to O_{L_2} then

$$g(x) = S_{K/L_1}(xS_{K/L_2}(N_{K/L_1}\Delta) - pxa).$$

Because of the previous lemma this is congruent to

$$S_{K/L_1}(xS_{L_2/F}a - pxa) = S_{L_2/F}\, xS_{L_2/F}a - pS_{L_2/F}(xa)$$

modulo $\mathfrak{P}_F^{1+t_2}$. We saw before that

$$S_{L_2/F}a \in \mathfrak{P}_{L_1}^{1+t_2}.$$

The same argument shows that

$$S_{L_2/F}(xa) \in \mathfrak{P}_{L_1}^{1+t_2}.$$

p belongs to $\mathfrak{P}_{L_1}^{(p-1)t_2}$. Since the integral part of

$$\frac{(p-1)\,(t_2+1)}{p}$$

is at least
$$\frac{(p-1)t_2}{p},$$
so does $S_{L_2/F}x$. This takes care of the case $j=0$.

If $1 \le j = p-1$ then $g(x\Delta^j)$ is equal to
$$S_{L_2/F}(xS_{K/L_2}(\Delta^j\, N_{K/L_1}\Delta)) - (p-1)\delta\, S_{L_2/F}(xa)$$
where $\delta = 0$ if $j \ne p-1$ and $\delta = 1$ if $j = p-1$. Consider
$$Z_j = x\, S_{K/L_2}(\Delta^j\, N_{K/L_1}\Delta).$$
It lies in L_2 and is equal to
$$x\Delta^j\, N_{K/L_1}\Delta + \sum\nolimits_{\substack{\sigma\in G^2\\ \sigma\ne 1}} x\Delta^{\sigma\, j}\, N_{K/L_1}\Delta^{\sigma}.$$

We observe first of all that if Λ is in $K,\ v_K(\Lambda) = -u,\ x$ is in $L_2,\ x\Lambda^j$ lies in $\mathfrak{P}_K^{1+t_2-t_1}$, and z lies in $\mathfrak{P}_K^{(p-1)\,(pt_2-t_1)}$ then
$$x(\Lambda+z)^j N_{K/L_1}(\Lambda+z) \equiv x\Lambda^j N_{K/L_1}\Lambda \pmod{\mathfrak{P}_K^{1+pt_2}}$$
provided p is greater than 3. To establish this congruence we show that
$$\left(1+\frac{z}{\Lambda}\right)^j\ N_{K/L_1}\ \left(1+\frac{z}{\Lambda}\right) \equiv 1 \pmod{\mathfrak{P}_K^{(p-1)t_2+(p+1)t_1}}.$$
To show this, one has only to observe that $\frac{z}{\Lambda}$ and all its conjugates lie in $\mathfrak{P}_K^{(p-1)pt_2-(p-2)t_1}$ and that
$$(p-1)pt_2 - (p-2)t_1 \ge (p-1)t_2 + ((p-1)^2 - (p-2))t_1$$
which equals
$$(p-1)t_2 + ((p-1)\,(p-2)+1)t_1 \ge (p-1)t_2 + (p+1)t_1$$
if $p > 3$.

Suppose for now that $p > 3$. Since
$$p^2e - (p-1)u \ge (p-1)\,(pt_2 - t_1).$$
Lemma 11.4 implies that Z_j is congruent to
$$x\Delta^j\, N_{K/L_1}\Delta + \sum\nolimits_{\xi} x(\Delta+\xi)^j\, N_{K/L_1}(\Delta+\xi)$$
modulo $\mathfrak{P}_K^{1+pt_2}$
$$N_{K/L_1}(\Delta+\xi) = \xi\left\{1 + \frac{1}{\xi}\ N_{K/L_1}\Delta + \sum\nolimits_{i=1}^{p-1} \xi^{-i} E^i_{K/L_1}(\Delta)\right\}.$$

According to Lemma 11.7 this is congruent to

$$\xi + N_{K/L_1}\Delta + \xi\, E^{p-1}_{K/L_1}(\Delta)$$

modulo $\mathfrak{P}_K^{pt_2}$. Thus if $x\Delta^j$ belongs to $\mathfrak{P}_K^{1+t_2-t_1}$

$$Z_j \equiv x\Delta^j\, N_{K/L_1}\Delta + \sum\nolimits_\xi x(\Delta+\xi)^j\,(\xi + N_{K/L_1}\Delta + \xi\, E^{p-1}_{K/L_1}(\Delta))$$

modulo $\mathfrak{P}_K^{1+pt_2}$. We expand $(\Delta+\xi)^j$ and sum over ξ to obtain

$$px\Delta^j\, N_{K/L_1}\Delta \tag{11.8}$$

if $j < p-2$. If $j = p-2$ we obtain

$$px\Delta^j\, N_{K/L_1}\Delta + (p-1)x\,(1 + E^{p-1}_{K/L_1}(\Delta))$$

and if $j = p-1$ we obtain

$$px\Delta^j\, N_{K/L_1}\Delta + (p-1)x\,\{N_{K/L_1}\Delta + (p-1)\Delta + (p-1)\Delta\, E^{p-1}_{K/L_1}(\Delta)\}.$$

The expression (11.8) lies in

$$\mathfrak{P}_K^{1+p^2e-pt_1}$$

provided $x\Delta^j$ lies in $\mathcal{P}_K$.

$$p^2e - pt_1 \geq p(p-1)t_2 - pt_1 \geq pt_2.$$

Since

$$L_2 \cap \mathfrak{P}_K^{1+pt_2} = \mathfrak{P}_{L_1}^{1+t_2}$$

and

$$S_{L_2/F}(\mathfrak{P}_{L_2}^{1+t_2}) \subseteq \mathfrak{P}_F^{1+t_2},$$

we have

$$g(x\Delta^j) \equiv 0 \pmod{\mathfrak{P}_F^{1+t_2}}$$

if $1 \leq j < p-2$ and $x\Delta^j$ lies in $\mathfrak{P}_K^{1+t_2-t_1}$.

Since

$$E^{p-1}_{K/L_1}(\Delta)$$

lies in O_{L_1},

$$Z_j = (\omega - 1)x$$

with

$$\omega\, x = Z_j + x \equiv -x\, E^{p-1}_{K/L_1}(\Delta) \pmod{\mathfrak{P}_K^{1+pt_2}}$$

if $j = p-2$. We may take ω in L_2 and then

$$g(x\Delta^j) \equiv -\{S_{L_2/F}x - S_{L_2/F}(x\omega)\} \pmod{\mathfrak{P}_F^{1+t_2}}.$$

If $j = p-1$ then
$$g(x\Delta^j) = S_{L_2/F}\left(Z_j - (p-1)xa\right)$$
and
$$Z_j - (p-1)xa$$
is congruent to
$$(p-1)x\left\{N_{K/L_1}\Delta + p\Delta + (p-1)\Delta\, E^{p-1}_{K/L_1}(\Delta) - \Delta^p\right\}$$
modulo $\mathfrak{P}_K^{1+pt_2}$. The product
$$\{(p-1)x\}\,\{p\Delta\}$$
lies in $\mathfrak{P}_K^{1+pt_2}$ and
$$(p-1)\,E^{p-1}_{K/L_1}(\Delta) \equiv -E^{p-1}_{K/L_1}(\Delta) \pmod{\mathfrak{P}_K^{1+pt_2}}.$$
It is easily seen that
$$\Delta^p + \Delta\,E^{p-1}_{K/L_1}(\Delta) - N_{K/L_1}\Delta$$
is equal to
$$-\sum_{i=1}^{p-2}(-1)^i\,\Delta^{p-i}\,E^i_{K/L_1}(\Delta).$$
Recalling that $x\Delta^{p-1}$ is supposed to lie in $\mathfrak{P}_K$ we appeal to Lemma 11.7 to see that the product of this expression with x lies in $\mathfrak{P}_K^{1+pt_2}$. Thus
$$g(x\Delta^j) \equiv 0 \pmod{\mathfrak{P}_F^{1+t_2}}.$$

If $p = 3$ and $\xi = \xi(\sigma)$ then
$$\Delta^\sigma = \Delta + \xi + 3\xi\Delta^2 + 3\xi^2\Delta + z$$
with
$$z = O(\varpi_K^{2(p^2e-(p-1)u)}).$$
If
$$\Delta_\sigma = \Delta + \xi + 3\xi\Delta^2$$
then
$$\Delta^\sigma = \Delta_\sigma + 3\xi^2\Delta + z.$$
If we can show that
$$3\xi^2\Delta + z = O(\varpi_K^{(p-1)t_2+pt_1})$$
it will follow that
$$x\Delta^{\sigma\,j}N_{K/L_1}\Delta^\sigma \equiv x\Delta_\sigma^j N_{K/L_1}\Delta_\sigma \pmod{\mathfrak{P}_K^{1+pt_2}} \tag{11.9}$$
if $x\Delta^j$ lies in $\mathfrak{P}_K^{1+t_2-t_1}$
$$3\xi^2\Delta = O(\varpi_K^{p^2e-t_1})$$
and
$$p^2e - t_1 \geq p(p-1)t_2 - t_1 \geq (p-1)t_2 + pt_1$$

because $(p-1)^2 \geq p$. Moreover

$$2(p^2e-(p-1)u) \geq 2(p(p-1)t_2-(p-1)t_1)$$

which is at least

$$(p-1)t_2+((2p-1)\,(p-1)-2(p-1))t_1$$

and

$$(2p-1)\,(p-1)-2(p-1)=(2p-3)\,(p-1) \geq p.$$

We want to replace $N_{K/L_1}\Delta_\sigma$ by

$$N_{K/L_1}(\Delta+\xi)$$

in the right side of (11.9). To do this we have to show that

$$N_{K/L_1}\ \left(\frac{\Delta_\sigma}{\Delta+\xi}\right) \equiv 1 \pmod{\mathcal{P}_K^{(p-1)t_2+(p+1)t_1}}.$$

Since

$$\frac{\Delta_\sigma}{\Delta+\xi}=1+O(\varpi_K^{p^2e-t_1})$$

and

$$p^2e-t_1 \geq p(p-1)t_2-t_1,$$

we have only to verify that

$$p\{p(p-1)t_2-t_1\} \geq (p-1)t_2+(p+1)t_1 \tag{11.10}$$

and that the integral part of

$$\frac{p(p-1)t_2-t_1+(p-1)\,(t+1)}{p} \tag{11.11}$$

is at least

$$\frac{(p-1)t_2+(p+1)t_1}{p}.$$

The inequality (11.10) is clear. Since $t \geq t_1$ the integral part of (11.11) is at least

$$\frac{p(p-1)t_2+(p-2)t_1}{p} \geq \frac{(p-1)t_2+((p-1)^2+(p-2))t_1}{p}$$

and

$$(p-1)^2+(p-2) \geq p+1.$$

Just as when $p>3$ we may replace $N_{K/L_1}(\Delta+\xi)$ in (11.9) by

$$\xi+N_{K/L_1}\Delta+\xi\,E_{K/L_1}^{p-1}(\Delta).$$

Thus Z_j is congruent to

$$x\Delta^j N_{K/L_1}\Delta+\sum\nolimits_\xi x(\Delta+\xi+3\xi\Delta^2)^j\ \left(\xi+N_{K/L_1}\Delta+\xi\,E_{K/L_1}^2(\Delta)\right)$$

modulo $\mathfrak{P}_K^{1+pt_2}$ if $p=3$, j is 1 or 2, and $x\Delta^j$ belongs to $\mathfrak{P}_K^{1+t_2-t_1}$. If $j=1$ this expression is equal to

$$px\Delta^j\,N_{K/L_1}\Delta + 2x(1+3\Delta^2)\,(1+E^2_{K/L_1}(\Delta)) \tag{11.12}$$

and if $j=2$ it is equal to

$$px\Delta^j\,N_{K/L_1}\Delta + 2x\{2(1+3\Delta^2)\Delta(1+E^2_{K/L_1}(\Delta)) + (1+3\Delta^2)^2N_{K/L_1}\Delta\}. \tag{11.13}$$

The term

$$px\Delta^j\,N_{K/L_1}\Delta$$

can be ignored as before because it lies in $\mathfrak{P}_K^{1+pt_2}$. Also

$$3x\Delta^{j+1} = O(\varpi_K^{1+p^2e+t_2-2t_1})$$

because $x\Delta^j$ lies in $\mathfrak{P}_K^{1+t_2-t_1}$ and

$$p^2e+t_2-2t_1 \geq p(p-1)t_2-t_1 \geq pt_2.$$

We may also replace the factor 2 in (11.12) by 1. Thus (11.12) is congruent to

$$-x(1+E^2_{K/L_1}(\Delta))$$

modulo $\mathfrak{P}_K^{1+pt_2}$. At this point we may argue as we did for $p>3$. To simplify (11.13), we observe that

$$9\Delta^4\,N_{K/L_1}\Delta = O(\varpi_K^{2p^2e-7t_1})$$

and that

$$2p^2e-7t_1 \geq 12t_2-7t_1 \geq 3t_2.$$

Moreover

$$3x\Delta^2\,N_{K/L_1}\Delta = O(\varpi_K^{1+p^2e-3t_1})$$

if $x\Delta^2$ belongs to $\mathfrak{P}_K$ and

$$p^2e-3t_1 \geq 6t_2-3t_1 \geq 3t_2.$$

Thus (11.13) is congruent to

$$2x\{2\Delta(1+E^2_{K/L_1}(\Delta)) + N_{K/L_1}\Delta\}$$

modulo $\mathfrak{P}_K^{1+3t_2}$. We may again argue as we did for $p>3$.

We turn to the second part of the lemma. We observe first that if x belongs to L_2, y belongs to K, and

$$xy \in \mathfrak{P}_K$$

then

$$h(xy) \equiv h(y)\,N_{K/L_1}(x) \pmod{\mathfrak{P}_F^{1+t_2}}.$$

The left side is

$$S_{L_1/F}(N_{K/L_1}xN_{K/L_1}y\Delta) - S_{L_2/F}(x^p\,N_{K/L_2}y\Delta).$$

Since $N_{K/L_2}x = N_{L_2/F}x$ lies in F this equals

$$\{N_{K/L_1}x\}h(y) + S_{L_2/F}\{N_{K/L_2}(y\Delta)\,(N_{L_2/F}x - x^p)\}.$$

The second term is the trace from L_2 to F of

$$\{N_{K/L_2}(xy\Delta)\}\left\{\frac{N_{L_2/F}x - x^p}{N_{K/L_2}x}\right\}$$

if, as we may as well assume, $x \neq 0$. All we need do is show that this expression lies in $\mathfrak{P}_{L_2}^{1+t_2}$ for then its trace will lie in $\mathfrak{P}_F^{1+t_2}$. The first factor lies in $\mathfrak{P}_{L_2}^{1-t_2}$. The second factor is equal to

$$\left\{\prod\nolimits_{\sigma\in\overline{G}^2} x^{\sigma-1}\right\} - 1.$$

Since $p \geq 3$ it will be sufficient to show that the image of the homomorphism

$$x \longrightarrow \varphi(x) = \prod\nolimits_{\sigma\in\overline{G}^2} x^{\sigma-1}$$

of C_{L_2} into U_{L_2} is contained in $U_{L_2}^{(p-1)t_2}$. Let ρ be a generator of $\overline{G}^2$ and let $P(X)$ be the polynomial

$$\sum\nolimits_{i=1}^{p-1}(X^i - 1) = \sum\nolimits_{i=0}^{p-1} X^i - p$$

then

$$\varphi(x) = x^{P(\rho)}.$$

Let

$$Q(X) = (X-1)^{p-1}.$$

If $1 \leq i \leq p-1$ the ith coefficient of $Q(X)$ is

$$(-1)^{p-1-i}\ \frac{(p-1)\dots(p-i)}{i!} \equiv 1 \pmod{p}.$$

Since both $P(X)$ and $Q(X)$ are divisible by $X-1$

$$P(X) = Q(X) + p(X-1)R(X)$$

where $R(X)$ is a polynomial with integral coefficients. For all z in C_{L_2},

$$z^{\rho-1} = 1 + w$$

with $w = O(\varpi_{L_2}^{t_2})$. Then

$$z^{p(\rho-1)} = (1+w)^p \equiv 1 + w^p \equiv 1 \pmod{\mathfrak{P}_{L_2}^{pt_2}}$$

and

$$z^{p(\rho-1)R(\rho)} \in U_{L_2}^{pt_2}.$$

If $a \geq 1$ and
$$w \in \mathfrak{P}_{L_2}^{a}$$
then
$$(1+w)^{p-1} = \frac{1+w^p}{1+w} = 1 + \frac{w^p - w}{1+w} \equiv 1 \pmod{\mathfrak{P}_{L_2}^{a+t_2}}.$$
One then shows easily by induction that, for all z in C_{L_2} and all $n \geq 1$,
$$z^{(\rho-1)^n} \in U_{L_2}^{nt_2}.$$

If x lies in $\mathfrak{P}_K$ we may take $y = 1$. Applying Lemma 11.8 we see that
$$h(x) \equiv N_{L_2/F}\, xh(1) \equiv 0 \pmod{\mathfrak{P}_F^{1+t_2}}.$$
If $1 \leq j \leq p-1,$ x lies in L_2, and $x\Delta^j$ lies in $\mathfrak{P}_K$,
$$h(x\Delta^j) \equiv P_j - Q_j \pmod{\mathfrak{P}_F^{1+t_2}}$$
with
$$P_j = N_{L_2/F}\, xS_{L_1/F}(N_{K/L_1}\Delta^{j+1})$$
and
$$Q_j = N_{L_2/F} x\, S_{L_2/F}(N_{K/L_2}\Delta^{j+1}).$$

The expression P_j is congruent to
$$N_{L_2/F} x\{N_{K/L_1}\Delta^{j+1} + \sum\nolimits_{\xi} N_{K/L_1}(\Delta+\xi)^{j+1}\,\{1 - S_{K/L_1}Z(\xi)\}^{j+1}\} \tag{11.14}$$
modulo $\mathfrak{P}_{L_1}^{1+pt_2}$. Since we are working modulo $\mathfrak{P}_{L_1}^{1+pt_2}$ we need only consider
$$(1 - S_{K/L_1}\, Z(\xi))^{j+1} \tag{11.15}$$
modulo $\mathfrak{P}_{L_1}^{pt_2+t_1}$. Suppose first that $p > 3$. Then
$$Z(\xi) = O(\varpi_K^{p^2e-(p-2)u})$$
and
$$p^2e - (p-2)u \geq p(p-1)t_2 - (p-2)u \geq p(p-2)t_2.$$
Moreover the integral part of
$$\frac{p(p-2)t_2 + (p-1)\,(t+1)}{p}$$
is at least
$$(p-2)t_2 - \frac{(p-1)}{p}t$$
and twice this is at least $pt_2 + t_1$. We replace (11.15) by
$$1 - (j+1)\, S_{K/L_1}\, Z(\xi).$$

Since

$$Z(\xi) \equiv p\Delta^{p-1} \sum_{i=1}^{p-2} a_i \left(\frac{\xi}{\Delta}\right)^i \pmod{p^2} \tag{11.16}$$

and

$$p^2 = O(\varpi_K^{2p^2 e})$$

while

$$2p^2 e \geq 2p(p-1)t_2 \geq p(pt_2 + t_1),$$

we may replace $Z(\xi)$ by the right side of (11.16). By Lemma 11.7

$$pS_{K/L_1}(\Delta^{p-1-i}) = O(\varpi_{L_1}^{pe+it_2})$$

if $1 \leq i \leq p-2$ and

$$pe + it_2 \geq (p-1)t_2 + it_2 \geq pt_2 + t_1$$

if $i \geq 2$. We replace $Z(\xi)$ by

$$pa_1\xi\Delta^{p-2}.$$

We may write (11.14) as

$$N_{L_2/F}xN_{K/L_1}\Delta^{j+1}\left\{1 + \sum_{\xi} N_{K/L_1}\left(1 + \frac{\xi}{\Delta}\right)^{j+1} \{1 - S_{K/L_1}(pa_1\xi\Delta^{p-2})\}\right\}.$$

When we expand

$$N_{K/L_1}\left(1 + \frac{\xi}{\Delta}\right)^{j+1}$$

and sum over ξ we will obtain

$$N_{L_2/F}xN_{K/L_1}\Delta^{j+1}\left\{1 + \sum_{\xi} N_{K/L_1}\left(1 + \frac{\xi}{\Delta}\right)^{j+1}\right\}$$

which we write as

$$N_{L_2/F}x\left\{N_{K/L_1}\Delta^{j+1} = \sum_{\xi} N_{K/L_1}(\Delta + \xi)^{j+1}\right\}$$

plus a sum of terms of the form

$$\alpha p\, N_{L_2/F}xN_{K/L_1}\Delta^{j+1}\, E^i_{K/L_1}\left(\frac{1}{\Delta}\right) S_{K/L_1}(\Delta^{p-2})$$

where α is rational and lies in O_F and i is at least 1. Since

$$E^i_{K/L_1}\left(\frac{1}{\Delta}\right) = O(\varpi_{L_1}^{t_1})$$

for $i \geq 1$ and

$$pS_{K/L_1}(\Delta^{p-2}) = O(\varpi_{L_1}^{pt_2})$$

these supplementary terms may be ignored.

Now take $p = 3$.*

*(1998) This is where and how the manuscript of Chapter 11 breaks off.

Chapter 12.

The Second Main Lemma

Suppose K is a normal extension of the local field F and $G = \mathfrak{G}(K/F)$ is the direct product of two cyclic groups of prime order ℓ. Let $\mathcal{X}_K$ be a quasi-character of C_K. If σ belongs to G define $\mathcal{X}_K^\sigma$ by the relation

$$\mathcal{X}_K^\sigma(\alpha) = \mathcal{X}_K(\alpha^{\sigma^{-1}}).$$

Suppose that $\mathcal{X}_K^\sigma = \mathcal{X}_K$ for all σ in G but that for no quasi-character $\mathcal{X}_F$ of C_F does $\mathcal{X}_K = \mathcal{X}_{K/F}$. If $F \subseteq L \subseteq K$ and $[K:L] = \ell$ then $\mathcal{X}_K$ can be extended to a quasi-character of $W_{K/L}$ because $W_{K/L}/C_K$ is isomorphic to $\mathfrak{G}(K/L)$ which is cyclic. If this quasi-character is $\mathcal{X}_L$ then $\mathcal{X}_K = X_{K/L}$.

Lemma 12.1

Suppose L_1 and L_2 are two fields lying between F and K and $[K:L_1] = [K:L_2] = \ell$. Suppose $\mathcal{X}_{L_1}$ is a quasi-character of C_{L_1}, $\mathcal{X}_{L_2}$ is a quasi-character of C_{L_2}, and

$$\mathcal{X}_K = \mathcal{X}_{K/L_1} = \mathcal{X}_{K/L_2}.$$

Then

$$\Delta(\mathcal{X}_{L_1},\, \psi_{L_1/F}) \prod\nolimits_{\mu_F \in S(L_1/F)} \Delta(\mu_F, \psi_F)$$

is equal to

$$\Delta(\mathcal{X}_{L_2}, \psi_{L_2/F}) \prod\nolimits_{\mu_F \in S(L_2/F)} \Delta(\mu_F, \psi_F).$$

Because of the assumption on $\mathfrak{G}(K/F)$ the field F must be non-archimedean. To prove the lemma in general it is enough to prove it for a given L_1 and all L_2. There are three possibilities to consider.

(i) The sequence of groups of ramification takes the form

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

(ii) The sequence of groups of ramification takes the form

$$G = G_{-1} = G_0 = G_1 = \ldots = G_u \neq G_{u+1} = \ldots = G_t \neq G_{t+1} = \ldots = \{1\}.$$

(iii) The sequence of groups of ramification takes the form

$$G = G_{-1} = G_0 = G_1 = \ldots = G_t \neq G_{t+1} = \ldots = \{1\}.$$

In the first two cases we take $G^1 = \mathfrak{G}(K/L_1)$ to be G_t. In the third case the choice of L_1 is immaterial.

If the relation $\mathcal{X}_{L_i}^\sigma = \mathcal{X}_{L_i}$ obtains for one σ different from 1 in $\overline{G}^i = \mathfrak{G}(L_i/F)$ it obtains for all such σ and $\mathcal{X}_{L_i}$ is of the form $\mathcal{X}_{L_i/F}$ for some quasi-character $\mathcal{X}_F$ of C_F. Then $\mathcal{X}_K = \mathcal{X}_{K/F}$ which is contrary to assumption. Thus the characters $\mathcal{X}_{L_i}^{\sigma-1}$ with σ in $\overline{G}^i$ are distinct. They are clearly trivial on $N_{K/L_i}\, C_K$ so

$$\{\mathcal{X}_{L_i}^{\sigma-1} \,|\, \sigma \in \overline{G}^i\} = S(K/L_i) = \{\mu_{L_i/F} \,|\, \mu_F \in S(L_j/F)\}.$$

Here j is 2 or 1 according as i is 1 or 2.

Let $t_i \geq -1$ be that integer for which
$$\overline{G}^i = \overline{G}^i_{t_i}$$
while
$$\overline{G}^i_{t_i+1} = \{1\}.$$
Then
$$\delta_i = \delta(L_i/F) = (t_i + 1)\,(\ell - 1).$$
In the first case L_1/F is unramified and L_2/F is ramified. We choose ϖ_{L_2} arbitrarily and take $\varpi_K = \varpi_{L_2}$. Also we set
$$\varpi_{L_1} = \varpi_F = N_{L_2/F}\varpi_{L_2}.$$
In the second and third cases K/L_1 and K/L_2 are ramified and K/F is totally ramified. We choose ϖ_k first and set
$$\varpi_{L_i} = N_{K/L_i}\varpi_K$$
and
$$\varpi_F = N_{K/F}\varpi_K.$$

Let $m_i = m(\mathcal{X}_{L_i})$. The $m(\mathcal{X}^\sigma_{L_i}) = m_i$ and
$$m(\mathcal{X}^{\sigma-1}_{L_i}) \leq m_i.$$
Thus $m(\nu) \leq m_i$ if ν belongs to $S(K/L_i)$. If $G^i = \mathfrak{G}(K/L_i)$ and if
$$G^i_{u_i} = G^i$$
while
$$G^i_{u_i+1} = \{1\}$$
then $m(\nu) = u_i + 1$ if ν is non-trivial. Thus $u_i + 1 \leq m_i$. Since $\nu\mathcal{X}_{L_i}$ is of the form $\mathcal{X}^\sigma_{L_i}$ for all ν in $S(K/L_i)$,
$$m(\nu\mathcal{X}_{L_i}) = m(\mathcal{X}_{L_i}).$$
Lemma 8.8 and 8.12 imply that*
$$m(\mathcal{X}_K) = \psi_{K/L_i}\ (m_i - 1) + 1.$$
This $m(\mathcal{X}_K) = m_i$ if K/L_i is unramified and
$$m(\mathcal{X}_K) = \ell m_i - \delta(K/L_i)$$
if K/L_i is ramified. If $n = n(\psi_F)$ then $n_i = n(\psi_{L_i/F})$ is n if L_i/F is unramified and is $\ell n + \delta_i$ if L_i/F is ramified.

In the first case
$$\delta(K/L_2) = \delta(L_1/F) = 0.$$

* We are encountering once again the conflicting uses of the symbole ψ.

The relations

$$\delta(K/F) = \delta(K/L_1) + \ell\delta(L_1/F) = \delta(K/L_1) = (t+1)\,(\ell-1)$$

and

$$\delta(K/F) = \delta(K/L_2) + \delta(L_2/F) = \delta_2 = (t_2+1)\,(\ell-1)$$

imply that $t_2 = t$. Also

$$m(\mathcal{X}_K) = m_2 = \ell m_1 - \delta(K/L_1) = \ell m_1 - \delta_2$$

so that

$$m_2 + n_2 = \ell(m_1 + n_1).$$

Moreover

$$\mathcal{X}_{L_1}(\varpi_{L_1}^{m_1+n_1}) = \mathcal{X}_K\,(\varpi_{L_2}^{m_1+n_1})$$

is equal to

$$\mathcal{X}_{L_2}(\varpi_{L_2}^{m_2+n_2}) = \mathcal{X}_{L_2}(\varpi_F^{m_1+n_1})\,\left\{\mathcal{X}_{L_2}\,\left(\prod\nolimits_{\sigma\in\overline{G}^2}\,\varpi_{L_2}^{1-\sigma}\right)\right\}^{m_1+n_1}$$

and

$$\prod\nolimits_{\sigma\in\overline{G}_2}\,\mathcal{X}_{L_2}(\varpi_{L_2}^{1-\sigma}) = \prod\nolimits_{\mu_F\in S(L_1/F)}\,\mu_{L_2/F}(\varpi_{L_2})$$

is equal to

$$\prod\nolimits_{\mu_F\in S(L_1/F)}\,\mu_F(\varpi_F) = (-1)^{\ell-1}.$$

If

$$S_i' = S(L_i/F) - \{1\}$$

then

$$\prod\nolimits_{S_1'}\,\mu_F(\varpi_F^{t_1+1+n}) = (-1)^{n(\ell-1)}$$

and

$$\prod\nolimits_{S_2'}\,\mu_F\,(\varpi_F^{t_2+1+n}) = 1.$$

Thus we have to show that

$$(-1)^{m_1(\ell-1)}\,\Delta_1(\mathcal{X}_{L_1},\psi_{L_1/F}\,\varpi_F^{m_1+n_1})$$

is equal to

$$\Delta_1(\mathcal{X}_{L_2},\psi_{L_2/F},\varpi_F^{m_1+n_1})\,\prod\nolimits_{S_2'}\,\Delta_1(\mu_F,\psi_F,\varpi_F^{t+1+n}).$$

In the second and third cases the relations

$$m(\mathcal{X}_K) = \ell m_1 - \delta(K/L_1) = \ell m_2 - \delta(K/L_2)$$

and

$$\delta(K/F) = \delta(K/L_1) + \ell\delta_1 = \delta(K/L_2) + \ell\delta_2$$

imply that $m_1 + \delta_1 = m_2 + \delta_2$ and hence that $m_1 + n_1 = m_2 + n_2$. Thus

$$\mathcal{X}_{L_1}(\varpi_{L_1}^{m_1+n_2}) = \mathcal{X}_K\,(\varpi_K^{m_1+n_1}) = \mathcal{X}_{L_2}(\varpi_{L_2}^{m_2+n_2}).$$

Since

$$\prod_{S_i'} \mu_F(\varpi_F^{t_i+1+n}) = 1$$

we have to show that

$$\Delta_1(\mathcal{X}_{L_1}, \psi_{L_1/F}, \varpi_{L_1}^{m_1+n_1}) \ \prod_{S_1'} \Delta_1(\mu_F, \psi_F, \varpi_F^{t_1+1+n})$$

is equal to

$$\Delta_1(\mathcal{X}_{L_2}, \psi_{L_2/F}, \varpi_{L_2}^{m_2+n_2}) \ \prod_{S_2'} \Delta_1(\mu_F, \psi_F, \varpi_F^{t_2+1+n}).$$

Suppose $\mathcal{X}_F'$ is a quasi-character of C_F. According to Lemma 10.1

$$\Delta(\mathcal{X}_{L_1/F}', \psi_{L_1/F}) \ \prod_{\mu_F \in S(L_1/F)} \Delta(\mu_F, \psi_F)$$

is equal to

$$\prod_{\mu_F \in S(L_1/F)} \Delta(\mu_F \mathcal{X}_F', \psi_F) \tag{12.1}$$

and

$$\Delta(\mathcal{X}_{L_2/F}', \psi_{L_2/F}) \ \prod_{\mu_F \in S(L_2/F)} \Delta(\mu_F, \psi_F)$$

is equal to

$$\prod_{\mu_F \in S(L_2/F)} \Delta(\mu_F \mathcal{X}_F', \psi_F). \tag{12.2}$$

Suppose $m' = m(\mathcal{X}_F') = 2d' + \varepsilon'$ and d' is greater than or equal to both $1+t_1$ and $1+t_2$. Choose γ in F such that

$$\gamma\, O_F = \mathcal{P}_F^{m'+n}$$

and then choose $\beta = \beta(\mathcal{X}_F)$. By Lemma 9.4 the expression (12.1) is equal to

$$\{\Delta(\mathcal{X}_F', \psi_F)\}^{\ell} \left\{ \prod_{\mu_F \in S(L_1/F)} \mu_F \left(\frac{\gamma}{\beta}\right) \right\}$$

and (12.2) is equal to

$$\{\Delta(\mathcal{X}_F', \psi_F)\}^{\ell} \left\{ \prod_{\mu_F \in S(L_2/F)} \mu_F \left(\frac{\gamma}{\beta}\right) \right\}.$$

Consequently

$$\Delta(\mathcal{X}_{L_1/F}', \psi_{L_1/F}) \left\{ \prod_{\mu_F \in S(L_1/F)} \mu_F \left(\frac{\beta}{\gamma}\right) \Delta(\mu_F, \psi_F) \right\}$$

is equal to

$$\Delta(\mathcal{X}_{L_2/F}', \psi_{L_2/F}) \left\{ \prod_{\mu_F \in S(L_2/F)} \mu_F \left(\frac{\beta}{\gamma}\right) \Delta(\mu_F, \psi_F) \right\}.$$

Suppose that both $m_1 = m(\mathcal{X}_{L_1})$ and $m_2 = m(\mathcal{X}_{L_2})$ are at least 2 and let $m_i = 2d_i + \varepsilon_i$. Suppose that

$$m(\mathcal{X}_{L_i}^{-1} \mathcal{X}_{L_i/F}') \le d_i$$

for i equal to 1 and 2. Then

$$m_i = m(\mathcal{X}'_{L_i/F}) = \psi_{L_i/F}(m'-1)+1.$$

If

$$\mathcal{X}'_{L_i/F}(1+x) = \psi_{L_i/F}\ \left(\frac{\beta_i x}{\gamma}\right)$$

for x in $\mathfrak{P}_{L_i}^{d_i+\varepsilon_i}$ then, by Lemma 9.4 again,

$$\Delta(\mathcal{X}_{L_i},\psi_{L_i/F}) = \mathcal{X}_{L_i}^{-1}\mathcal{X}'_{L_i/F}\ \left(\frac{\beta_i}{\gamma}\right)\ \Delta\,(\mathcal{X}'_{L_i/F},\psi_{L_i/F}).$$

Thus to prove Lemma 12.1 in the present circumstances we have only to verify that

$$\mathcal{X}_{L_1}^{-1}\mathcal{X}'_{L_1/F}\ \left(\frac{\beta_1}{\gamma}\right)\ \prod\nolimits_{\mu_F\in S(L_1/F)}\ \mu_F\ \left(\frac{\gamma}{\beta}\right)$$

is equal to

$$\mathcal{X}_{L_2}^{-1}\mathcal{X}'_{L_2/F}\ \left(\frac{\beta_2}{\gamma}\right)\ \prod\nolimits_{\mu_F\in S(L_2/F)}\ \mu_F\ \left(\frac{\gamma}{\beta}\right).$$

Suppose first that ℓ is odd. Then

$$\prod\nolimits_{\mu_F\in S(L_i/F)}\ \mu_F\ \left(\frac{\gamma}{\beta}\right) = 1$$

and we need only verify that

$$\mathcal{X}_{L_1}^{-1}\ \left(\frac{\gamma}{\beta_1}\right)\ \mathcal{X}'_{L_2/F}\ \left(\frac{\gamma}{\beta_2}\right) = \mathcal{X}_{L_2}^{-1}\ \left(\frac{\gamma}{\beta_2}\right)\ \mathcal{X}'_{L_2/F}\ \left(\frac{\gamma}{\beta_2}\right).$$

According to Lemmas 8.3 and 8.4 we may take $\beta_1=\beta_2=\beta$.

Certainly

$$\mathcal{X}'_{L_1/F}\ \left(\frac{\gamma}{\beta}\right) = \mathcal{X}'_F\ \left(\frac{\gamma^\ell}{\beta^\ell}\right) = \mathcal{X}'_{L_2/F}\ \left(\frac{\gamma}{\beta}\right).$$

Since C_F is the product of $N_{L_1/F}C_{L_1}$ and $N_{L_2/F}C_{L_2}$ we may write $\frac{\gamma}{\beta}$ as a product

$$\frac{\gamma}{\beta} = N_{L_1/F}\,\delta_1\ N_{L_2/F}\,\delta_2.$$

Consider

$$\mathcal{X}_{L_i}(N_{L_j/F}\delta_j) = \mathcal{X}_K(\delta_j)$$

where j is 1 or 2 according as i is 2 or 1. The right side equals

$$\mathcal{X}_{L_j}(\delta_j^\ell) = \mathcal{X}_{L_j}(N_{L_j/F}\,\delta_j)\ \prod\nolimits_{\sigma\in\mathfrak{G}(L_j/F)}\ \mathcal{X}_{L_j}(\delta_j^{1-\sigma}).$$

The product is equal to

$$\prod_{\mu_F \in S(L_i/F)} \mu_{L_j/F}(\delta_j)$$

which is 1 because ℓ is odd.

Before discussing the case $\ell = 2$ we consider the circumstances under which, for a given $\mathcal{X}_{L_1}$ and $\mathcal{X}_{L_2}$, a quasi-character $\mathcal{X}'_F$ with the properties described above exists.

Lemma 12.2

(a) *If L_i/F is unramified, x belongs to $U_{L_i}^{u_i+1}$, and*

$$N_{L_i/F}(x) = 1$$

then

$$\mathcal{X}_{L_i}(x) = 1.$$

(b) *If L_i/F is ramified, K/L_i is unramified, x belongs to $U_{L_i}^{t_i+1}$, and*

$$N_{L_i/F}(x) = 1$$

then

$$\mathcal{X}_{L_i}(x) = 1.$$

(c) *If L_i/F and K/L_i are ramified, x belongs to $U_{L_i}^{u_i+t_i+1}$, and*

$$N_{L_i/F}(x) = 1$$

then

$$\mathcal{X}_{L_i}(x) = 1.$$

Choose some non-trivial σ_i in $\overline{G}^i = \mathfrak{G}(L_i/F)$. Then

$$\mu_{L_i} = \mathcal{X}_{L_i}^{\sigma_i^{-1}-1}$$

is a non-trivial character in $S(K/L_i)$ and

$$m(\mu_{L_i}) = u_i + 1.$$

Since L_i/F is cyclic there is a y in C_{L_i} such that

$$x = y^{\sigma_i - 1}.$$

We shall show that y can be taken in $U_{L_i}^{u_i+1}$. Then

$$\mathcal{X}_{L_i}(x) = \mu_{L_i}(y) = 1.$$

Suppose L_i/F is unramified. If we cannot choose y in $U_{L_i}^{u_i+1}$ there is a largest integer $a \geq -1$ such that we can choose y in $U_{L_i}^a$ where a is of course less than $u_i + 1$. Choose such a y. Then a is not -1 because we can always divide y by a power of ϖ_F. If a were 0 then y could not be congruent to an element of U_F modulo $\mathfrak{P}_F$. Then $y^{\sigma_i - 1}$ would not be in U_F^1. Since $u_i + 1 > 0$ in the present situation this is impossible. Let

$$y = 1 + \varepsilon \varpi_F^a.$$

Then ε cannot be congruent to an element of O_F modulo $\mathfrak{P}_F$. Thus

$$\varepsilon^{\sigma_i} - \varepsilon \not\equiv 0 \pmod{\mathfrak{P}_{L_i}}$$

and

$$y^{\sigma_i - 1} \equiv 1 + (\varepsilon^{\sigma_i} - \varepsilon)\,\varpi_F^a \pmod{\mathfrak{P}_{L_i}^{a+1}}$$

is not in $U_{L_i}^{a+1}$. This is a contradiction.

Now suppose L_i/F is ramified and K/L_i is unramified. Then $t_i + 1 \geq 1$ and $u_i + 1 = 0$. We need only show that y can be taken to be a unit. Write

$$y = \varepsilon \varpi_{L_i}^b$$

where ε is a unit. If b is congruent to 0 modulo ℓ we can divide y by some power of ϖ_F to obtain an element of $U_F = U_F^0$. To see that b must be congruent to 0 modulo ℓ we suppose the contrary. Then

$$y^{\sigma_i - 1} = \varepsilon^{\sigma_i - 1}\,(\varpi_{L_i}^{\sigma_i - 1})^b \equiv (\varpi_{L_i}^{\sigma_i - 1})^b \pmod{\mathfrak{P}_{L_i}^{t_i+1}}.$$

If $t_i = 0$ the residue of $\varpi_{L_i}^{\sigma_i - 1}$ modulo $\mathfrak{P}_{L_i}$ is a non-trivial ℓth root of unity and

$$(\varpi_{L_i}^{\sigma_i - 1})^b \not\equiv 1 \pmod{\mathfrak{P}_{L_i}}.$$

If $t_i > 0$ then

$$\varpi_{L_i}^{\sigma_i - 1} = 1 + \alpha\,\varpi_{L_i}^{t_i}$$

where α is a unit. Thus

$$(\varpi_{L_i}^{\sigma_i - 1})^b \equiv 1 + \alpha\, b\; \varpi_{L_i}^{t_i} \pmod{\mathcal{P}_{L_i}^{t_i+1}}.$$

The right side is not congruent to 0 modulo $\mathfrak{P}_{L_i}^{t_i+1}$.

Now suppose L_i/F and K/L_i are both ramified. Then $\ell = p$ and both u_i and t_i are at least 1. Again suppose that y cannot be chosen in $U_{L_i}^{u_i+1}$ and let a be the largest integer such that y can be chosen in U^a. The argument just used shows that $a \geq 0$. Since L_i/F is ramified

$$U_{L_i}^{k_p} = U_F^k\, U_{L_i}^{k_p+1}.$$

Therefore a is not divisible by p and in particular is at least 1. Let

$$y = 1 + \varepsilon \varpi_{L_i}^a$$

where β is a unit. Then

$$y^{\sigma_i - 1} = (1 + \varepsilon^{\sigma_i} \varpi_{L_i}^{a\sigma_i})\; (1 + \varepsilon \varpi_{L_i}^a)^{-1}.$$

Let

$$\varepsilon^{\sigma_i} = \varepsilon + \eta\,\varpi_{L_i}^{t_i+1}$$

and

$$\varpi_{L_i}^{\sigma_i - 1} = 1 + \alpha\,\varpi_{L_i}^{t_i}$$

where α is a unit. Then $y^{\sigma_i - 1}$ is equal to

$$\left\{1 + (\varepsilon + \eta\,\varpi_{L_i}^{t_i+1})\;(1 + \alpha\,\varpi_{L_i}^{t_i})^a \varpi_{L_i}^a\right\}\;\left\{1 + \varepsilon\,\varpi_{L_i}^a\right\}^{-1}$$

which is congruent to

$$1 + a\alpha\varepsilon\,\varpi_{L_i}^{t_i+a}$$

modulo $\mathfrak{P}_{L_i}^{t_i+a+1}$. Therefore $a \geq u_i + 1$. This is a contradiction.

Lemma 12.3

If L_1/F is unramified we can choose $\mathcal{X}'_F$ such that

$$m(\mathcal{X}_{L_1}^{-1}\mathcal{X}'_{L_1/F}) = t + 1$$

and

$$m(\mathcal{X}_{L_2}^{-1}\mathcal{X}'_{L_2/F}) = t + 1.$$

If $m(\mathcal{X}_{L_1}) > t + 1$ then $m(\mathcal{X}'_F)$ will equal $m(\mathcal{X}_{L_1})$.

By the previous lemma we can define a quasi-character $\mathcal{X}'_F$ of

$$N_{L_1/F}U_{L_1}^{u_1+1}$$

by setting

$$\mathcal{X}'_F(N_{L_1/F}x) = \mathcal{X}_{L_1}(x).$$

We extend $\mathcal{X}'_F$ to a quasi-character, which we again denote by $\mathcal{X}'_F$, of C_F. Then

$$m(\mathcal{X}_{L_1}^{-1}\mathcal{X}'_{L_1/F}) \leq u_1 + 1.$$

However $\mathcal{X}_K^{-1}\mathcal{X}'_{K/F}$, $\mathcal{X}_{L_1}^{-1}\mathcal{X}'_{L_1/F}$, and $\mathcal{X}_{L_2}^{-1}\mathcal{X}'_{L_2/F}$ satisfy the conditions of Lemma 12.1. Therefore

$$m(\mathcal{X}_{L_1}^{-1}\mathcal{X}'_{L_1/F}) \geq u_1 + 1.$$

Since L_1/F is unramified u_1 and t_2 are both equal to t. Thus

$$m(\mathcal{X}_{L_1}^{-1}\mathcal{X}'_{L_1/F}) = t + 1$$

and

$$m(\mathcal{X}_{L_2}^{-1}\mathcal{X}'_{L_2/F}) = \ell(u_1 + 1) - \delta_2 = \ell(u_1 + 1) - (\ell - 1)\,(t_2 + 1) = t + 1.$$

The last assertion of the lemma is clear.

Lemma 12.4

If K/F is totally ramified then

$$m(\mathcal{X}_{L_i}) \geq t_i + u_i + 1.$$

There exists $\mathcal{X}'_F$ such that
$$m(\mathcal{X}_{L_i}^{-1}\mathcal{X}'_{L_i/F}) = t_i + u_i + 1$$
for i equal to 1 and 2.

In the present circumstances t_i and u_i are both at least 1. Choose a non-trivial σ_i in $\overline{G}^i$ and let
$$\mu_{L_i} = \mathcal{X}_{L_i}^{\sigma_i^{-1}-1}$$
as before. Choose y in $U_{L_i}^{u_i}$ so that
$$\mu_{L_i}(y) \neq 1.$$
Then
$$\mathcal{X}_{L_i}(y^{\sigma_i-1}) \neq 1.$$
However if
$$y = 1 + \varepsilon\,\varpi_{L_i}^{u_i}$$
where ε is a unit then
$$y^{\sigma_i-1} \equiv 1 + u_i\alpha\,\varepsilon\,\varpi_{L_i}^{t_i+u_i} \pmod{\mathfrak{P}_{L_i}^{t_i+u_i+1}}$$
if
$$\varpi_{L_i}^{\sigma_i-1} = 1 + \alpha\,\varpi_{L_i}^{t_i}.$$
In particular
$$y^{\sigma_i-1} \in U_{L_i}^{t_i+u_i}$$
so that
$$m(\mathcal{X}_{L_i}) \geq t_i + u_i + 1.$$

Just as in the previous lemma we can find a quasi-character $\mathcal{X}'_F$ of C_F such that
$$m(\mathcal{X}_{L_1}^{-1}\mathcal{X}'_{L_1/F}) = t_1 + u_1 + 1.$$
We have seen that $m_1 + \delta_1 = m_2 + \delta_2$. The same argument shows that
$$m(\mathcal{X}_{L_1}^{-1}\mathcal{X}'_{L_1/F}) + \delta_1 = m(\mathcal{X}_{L_2}^{-1}\mathcal{X}'_{L_2/F}) + \delta_2.$$
To complete the proof of the lemma we show that
$$t_1 + u_1 + \delta_1 = t_2 + u_2 + \delta_2.$$
Since
$$\delta_i = (\ell - 1)\,(t_i + 1)$$
we have only to show that
$$u_1 + 1 + \ell(t_1 + 1) = u_2 + 1 + \ell(t_2 + 1).$$
Multiplying the left or the right side by $\ell - 1$ we obtain $\delta(K/F)$. The equality follows immediately.

Lemmas 12.3 and 12.4 together with the remarks which provoked them allow us to prove Lemma 12.1 in many, but by no means all, cases. We shall not however apply these lemmas immediately. We shall rather begin the systematic exposition of the proof of Lemma 12.1 taking up the cases to which these lemmas apply in their turn.

Suppose first that L_1 is unramified over F. As before $m_i = m(\mathcal{X}_{L_i})$. Then

$$m_2 = m_1 + (\ell - 1)\,(m_1 - t - 1) \geq m_1$$

because $u_1 = t$. Since the number m_1 is at least $t+1$ and $t \geq 0$ it is at least 1. If $m_1 = 1$ then $t = 0$ and $m_2 = 1$. Once we have treated this case, as we shall immediately, we may suppose that $m_2 \geq m_1 > 1$.

If $m_2 = 1$ let

$$\lambda = O_{L_2}/\mathfrak{P}_{L_2} = O_F/\mathfrak{P}_F$$

and let

$$\kappa = O_K/\mathfrak{P}_K = O_{L_1}/\mathfrak{P}_{L_1}.$$

κ is an extension of λ. The restriction of $\mathcal{X}_{L_1}$ to U_{L_1} defines a character $\mathcal{X}_\lambda$ of λ^* and the restriction of $\mathcal{X}_{L_2}$ to U_K defines a character $\mathcal{X}_\kappa$ of κ^*. The restriction of $\mathcal{X}_K$ to U_K defines a character of κ^* which is equal to $\mathcal{X}_{\kappa/\lambda}$ and to $\mathcal{X}_\kappa^\ell$ so that

$$\mathcal{X}_\kappa^\ell = \mathcal{X}_{\kappa/\lambda}.$$

As σ varies over $\overline{G}^2$, $\varpi_{L_2}^{\sigma-1}$, taken modulo $\mathcal{P}_{L_2}$, varies over the ℓth roots of unity in λ and if

$$\mathcal{X}_{L_2}^{\sigma^{-1}-1} = \nu$$

then

$$\mathcal{X}_\lambda(\varpi_{L_2}^{\sigma-1}) = \nu(\varpi_{L_2}).$$

The right side is not 1 if $\sigma \neq 1$ because ν is then non-trivial. Thus the restriction of $\mathcal{X}_\lambda$ to the ℓth roots of unity is not trivial. To every μ_F in $S(L_2/F)$ is associated a character μ_λ of λ^* which is of order 1 if $\mu_F = 1$ and of order ℓ otherwise. If ψ_λ is the additive character of λ defined by

$$\psi_\lambda(x) = \psi_F\ \left(\frac{x}{\varpi_F^{1+n}}\right)$$

then

$$\Delta_1(\mu_F, \psi_F, \varpi_F^{1+n}) = A\ [-\tau(\mu_\lambda, \psi_\lambda)]$$

if μ_F is not trivial. Moreover

$$\psi_{L_2/F}\ \left(\frac{x}{\varpi_F^{1+n}}\right) = \psi_\lambda(\ell\, x)$$

and

$$\Delta_1(\mathcal{X}_{L_2}, \psi_{L_2/F}, \varpi_F^{1+n}) = A\ [-\mathcal{X}_\lambda(\ell)\tau(\mathcal{X}_\lambda, \psi_\lambda)].$$

Finally

$$\Delta_1(\mathcal{X}_{L_1}, \psi_{L_1/F}, \varpi_F^{1+n}) = A\ [-\tau(\mathcal{X}_\kappa, \psi_{\kappa/\lambda})].$$

Thus the required identity is a consequence of the relation

$$\tau(\mathcal{X}_\kappa, \psi_{\kappa/\lambda}) = \mathcal{X}_\lambda(\ell)\tau(\mathcal{X}_\lambda, \psi_\lambda)\ \prod\nolimits_{\mu_\lambda \neq 1} \tau(\mu_\lambda, \psi_\lambda)$$

which we proved as Lemma 7.9.

Retaining the assumption that L_1/F is unramified we now suppose that $m_1 > 1$. There are two possibilities.

(a)
$$m_1 \geq 2(t+1)$$

(b)
$$t+1 \leq m_1 < 2(t+1).$$

The second possibility occurs only when $t > 0$.

If $m_j \geq 2(t+1)$ choose $\mathcal{X}'_F$ so that

$$m(\mathcal{X}_{L_i}^{-1}\mathcal{X}'_{L_i/F}) = t+1$$

for $i = 1$ and 2. It is clear that
$$m(\mathcal{X}_{L_1}^{-1}\mathcal{X}'_{L_1/F}) \leq d_1$$
if $m_i = 2di + \varepsilon_i$. Since $m_2 \geq m_1$ we also have

$$m(\mathcal{X}_{L_2}^{-1}\mathcal{X}'_{L_2/F}) \leq d_2.$$

Moreover
$$m' = m(\mathcal{X}'_F) = m_1$$
so that d' is greater than or equal to both $1+t_2 = 1+t$ and $1+t_1 = 0$. Lemma 12.1 for $L_{1/F}$ unramified and $m_1 \geq 2(t+1)$, follows immediately if ℓ is odd. Suppose $\ell = 2$.

If $t = 0$ we can invoke Lemmas 8.3 and 8.7 to see that if $\beta = \beta(\mathcal{X}'_F)$ we may choose $\beta_1 = \beta(\chi_{L_1/F})$ and $\beta_2 = \beta(\mathcal{X}'_{L_2/F})$ equal to β. If $\mu_F^{(1)}$ is the non-trivial element of $S(L_1/F)$ and $\mu_F^{(2)}$ is the non-trivial element of $S(L_2/F)$ we have only to show that

$$\mathcal{X}_{L_1}\left(\frac{\gamma}{\beta}\right)\ \mathcal{X}'_{L_1/F}\left(\frac{\beta}{\gamma}\right)\ \mu_F^{(1)}\left(\frac{\gamma}{\beta}\right)$$

is equal to
$$\mathcal{X}_{L_2}\left(\frac{\gamma}{\beta}\right)\ \mathcal{X}'_{L_2/F}\left(\frac{\beta}{\gamma}\right)\ \mu_F^{(2)}\left(\frac{\gamma}{\beta}\right).$$

Certainly
$$\mathcal{X}'_{L_1/F}\left(\frac{\beta}{\gamma}\right) = \mathcal{X}'_{L_2/F}\left(\frac{\beta}{\gamma}\right)$$

and we need only show that if δ is in C_F then

$$\mathcal{X}_{L_1}(\delta)\,\mu_F^{(1)}(\delta) = \mathcal{X}_{L_2}(\delta)\,\mu_F^{(2)}(\delta).$$

We may write
$$\delta = N_{L_1/F}\,\delta_1\ N_{L_2/F}\,\delta_2.$$

Then

$$\mu_F^{(i)}(N_{L_1/F}\,\delta_i) = 1$$

and, if j is 1 or 2 according as i is 2 or 1,

$$\mathcal{X}_{L_i}(N_{L_j/F}\,\delta_j) = \mathcal{X}_K(\delta_j) = \mathcal{X}_{L_j}(\delta_j^2)$$

which equals

$$\mathcal{X}_{L_j}(N_{L_j/F}\,\delta_j)\mu_{L_j/F}^{(i)}(\delta_j) = \mathcal{X}_{L_j}(N_{L_j/F}\,\delta_j)\mu_F^{(i)}(N_{L_j/F}\,\delta_j).$$

The required equality follows immediately.

If t is positive we may still choose $\beta_1 = \beta$. If $m_1 - t - 1 = v$ then, by Lemma 8.6, we may choose β_2 in the form

$$\beta_2 = \beta + \eta$$

with η in $\mathfrak{P}_{L_2}^v$. Since $v \geq t+1$

$$\mathcal{X}_{L_2}^{-1}(\beta_2)\mathcal{X}'_{L_2/F}(\beta_2) = \mathcal{X}_{L_2}^{-1}(\beta)\mathcal{X}'_{L_2/F}(\beta).$$

This observation made, we can proceed as before.

Some preparation is necessary before we discuss the second possibility. Suppose that t is positive so that ℓ is equal to the residual characteristic p. The finite field $\lambda_1 = O_{L_1}/\mathcal{P}_{L_1}$ is an extension of degree p of $\phi = O_F/\mathcal{P}_F$.

The map

$$x \longrightarrow x^p - x$$

is an additive endomorphism of ϕ with the prime field as kernel. Choose a y in ϕ which is not in the image of this map and consider the equation

$$x^p - x = y.$$

If x, in some extension field of ϕ, satisfies this equation and ϕ has q elements then $x^q \neq x$. However

$$(x^q - x)^p - (x^q - x) = (x^p - x)^q - (x^p - x) = y^q - y = 0.$$

So

$$x^q - x = z$$

where z is a non-zero element of the prime field. Then

$$x^{q^2} = (x+z)^q = x^q + z = x + 2z$$

and in general

$$x^{q^n} = x + nz.$$

Thus the lowest power n of q such that $x^{q^n} = x$ is $n = p$ and x determines an extension of degree p. Consequently x may be chosen to lie in λ_1 and then $\lambda_1 = \phi(x)$.

Let $E^r(x)$ be the rth elementary symmetric function of x and its conjugates. Since

$$x^p - x + (-1)^p N_{\lambda_1/\phi} x = 0 \tag{12.3}$$

we have

$$E^r(x) = 0 \tag{12.4}$$

if $1 \leq r < p - i$,

$$E^{p-1}(x) = (-1)^p \tag{12.5}$$

and, of course,

$$E^p(x) = N_{\lambda_1/\phi} x. \tag{12.6}$$

If λ is a non-zero element of the prime field we can replace y by λy. Then x is to be replaced by λx. Also we can replace x by $x + \lambda$ without changing y.

Let $R(L_1)$ be the set of $(q^p - 1)$th roots of unity in L_1. Choose a γ in $R(L_1)$ whose image in λ_1 is x. If we are dealing with fields of power series γ will also satisfy the equations (12.3), (12.4), (12.5) and (12.6). Let us see how these equations are to be modified for fields of characteristic zero. F and L_1 are then extensions of the p-adic field $\mathbb{Q}_p$. Let F^0 and L_1^0 be the maximal unramified extensions of $\mathbb{Q}_p$ contained in F and L_1 respectively. $R(L_1)$ is a subset of L_1^0 and p generates the ideal $\mathfrak{P}_{F^0}$ and the ideal $\mathfrak{P}_{L_1^0}$. Thus

$$\gamma^p - \gamma + (-1)^p\, N_{L_1/F}\, \gamma \equiv 0 \pmod p$$

and

$$E^r(\gamma) \equiv 0 \pmod p$$

if $1 \leq r < p - 1$ while

$$E^{p-1}(\gamma) \equiv (-1)^p \pmod p.$$

Let

$$S^r(\gamma) = \sum\nolimits_{\sigma \in \mathfrak{G}(L_1/F)} \gamma^{r\sigma}.$$

The following relations are special cases of Newton's formulae.

$$
\begin{aligned}
S^1(\gamma) - E^1(\gamma) &= 0 \\
S^2(\gamma) - E^1(\gamma)\, S^1(\gamma) + 2E^2(\gamma) &= 0 \\
S^3(\gamma) - E^1(\gamma)\, S^2(\gamma) + E^2(\gamma)\, S^1(\gamma) - 3E^3(\gamma) &= 0 \\
&\vdots \\
S^{p-1}(\gamma) - E^1(\gamma)\, S^{p-2}(\gamma) + \ldots + (-1)^{p-1}(p-1)E^{p-1}(\gamma) &= 0 \\
S^p(\gamma) - E^1(\gamma)\, S^{p-1}(\gamma) + \ldots + (-1)^p p\, E^p(\gamma) &= 0.
\end{aligned}
$$

We infer that

$$S^r(\gamma) \equiv 0 \pmod p$$

if $1 \leq r < p-1$ and that

$$S^{p-1}(\gamma) \equiv (-1)^p (p-1)\, E^{p-1}(\gamma) \pmod p.$$

Combining the first of these congruences with Newton's formulae we obtain

$$S^r(\gamma) \equiv r(-1)^{r+1}\, E^r(\gamma) \pmod{p^2}$$

if $1 \leq r \leq p-1$. If p is odd

$$S^p(\gamma) - p\, E^p(\gamma) \equiv E^1(\gamma)\, S^{p-1}(\gamma) - E^{p-1}(\gamma)\, S^1(\gamma) \pmod{p^2}.$$

The right side is equal to

$$E^1(\gamma)\, (S^{p-1}(\gamma) - E^{p-1}(\gamma)) \equiv 0 \pmod{p^2}.$$

If p is even

$$S^2(\gamma) + 2E^2(\gamma) = \{E^1(\gamma)\}^2.$$

Since

$$E^1(\gamma) \equiv 1 \pmod 2$$

we have

$$S^2(\gamma) + 2E^2(\gamma) \equiv 1 \pmod 4.$$

If $\sigma \neq 1$ belongs to $\mathfrak{G}(L_1/F)$ there is a $(p-1)$th root of unity ζ such that

$$\gamma^\sigma - \gamma \equiv \zeta \pmod p.$$

By a suitable choice of y the root ζ can be made to equal, for a given σ, any chosen $(p-1)$th root of unity.

The above relations are of course also valid when F is a field of power series.

Choose a non-trivial character μ_F in $S(L_2/F)$ and choose α so that

$$\mu_F(1+x) = \psi_F \left(\frac{\alpha\, x}{\varpi_F^{t+1+n}} \right)$$

if x is in $\mathfrak{P}_F^s$. Here s is the least integer greater than or equal to $\frac{t+1}{2}$. If ζ is a $(p-1)$th root of unity we define μ_F^ζ to be μ_F^j if j is the unique integer such that

$$\zeta \equiv j \pmod p.$$

As we observed in the proof of Lemma 8.5

$$\mu_F^\zeta(1+x) = \psi_F\ \left(\frac{\alpha\,\zeta x}{\varpi_F^{1+t+n}}\right)$$

if x is in $\mathfrak{P}_F^s$.

Let $m_i = 2d_i + \varepsilon_i$ as usual. If β_1 in L_1 is such that

$$\mathcal{X}_{L_1}(1+x) = \psi_{L_1/F}\ \left(\frac{\alpha\beta_1 x}{\varpi_F^{m_1+n_1}}\right)$$

for x in $\mathfrak{P}_{L_1}^{d_1+\varepsilon_1}$ then, if $\sigma \neq 1$ belongs to $\overline{G}^1 = \mathfrak{G}(L_1/F)$ and x belongs to $\mathfrak{P}_{L_1}^{d_1+\varepsilon_1}$,

$$\psi_{L_1/F}\ \left(\frac{\alpha(\beta_1^\sigma - \beta_1)x}{\varpi_F^{m_1+n_2}}\right) = \mathcal{X}_{L_1}^{\sigma-1}(1+x)$$

is equal to

$$\psi_{L_1/F}\ \left(\frac{\alpha\zeta_\sigma x}{\varpi_F^{1+t+n}}\right)$$

if ζ_σ is such that

$$\mathcal{X}_{L_1}^{\sigma-1} = \mu_F^{\zeta_\sigma}.$$

Thus if

$$v = m_1 - 1 - t$$

we have

$$\beta_1^\sigma - \beta_1 \equiv \zeta_\sigma\,\varpi_F^v \pmod{\mathfrak{P}_{L_1}^{d_1}}.$$

It is clear that

$$\zeta_{\sigma\tau} \equiv \zeta_\sigma^\tau + \zeta_\sigma \pmod{\mathfrak{P}_{L_1}}.$$

Suppose

$$\gamma^\sigma - \gamma \equiv \xi_\sigma \pmod p$$

where ξ_σ is also a $(p-1)$th root of unity. Then

$$\xi_{\sigma\tau} \equiv \xi_\sigma^\tau + \xi_\sigma \pmod{\mathfrak{P}_{L_1}}.$$

We observed that we could arrange that

$$\xi_\sigma = \zeta_\sigma$$

for one non-trivial σ. Once we do this the equality will hold for all σ. Then $\gamma^{p\sigma} - \gamma^p \equiv \xi_\sigma \pmod p$ and

$$(\beta_1 - \gamma^p\varpi_F^v)^\sigma \equiv \beta_1 - \gamma^p\varpi_F^v \pmod{\mathfrak{P}_{L_1}^{d_1}}$$

for all σ because, as we observed in the proof of Lemma 8.5, p belongs to $\mathcal{P}_{L_1}^r$ if $r+s=t+1$ and

$$2(r+v) \geq t+2v = 2m_1 - 2 - 2t + t$$

which is at least

$$(m_1-1)+(m_1-1-t) \geq m_1 - 1$$

so that $r+v \geq d_1$. Since L_1/F is unramified there is therefore a β in F such that

$$\beta_1 - \gamma^p \varpi_F^v \equiv \beta \pmod{\mathfrak{P}_{L_1}^{d_1}}.$$

We may suppose that

$$\beta_1 = \beta + \gamma^p \varpi_F^v.$$

β is a unit unless $v=0$. If $v=0$ then, by replacing γ by a root of unity congruent to $\gamma+1$ modulo $\mathfrak{P}_{L_1}$ if necessary, we can still arrange that β is a unit. β is congruent to a norm $N_{L_2/F}\beta'$ modulo $\mathcal{P}_F^t$. Since $d_1 \leq t$ we*

*(1998) At the moment this is all that could be found of Chapter 12.

Chapter Thirteen.

The Third Main Lemma

Suppose K/F is Galois and $G = \mathfrak{G}(K/F)$. Suppose $G = HC$ when $H \neq \{1\}$, $H \cap C = \{1\}$, and C is a non-trivial abelian normal subgroup of G which is contained in every non-trivial normal subgroup of G.

Lemma 13.1

Let E be the fixed field of H and let $\mathcal{X}_F$ be a quasi-character of C_F. If $m = m(\mathcal{X}_F)$ then

$$m(\mathcal{X}_{E/F}) = \psi_{E/F}(m-1) + 1.$$

Set

$$m' = m(\mathcal{X}_{E/F}) - 1.$$

Observe that $m' - 1$ is the greatest lower bound of all real numbers $v > -1$ such that $\mathcal{X}_{E/F}$ is trivial on U_E^v and that $m-1$ is the greatest lower bound of all real numbers u such that $\mathcal{X}_F$ is trivial on U_F^u. Since

$$N_{E/F}(U_E^{\psi_{E/F}(u)}) \subseteq U_F^u$$

we see immediately that

$$m' - 1 \leq \psi_{E/F}(m-1).$$

To prove the lemma we need only show that

$$N_{E/F}(U_E^{\psi_{E/F}(m-1)}) \supseteq U_F^{m-1}.$$

We show this with $m-1$ replaced by any $u \geq -1$.

By Lemma 6.15, $\tau_{K/F}$ maps $W_{K/F}^u$ onto U_F^u. The projection of $W_{K/F}^u$ on G is a normal subgroup of G. Thus it is either $\{1\}$ or a subgroup containing C. If it is $\{1\}$ then

$$W_{K/F}^u = W_{K/F}^u \cap C_K = U_K^{\psi_{K/F}(u)}$$

and

$$U_F^u = N_{K/F}(U_K^{\psi_{K/F}(u)}) = N_{E/F}(N_{K/E}U_K^{\psi_{K/F}(u)})$$

which, by Lemma 6.6, is contained in

$$N_{E/F}(U_E^{\psi_{E/F}(u)}).$$

Suppose the projection is not $\{1\}$. If L is the fixed field of C the group $W_{K/F}^u$ contains

$$\{wvw^{-1}v^{-1} \mid w \in W_{K/F}, v \in W_{K/F}^u \cap W_{K/L}\}. \tag{13.1}$$

Since C is generated by

$$\{\sigma\rho\sigma^{-1}\rho^{-1} \mid \sigma \in G,\ \rho \in C\}$$

the group generated by the set (13.1) contains a set of representatives for the cosets of C_K in $W_{K/L}$. This group clearly lies in the kernel of $\tau_{K/F}$. Thus every element of $W^u_{K/F}$ is congruent modulo the kernel of $\tau_{K/F}$ in $W^u_{K/F}$ to an element of

$$W^u_{K/F} \cap W_{K/E} = W^{\psi_{E/F}(u)}_{K/E}$$

and

$$U^u_F = \tau_{K/F}(W^u_{K/F}) = \tau_{K/F}(W^{\psi_{E/F}(u)}_{K/E})$$

which is

$$N_{E/F}(\tau_{K/E}(W^{\psi_{E/F}(u)}_{K/E}))$$

and this set is contained in

$$N_{E/F}(U^{\psi_{E/F}(u)}_E).$$

Suppose F_1 is non-archimedean, K_1/F_1 is Galois and $F_1 \subseteq E_1 \subseteq K_1$. Let μ_1 be a character of $\mathfrak{G}(K_1/E_1)$. We may also regard μ_1 as a character of C_{E_1}. Let σ be an element of $\mathfrak{G}(K_1/F_1)$ and define the character of μ_1^σ of $\mathfrak{G}(K_1/E_1^\sigma)$ by

$$\mu_1^\sigma(\rho) = \mu_1(\sigma\rho\sigma^{-1})$$

for $\rho \in \mathfrak{G}(K_1/E_1^\sigma)$ or, what amounts to the same

$$\mu_1^\sigma(\alpha) = \mu_1(\alpha^{\sigma^{-1}})$$

for $\alpha \in C_{E_1^\sigma}$. Since

$$\psi_{E_1^\sigma/F_1}(\alpha) = \psi_{E_1/F_1}(\alpha^{\sigma^{-1}})$$

the next lemma is a congruence of the definitions.

Lemma 13.2

$$\Delta(\mu_1^\sigma, \psi_{E_1^\sigma/F_1}) = \Delta(\mu_1, \psi_{E_1/F_1}).$$

We return to the extension K/L and the group G. Let T be a set of representatives for the orbits under G of the non-trivial characters in $S(K/L)$. If $\mu \in T$ let G_μ be the isotropy group of μ and let F_μ be the fixed field of G_μ. Let $H_\mu = H \cap G_\mu$. Since C is contained in G_μ we have $G_\mu = H_\mu \cdot C$. Then μ may also be regarded as a character of C. Let μ' be the character of G_μ defined by

$$\mu'(hc) = \mu(c)$$

if $h \in H_\mu$ and $c \in C$. Eventually we must show that

$$\Delta(\mathcal{X}_{E/F}, \psi_{E/F}) \prod_{\mu\in T} \Delta(\mu', \psi_{F_\mu/F}) \tag{13.2}$$

is equal to

$$\Delta(\mathcal{X}_F, \psi_F) \prod_{\mu\in T} \Delta(\mu'\mathcal{X}_{F_\mu/F}, \psi_{F_\mu/F}) \tag{13.3}$$

if $\mathcal{X}_F$ is a quasi-character of C_F. At the moment we content ourselves with a special case. The next lemma will be referred to as the Third Main Lemma.

Lemma 13.3

If K/F is tamely ramified the expressions (13.2) and (13.3) are equal.

As we observed in Lemma 6.4 the extension L/F will be unramified and $\ell = [C : 1]$ will be a prime. Choose a generator ϖ_F of $\mathfrak{P}_F$. Since F_μ/F is unramified we may choose $\varpi_{F_\mu} = \varpi_F$. Choose ϖ_E so that $N_{E/F}\,\varpi_E = \varpi_F$. Certainly

$$\delta_{L/F} = \delta_{K/E} = 0$$

while

$$\delta_{K/L} = \ell - 1.$$

Since

$$\delta_{K/F} = \delta_{K/L} + \ell\,\delta_{L/F} = \delta_{K/E} + \delta_{E/F}$$

we conclude that

$$\delta_{E/F} = \ell - 1.$$

Clearly

$$\sum\nolimits_\mu [F_\mu : F] = \sum\nolimits_\mu [H : H_\mu] = \sum\nolimits_\mu [G : G_\mu]$$

is just the number of non-trivial characters in $S(K/L)$, that is $\ell - 1$. Moreover $m(\mu') = 1$. Let E_μ be the fixed field of H_μ. Then

$$N_{E_\mu/F_\mu}(\varpi_E) = N_{E/F}(\varpi_E) = \varpi_F.$$

Thus, as an element of C_{F_μ}, ϖ_F lies in the image of W_{K/E_μ} under τ_{K/F_μ} and hence $\mu'(\varpi_F) = 1$. Also

$$n(\psi_{E/F}) = \ell n(\psi_F) + \delta_{E/F} = \ell n + (\ell - 1)$$

while

$$n(\psi_{F_\mu/F}) = n.$$

If $m = m(\mathcal{X}_F) = 0$ then

$$m(\mathcal{X}_{E/F}) = m(\mathcal{X}_{F_\mu/F}) = 0$$

and

$$\mathcal{X}_{E/F}(\varpi_E^{\ell n+\ell-1}) = \mathcal{X}_F(\varpi_F^{\ell n+\ell-1}) = \mathcal{X}_F(\varpi_F^n)\prod\nolimits_\mu \mathcal{X}_{F_\mu/F}(\varpi_F^{1+n})$$

so that the lemma amounts to the equality

$$\prod\nolimits_\mu \Delta_1(\mu, \psi_{F_\mu/F}, \varpi_F^{1+n}) = \prod\nolimits_\mu \Delta_1(\mu, \psi_{F_\mu/F}, \varpi_F^{1+n}).$$

If $m > 0$ then, by Lemma 6.4,

$$m(\mathcal{X}_{E/F}) = \ell m - (\ell - 1)$$

and

$$m(\mathcal{X}_{E/F}) + n(\psi_{E/F}) = \ell(m + n).$$

Since K/E is unramified
$$m(\mathcal{X}_{K/F}) = m(\mathcal{X}_{E/F}) = \ell m - (\ell - 1).$$
However
$$\mathcal{X}_{K/F} = (\mu' \mathcal{X}_{F_\mu/F})_{K/F_\mu}$$
so that
$$\psi_{K/F_\mu}(m(\mu' \mathcal{X}_{F_\mu/F}) - 1) \geq m(\mathcal{X}_{K/F}) - 1 = \ell(m-1)$$
or
$$m(\mu' \mathcal{X}_{F_\mu/F}) - 1 \geq \varphi_{K/F_\mu}(\ell(m-1)) = m - 1.$$
Consequently
$$m(\mu' \mathcal{X}_{F_\mu/F}) \geq m.$$
Since it is clearly less than or equal to m it is equal to m. Because
$$\mathcal{X}_{E/F}(\varpi_F^{m+n}) = \mathcal{X}_F(\varpi_F^{\ell(m+n)}) = \mathcal{X}_F(\varpi_F^{m+n}) \prod\nolimits_\mu \mathcal{X}_{F_\mu/F}(\varpi_F^{m+n})$$
we have to show that
$$\Delta_1(\mathcal{X}_{E/F}, \psi_{E/F}, \varpi_F^{m+n}) \prod \Delta_1(\mu', \psi_{F_\mu/F}, \varpi_F^{m+n})$$
is equal to
$$\Delta_1(\mathcal{X}_F, \psi_F, \varpi_F^{m+n}) \prod \Delta_1(\mu' \mathcal{X}_{F_\mu/F}, \psi_{F_\mu/F}, \varpi_F^{m+n}).$$

Let ϕ be the field $O_F/\mathcal{P}_F$, let $\lambda = O_L/\mathcal{P}_L$, let q be the number of elements in ϕ, and let
$$f = [\lambda : \phi] = [L : F].$$
Let θ be the homomorphism of C into λ^* introduced in Chapter IV of Serre's book. Thus
$$\theta(c) = \varpi_E^{c-1} \pmod{\mathfrak{P}_F}$$
so that if $h \in H$
$$\theta(h^{-1}ch) \equiv (\varpi_E^{h^{-1}c - h^{-1}}) \equiv (\varpi_E^{c-1})^h \equiv \theta(c)^h.$$
Let h_0 be that element of H such that
$$\alpha^{h_0} = \alpha^q$$
if $\alpha \in \lambda$ and let c_0 be a generator of C. Then $\theta(c_0)$ has order ℓ and, since the centralizer of C in H is $\{1\}$,
$$\theta(h_0^{-r} c h_0^r) = \theta(c_0)^{q^r}$$
is $\theta(c_0)$ if and only if f divides r. On the other hand, it is $\theta(c_0)$ if and only if ℓ divides $q^r - 1$. Thus the order of q modulo ℓ is f. We also observe that both C and its dual group are cyclic of prime order so that any element of H which fixed an element of T would act trivially on the dual group and therefore on C itself. It follows that $F_\mu = L$ for all μ in T.

Suppose first that $m = 1$. Let ψ_ϕ be the character
$$\psi_\phi(x) = \psi_F \left(\frac{x}{\varpi_F^{1+n}} \right)$$

on ϕ. Since $O_E/\mathfrak{P}_E$ is naturally isomorphic to $O_F/\mathfrak{P}_F$ and the map $x \longrightarrow N_{E/F}x$ gives the map $x \longrightarrow x^\ell$ of ϕ into itself while the map $x \longrightarrow S_{E/F}x$ induces the map $x \longrightarrow \ell x$ the required identity reduces to the equality of

$$\mathcal{X}_\phi(\ell^\ell)\tau(\mathcal{X}_\phi^\ell, \psi_\phi) \prod\nolimits_{\mu\in T} \tau(\mu_\lambda, \psi_{\lambda/\phi})$$

and

$$\tau(\mathcal{X}_\phi, \psi_\phi) \prod\nolimits_{\mu\in T} \tau(\mu_\lambda \mathcal{X}_{\lambda/\phi}, \psi_{\lambda/\phi}).$$

This equality has been proved in Lemma 7.8.

Now let m be greater than 1. Since $F_\mu = 1$ for all μ we are trying to show that

$$\Delta_1(\mathcal{X}_{E/F}, \psi_{E/F}, \varpi_F^{m+n}) \prod \Delta_1(\mu, \psi_{L/F}, \varpi_F^{m+n})$$

is equal to

$$\Delta_1(\mathcal{X}_F, \psi_F, \varpi_F^{m+n}) \prod \Delta_1(\mu\mathcal{X}_{L/F}, \psi_{L/F}, \varpi_F^{m+n}).$$

Since the action of H on C is not trivial ℓ cannot be 2. If μ lies in T and μ^{-1} lies in the orbit of ν then

$$\Delta_1(\nu, \psi_{L/F}, \varpi_F^{m+n}) = \Delta_1(\mu^{-1}, \psi_{L/F}, \varpi_F^{m+n})$$

is $\mu(-1)$ times the complex conjugate of

$$\Delta_1(\mu, \psi_{L/F}, \varpi_F^{m+n}).$$

Since the order of μ is ℓ, $\mu(-1) = 1$ and, if $\mu \neq \nu$, the product of the two terms corresponding to μ and ν is 1. If

$$\mu^{-1} = \mu^{q^r}$$

with $0 \leq r < f$ lies in the orbit of μ then ℓ divides $q^r + 1$. Thus ℓ divides $q^{2r} - 1$ and $2r = f$. By Lemma 7.1

$$|\,\tau(\mu_\lambda, \psi_{\lambda/\phi})\,| = \sqrt{q}^f = q^r$$

and

$$\tau(\mu_\lambda, \psi_{\lambda/\phi}) = -\Delta_1(\mu, \psi_{L/F}, \varpi_F^{1+n})q^r$$

if $\psi_{\lambda/\phi}$ has the same meaning as before and μ_λ is the character of λ^* induced by μ. Since

$$\delta = \Delta_1(\mu, \psi_{L/F}, \varpi_F^{1+n})$$

is its own complex conjugate, it is ± 1. If $\alpha \in \phi$ then

$$\mu^{-1}(\alpha) = \mu(\alpha^{q^r}) = \mu(\alpha).$$

Since $u(\alpha)$ is an ℓth root of unity it is 1. Thus

$$\tau(\mu_\lambda, \psi_{\lambda/\phi}) = \tau(\mu_\lambda).$$

However it follows from Lemma 7.1 that

$$\tau(\mu_\lambda) \equiv 1 \pmod{\eta}$$

where η is a number in $\mathfrak{k}_{p(q^f-1)}$ which is not a unit and whose only prime divisors are divisors of ℓ. Thus

$$-\delta q^r = \tau(\mu_\lambda) \equiv 1 \pmod{\ell}$$

and $\delta = 1$. We are reduced to showing that

$$\Delta_1(\mathcal{X}_{E/F}, \psi_{E/F}, \varpi_F^{m+n})$$

is equal to

$$\Delta_1(\mathcal{X}_F, \psi_F, \varpi_F^{m+n}) \prod \Delta_1(\mu\mathcal{X}_{L/F}, \psi_{L/F}, \varpi_F^{m+n})$$

Let $\beta = \beta(\mathcal{X}_F)$. By repeated applications of Lemma 8.9 we see that we may take

$$\beta(\mathcal{X}_{L/F}) = \beta(\mathcal{X}_{K/F}) = \beta(\mu\mathcal{X}_{L/F}) = \beta.$$

If $\beta(\mathcal{X}_{E/F})$ is chosen we could also take

$$\beta(\mathcal{X}_{K/F}) = \beta(\mathcal{X}_{E/F}).$$

Thus if

$$m' = m(\mathcal{X}_{E/F}) = m(\mathcal{X}_{K/F}) = 2d' + \varepsilon'$$

we have

$$\beta \equiv \beta(\mathcal{X}_{E/F}) \pmod{\mathfrak{P}_K^{d'}}.$$

Since both sides of the congruence lie in E

$$\beta \equiv \beta(\mathcal{X}_{E/F}) \pmod{\mathfrak{P}_E^{d'}}$$

and we may take

$$\beta(\mathcal{X}_{E/F}) = \beta.$$

Then

$$\Delta_2(\mathcal{X}_{E/F}, \psi_{E/F}, \varpi_F^{m+n}) = \psi_F \left(\frac{\ell\beta}{\varpi_F^{m+n}}\right) \mathcal{X}_F^{-1}(\beta^\ell)$$

while

$$\Delta_2(\mathcal{X}_F, \psi_F, \varpi_F^{m+n}) \prod\nolimits_{\mu\in T} \Delta_2(\mu\mathcal{X}_F, \psi_{L/F}, \varpi_F^{m+n})$$

is equal to

$$\psi_F \left(\frac{\ell\beta}{\varpi_F^{m+n}}\right) \mathcal{X}_F^{-1}(\beta^\ell).$$

To complete the proof of the lemma we have to show that

$$\Delta_3(\mathcal{X}_F, \psi_F, \varpi_F^{m+n}) \prod\nolimits_{\mu\in T} \Delta_3(\mu\mathcal{X}_F, \psi_{L/F}, \varpi_F^{m+n}) \tag{13.4}$$

is equal to

$$\Delta_3(\mathcal{X}_{E/F}, \psi_{E/F}, \varpi_F^{m+n})$$

when one, and hence both, of m and m' is odd.

As remarked in Lemma 9.4

$$\Delta_3(\mu\mathcal{X}_{L/F},\psi_{L/F},\varpi_F^{m+n})=\Delta_3(\mathcal{X}_{L/F},\psi_{L/F},\varpi_F^{m+n}).$$

According to Lemma 9.6 the right side is equal to

$$\varepsilon\Delta_3(\mathcal{X}_F,\psi_F,\varpi_F^{m+n})^{[L:F]}$$

where ε is 1 if $f=[L:F]$ is odd and -1 if it is even. Thus (13.4) is equal to

$$\varepsilon^{\frac{\ell-1}{f}}\,\{\Delta_3(\mathcal{X}_F,\psi_F,\varpi_F^{m+n})\}.$$

As before

$$\phi=O_F/\mathfrak{P}_F=O_E/\mathfrak{P}_E.$$

Let φ_ϕ be the function on ϕ defined by

$$\varphi_\phi(x)=\psi_F\,\left(\frac{\beta x}{\varpi_F^{d+1+n}}\right)\,\mathcal{X}_F^{-1}(1+\varpi_F^d x)$$

if $m=2d+1$. Then $m'=2\ell d+1$ so that $d'=\ell d$. Let φ'_ϕ be the function on ϕ defined by

$$\varphi'_\phi(x)=\psi_{E/F}\,\left(\frac{\beta x}{\varpi_F^{d+1+n}}\right)\,\mathcal{X}_{E/F}^{-1}(1+\varpi_F^d x).$$

Because of Lemma 9.3, to complete the proof of the lemma we have only to show that

$$\varepsilon^{\frac{\ell-1}{f}}\,A[\sigma(\varphi_\phi)^\ell]=A[\sigma(\varphi'_\phi)].$$

Since $d'\geq m$ and

$$\frac{3d'+\ell-1}{\ell}\geq m$$

we have

$$N_{K/L}(1+\varpi_F^d x)\equiv 1+\varpi_F^d\,S_{K/L}x+\varpi_F^{2d}E_{K/L}^2(x)\pmod{\mathfrak{P}_L^m}$$

if $E_{K/L}^2(x)$ is the second elementary symmetric function of x and its conjugates over L. Thus

$$N_{E/F}(1+\varpi_F^d x)\equiv 1+\varpi_F^d S_{E/F}x+\varpi_F^{2d}E_{E/F}^2(x)\pmod{\mathfrak{P}_F^m}.$$

This in turn is congruent to

$$(1+\varpi_F^d\,S_{E/F}x)\,(1+\varpi_F^{2d}E_{K/F}^2(x)).$$

Thus

$$\varphi'_\phi(x)=\varphi_\phi(\ell x)\psi_\phi(-E_{\lambda/\phi}^2(x))$$

if

$$\psi_\phi(x)=\varphi_F\,\left(\frac{\beta x}{\varpi_F^{1+n}}\right)$$

or

$$\varphi'_\phi(x) = \varphi_\phi(\ell x)\psi_\phi\ \left(\frac{-\ell(\ell-1)}{2}\,x^2\right) = \{\varphi_\phi(x)\}^\ell.$$

Suppose first that p is odd and let

$$\varphi_\phi(x) = \psi_\phi\ \left(\frac{x^2-2\alpha x}{2}\right)$$

so that

$$\varphi'_\phi(x) = \psi_\phi\ \left(\frac{\ell x^2-2\ell\alpha x}{2}\right) = \psi_\phi\ \left(\frac{\ell(x-\alpha)^2}{2}\right)\ \psi_\phi\ \left(\frac{-\ell\alpha^2}{2}\right).$$

Referring to the observations in paragraph 9 we see that we must show that

$$\varepsilon^{\frac{\ell-1}{f}}\,\nu_\phi(-1)^{\frac{\ell-1}{2}}\psi_\phi\ \left(\frac{-\ell\alpha^2}{2}\right) = \nu_\phi(\ell)\psi_\phi\ \left(\frac{-\ell\alpha^2}{2}\right)$$

or

$$\varepsilon^{\frac{\ell-1}{f}} = \nu_\phi(-1)^{\frac{\ell-1}{2}}\nu_\phi(\ell)$$

if ν_ϕ is the quadratic character of ϕ^*. Let q be the number of elements in ϕ. If q is an even power of p the right side is 1 and if q is an odd power of p the right side is, by the law of quadratic reciprocity, $\omega(p)$ if ω is the quadratic character of the field with ℓ elements. Thus in all cases the right side is $\omega(q)$. If f is odd then q^f is a quadratic residue of ℓ if and only if q is. Since

$$q^f - 1 \equiv 0 \pmod{\ell}.$$

q is a quadratic residue and both sides of the equation are 1. If f is odd the left side is $(-1)^{\frac{\ell-1}{f}}$. Since f is the order of q modulo ℓ this is $\omega(q)$.

Now suppose that $p=2$. If

$$\psi_\phi(-x^2) = \psi_\phi(\alpha x)$$

then, by the remarks in the proof of Lemma 9.7, we have to show that

$$\varepsilon^{\frac{\ell-1}{f}}\varphi_\phi(\alpha)^{\frac{\ell-1}{2}} = 1$$

if $\ell \equiv 1 (\mathrm{mod}\, 4)$ and that

$$\varepsilon^{\frac{\ell-1}{f}}\varphi_\phi(\alpha)^{\frac{\ell+1}{2}} = 1$$

if $\ell \equiv 3\,(\mathrm{mod}\, 4)$. We also saw in paragraph 9 that

$$\{\varphi_\phi(\alpha)\}^2 = \psi_\phi(\alpha^2)$$

was +1 or -1 according as q is or is not an even power of p. By the second supplement to the law of quadratic reciprocity

$$\varphi_\phi(\alpha)^{\frac{\ell-1}{2}} = \omega(q)$$

if $\ell \equiv 1 \pmod 4$ and

$$\varphi_\phi(\alpha)^{\frac{\ell+1}{2}} = \omega(q)$$

if $\ell \equiv 3 \pmod 4$. We have just seen that

$$\varepsilon^{\frac{\ell-1}{f}} = \omega(q).$$

The lemma is proved.

Chapter Fourteen.

The Fourth Main Lemma.

In the previous paragraph we said that we would eventually have to show that

$$\Delta(\chi_{E/F},\psi_{E/F})\prod\nolimits_{\mu\in T}\Delta(\mu',\psi_{F_\mu/F}) \tag{14.1}$$

is equal to

$$\Delta(\chi_F,\psi_F)\prod\nolimits_{\mu\in T}\Delta(\mu'\chi_{F_\mu/F},\psi_{F_\mu/F}). \tag{14.2}$$

However we verified that the two expressions are equal only when K/F is tamely ramified. In this paragraph we shall show that they are equal if Theorem 2.1 is valid for all pairs K'/F' in $\mathcal{P}(K/F)$ for which $[K':F']<[K:F]$.

Lemma 14.1

Suppose K/F is wildly ramified and Theorem 2.1 is valid for all pairs K'/F' in $\mathcal{P}(K/F)$ for which $[K':F']<[K:F]$. If χ_F is any quasi-character of C_F the expressions (14.1) and (14.2) are equal.

If a and b are two non-zero complex numbers and m is a positive integer we again write $a\sim_m b$ if, for some non-negative integer r, $\frac{a}{b}$ is an m^rth root of unity. Define the non-zero complex number ρ by demanding that

$$\Delta(\chi_{E/F},\psi_{E/F})\prod\nolimits_{\mu\in T}\Delta(\mu',\psi_{F_\mu/F})$$

be equal to

$$\rho\Delta(\chi_F,\psi_F)\prod\nolimits_{\mu\in T}\Delta(\mu'\chi_{F_\mu/F},\psi_{F_\mu/F}).$$

We have to show that $\rho=1$. Lemma 14.1 will be an easy consequence of the following four lemmas.

Lemma 14.2

If $m(\chi_F)$ is 0 or 1 then $\rho=1$ and in all cases $p\sim_{2p}1$.

Lemma 14.3

If $[G:G_1]$ is a power of 2 then $\rho\sim_p 1$.

Lemma 14.4

If the induction assumption is valid, if $F \subseteq F' \subseteq L$, if F'/F is normal, and if $[F' : F] = \ell$ is a prime then $p \sim_\ell 1$.

Lemma 14.5

Suppose $H = H_1 H_2$ where H_2 is a cyclic normal subgroup of H, $[H_2 : 1]$ is a power of a prime ℓ, and $[H_1 : 1]$ is prime to ℓ. If the induction assumption is valid $\rho \sim_\ell 1$.

Grant these four lemmas for a moment and observe that if m and n are relatively prime then $\rho \sim_m 1$ and $\rho \sim_n 1$ imply that $\rho = 1$. If ℓ is a prime which divides $[G : G_0]$ there is a field F' containing F and contained in L so that F'/F is normal and $[F' : F] = \ell$. Thus Lemma 14.1 follows from Lemma 14.4 unless $[G : G_0]$ is a prime power. Lemma 14.1 follows from Lemmas 14.2 and 14.4 unless $[G : G_0]$ is a power of 2 or p. Suppose $[G : G_0]$ is a power of 2 or p. Then $\rho \sim_{[G:G_0]} 1$ except perhaps when $[G : G_0] = 1$. If ℓ is a prime which does not divide $[G : G_0]$ but does divide $[G_0 : G_1]$ let H_2 be the ℓ-Sylow subgroup of G_0/G_1. H_2 is a normal subgroup of G/G_1 which we may identify with H and H/H_2 has order prime to H_2. Thus, by a well-known theorem of Schur [7], $H = H_1 H_2$ where $H_1 \cap H_2 = \{1\}$ and H_1 has order prime to H_2. It follows from Lemma 14.5 that $\rho = 1$ unless $[G : G_0] = 1$ or $[G : G_1]$ is a power of 2 or p. If $[G : G_0] = 1$ and ℓ is a prime dividing $[G_0 : G_1]$ there is a field F' with $F \subseteq F' \subseteq L$ such that F'/F is normal and $[F' : F] = \ell$. Thus if $[G : G_0] = 1$ it follows from Lemma 14.4 that $\rho = 1$ unless $[G : G_1]$ is a power of 2. However if $[G : G_1]$ is a power of 2 there certainly is an F' in L with $[F' : F] = 2$. It follows from Lemmas 14.3 and 14.4 that $\rho = 1$ in this case unless $p = 2$. If $[G : G_1]$ is a power of p then $G_0 = G_1$ and G/G_1 is abelian. By assumption the abelian p-group G/G_1 acts on the p-group $C = G_1$ faithfully and irreducibly. This is impossible.

We prove Lemma 14.2 first. Let $t \geq 1$ be such that $C = G_t$ while $G_{t+1} = \{1\}$. Let θ_t be the homomorphism of G_t into $\mathfrak{P}_K^t/\mathfrak{P}_K^{t+1}$ and θ_0 the homomorphism of G_0/G_1 into U_K^0/U_K^1 introduced in Serre's book. If $\sigma \in G_0$ and $\gamma \in G_t$ then

$$\theta_t(\sigma\gamma\sigma^{-1}\gamma^{-1}) = (\theta_0^t(\sigma) - 1)\theta_t(\gamma).$$

If σ is not in G_1 then $\theta_0^t(\sigma)$ is not 1 and $\gamma \to \sigma\gamma\sigma^{-1}\gamma^{-1}$ is a one-to-one map of C onto itself. Thus, if $\sigma \in G_0$,

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

implies $\mu = 1$ or $\sigma \in G_1$. Consequently if $\mu \neq 1$, $G_\mu \cap G_0 = G_1$ and L/F_μ is unramified. Since $\mu = \mu'_{L/F_\mu}$,

$$m(\mu') = m(\mu) = t + 1.$$

Observe also that t must be relatively prime to $[G_0 : G_1]$. In particular if t is even $[G_0 : G_1]$ is odd.

The relations

$$\begin{aligned}\delta_{K/L} &= ([G_t : 1] - 1)\,(t + 1)\\ \delta_{L/F} &= [G_0 : G_1] - 1\\ \delta_{K/E} &= [G_0 : G_1] - 1\end{aligned}$$

and

$$\delta_{K/F} = \delta_{K/L} + [G_1 : 1]\,\delta_{L/F} = \delta_{K/E} + [G_0 : G_1]\delta_{E/F}$$

obtained from Proposition 4 of Chapter IV of Serre's book, imply that

$$\delta_{E/F} = ([G_1;1]-1)\left(\frac{t}{[G_0:G_1]}+1\right).$$

If $n = n(\psi_F)$ then

$$n(\psi_{F_\mu/F}) = [G_0:G_1]n + [G_0:G_1]-1$$

and

$$n' = n(\psi_{E/F}) = [G_1:1]n + ([G_1:1]-1)\left(\frac{t}{[G_0:G_1]}+1\right).$$

Choose a generator ϖ_K of $\mathfrak{P}_K$ and a generator ϖ_E of $\mathfrak{P}_E$. Then set $\varpi_L = N_{K/L}\varpi_K$ and $\varpi_F = N_{E/F}\varpi_E$. There is a unit δ in K such that

$$\frac{\varpi_F^{1+n}}{\varpi_E^{1+n'}} = \delta\ \frac{\varpi_K^t}{\varpi_L^t}.$$

Taking the norm from K to L of both sides we see that if $q=[G_1:1]$ and $k=[G_0:G_1]$ then

$$\frac{\varpi_L^{t(q-1)}}{\varpi_F^{t\frac{(q-1)}{k}}} = N_{K/L}\delta.$$

Let $m = m(\chi_F)$. If $m-1$ is equal to $\frac{t}{[G_0:G_1]}$ then $[G_0:G_1]$ divides t and $[G_0:G_1]$ is 1. Suppose that

$$m < \frac{t}{[G_0:G_1]}+1.$$

Then

$$m(\chi_{F_\mu/F}) < \psi_{F_\mu/F}\left(\frac{t}{[G_0:G_1]}\right)+1.$$

However $\psi_{F_\mu/F} = \varphi_{L/F_\mu}\circ\psi_{L/F} = \psi_{L/F}$ so that

$$\psi_{F_\mu/F}(u) = [G_0:G_1]u$$

if $u \geq 0$. Thus $m(\chi_{F_\mu/F}) < t+1$ and $m(\mu'\chi_{F_\mu/F}) = t+1$. Moreover, by Lemmas 13.1 and 6.4, $m' = m(\chi_{E/F}) = m$. Choose a generator ϖ_{F_μ} of $\mathfrak{P}_{F_\mu}$. Then

$$N_{F_\mu/F}(\varpi_{F_\mu}^t) = \gamma_\mu\,\varpi_F^{t\frac{[F_\mu:F]}{k}}$$

where γ_μ is a unit. The order of $\varpi_F^{1+n}\varpi_{F_\mu}^t$ in F_μ is $1+t+n(\psi_{F_\mu/F})$. Observing that

$$\sum\nolimits_\mu [F_\mu:F] = q-1$$

we see that

$$\Delta_1(\chi_{E/F},\psi_{E/F'}\varpi_E^{m'+n'})\prod\nolimits_{\mu\in T}\Delta_1(\mu',\psi_{F_\mu/F},\varpi_F^{1+n}\varpi_{F_\mu}^t)$$

is equal to

$$p\left\{\prod_\mu \chi_F(\gamma_\mu)\right\}\,\{\Delta_1(\chi_F,\psi_F,\varpi_F^{m+n}\}\,\left\{\prod_\mu \Delta_1(\mu'\chi_{F_\mu/F},\psi_{F_\mu/F},\varpi_F^{1+n}\varpi_{F_\mu}^t)\right\}.$$

It is now clear that $\rho=1$ if $m=0$.

If

$$m \geq \frac{t}{[G_0:G_1]}+1$$

so that in particular $m\geq 2$, then

$$m'=m(\chi_{E/F})=[G_1:1]m-([G_1:1]-1)\left(\frac{t}{[G_0:G_1]}+1\right)$$

is also greater than or equal to 2 and

$$m'+n'=[G_1:1]\,(m+n).$$

Since $m'\geq 2$ and K/E is tamely ramified

$$m(\chi_{K/F})=\psi_{K/E}(m(\chi_{E/F})-1)+1=\psi_{K/F}(m-1)+1.$$

Since

$$m(\chi_{F_\mu/F})\leq\psi_{F_\mu/F}(m-1)+1$$

and

$$\psi_{F_\mu/F}(m-1)+1\geq\psi_{F_\mu/F}\left(\frac{t}{k}\right)+1=t+1$$

we have

$$m(\mu'\chi_{F_\mu/F})\leq\psi_{F_\mu}(m-1)+1.$$

However

$$\chi_{K/F}=(\mu'\chi_{F_\mu/F})_{K/F_\mu}$$

so that

$$\psi_{K/F_\mu}(\psi_{F_\mu/F}(m-1))+1=\psi_{K/F}(m-1)+1=m(\chi_{K/F})$$

is at most

$$\psi_{K/F}(m(\mu'\chi_{F_\mu/F})-1)+1.$$

Thus

$$m(\mu'\chi_{F_\mu/F})=\psi_{F_\mu/F}(m-1)+1.$$

Consequently

$$m(\mu'\chi_{F_\mu/F})+n(\psi_{F_\mu/F})=[G_0:G_1]\,(m+n).$$

Since the range of each μ' lies in the group of qth roots of unity

$$\Delta_1(\chi_{E/F},\psi_{E/F},\varpi_F^{m+n})\,\prod_\mu\Delta_1(\mu',\psi_{F_\mu/F},\varpi_F^{n+1}\varpi_{F_\mu}^t)$$

is equal to

$$\sigma\Delta_1(\chi_F,\psi_F,\varpi_F^{m+n})\ \prod_\mu \Delta_1(\mu'\chi_{F_\mu/F},\psi_{F_\mu/F},\varpi_F^{m+n})$$

with $\sigma\sim_p\rho$.

The next step in the proof of the lemma is to establish a simple identity. As usual let r be the integral part of $\frac{t+1}{2}$ and let $r+s=t+1$. Choose $\beta(\mu')$ so that

$$\psi_{F_\mu/F}\left(\frac{\beta(\mu')x}{\varpi_F^{1+n}\varpi_{F_\mu}^t}\right)=\mu'(1+x)$$

for x in $\mathfrak{P}_{F_\mu}^s$. There is a unit α_μ in L such that $\alpha_\mu\varpi_{F_\mu}^t=\varpi_L^t$. Then

$$\psi_{L/F}\left(\frac{\alpha_\mu\beta(\mu')x}{\varpi_F^{1+n}\varpi_L^t}\right)=\mu(1+x)$$

for x in $\mathfrak{P}_L^s$. We take $\beta(\mu)=\alpha_\mu\beta(\mu')$. If $\sigma\in G$ a possible choice for $\beta(\mu^\sigma)$ is

$$\beta(\mu)^\sigma\frac{\varpi_L^t}{\varpi_L^{\sigma\,t}}.$$

Let $\phi=O_F/\mathfrak{P}_F=O_E/\mathfrak{P}_E$ and let ψ_ϕ be the additive character of ϕ defined by

$$\psi_\phi(x)=\psi_F\left(\frac{x}{\varpi_F^{1+n}}\right).$$

There is a unique α in ϕ such that

$$\psi_\phi(\alpha x)=\psi_\phi(x^q).$$

Finally let

$$\omega_1=S_{E/F}\left(\frac{\varpi_F^{1+n}}{\varpi_E^{1+n'}}\right).$$

I want to show that

$$\prod_\mu\gamma_\mu=\frac{\omega_1^q}{\alpha^q}\ \prod_\mu N_{F_\mu/F}\beta(\mu') \tag{14.3}$$

in ϕ.

Let $\lambda=O_L/\mathcal{P}_L=O_K/\mathcal{P}_K$. If

$$\omega=S_{K/L}\left(\frac{\varpi_K^t}{\varpi_L^t}\right)$$

then $\omega_1=\delta\omega$ in λ. We need the following lemma.

Lemma 14.6

Suppose K'/F' is an abelian extension and $G'=\mathfrak{G}(K'/F')$. Suppose there is a $t\geq 1$ such that $G'=G'_t$ and $G'_{t+1}=\{1\}$. Let $\varpi_{K'}$ be a generator of $\mathfrak{P}'_K$, let $\varpi_{F'}=N_{K'/F'}(\varpi_{K'})$, and let

$$\omega=S_{K'/F'}\left(\frac{\varpi_{K'}^t}{\varpi_{F'}^t}\right).$$

Also let $q = [K' : F']$*. There are numbers* $a, \ldots, f$ *in* $O_{F'}$ *such that for all* x *in* $O_{F'}$

$$N_{K'/F'}(1 + x\varpi_{K'}^t)$$

is congruent to

$$1 + (x^q + ax^{\frac{q}{p}} + \ldots + fx^p + \omega x)\varpi_{F'}^t$$

modulo $\mathfrak{P}_{F'}^{t+1}$.

Suppose $F' \subseteq L' \subseteq K'$ and the lemma is true for K'/L' and L'/F'. The lemma for K'/F' follows from the relations

$$[K' : F'] = [K' : L']\,[L' : F']$$

and

$$N_{K'/F'}(1 + x\varpi_{K'}^t) = N_{L'/F'}(N_{K'/L'}(1 + x\varpi_{K'}^t))$$

and

$$S_{K'/F'}\left(\frac{\varpi_{K'}^t}{\varpi_{F'}^t}\right) \equiv S_{L'/F'}\left(\frac{\varpi_{L'}^t}{\varpi_{F'}^t}\right)\, S_{K'/L'}\left(\frac{\varpi_{K'}^t}{\varpi_{L'}^t}\right).$$

The lemma for extensions of prime order is proved in Serre's book.

Suppose then

$$N_{K/L}(1 + x\varpi_K^t) \equiv 1 + (x^q + \ldots + \varpi x)\varpi_L^t \pmod{\mathfrak{P}_L^{t+1}}$$

for x in O_L. Since

$$\psi_{\lambda/\phi}(\alpha x) = \psi_\phi(\alpha S_{\lambda/\phi}(x)) = \psi_\phi((S_{\lambda/\phi}(x))^q)$$

which in turn equals

$$\psi_\phi(S_{\lambda/\phi}x^q) = \psi_{\lambda/\phi}(x^q)$$

we conclude that

$$\psi_{\lambda/\phi}(y(x^q + \ldots + \omega x)) = \psi_{\lambda/\phi}((\alpha y^{\frac{1}{q}} + \ldots + \omega y)x).$$

Also

$$\left(\alpha y^{\frac{1}{q}} + \ldots + \omega y\right)^q = \alpha^q y + \ldots + \omega^q y^q$$

is a polynomial $Q(y)$ in y.

For each ν in $S(K/L)$, we choose $\beta_1(\nu)$ so that

$$\psi_{L/F}\left(\frac{\beta_1(\nu)x}{\varpi_F^{1+n}\varpi_L^t}\right) = \nu(1 + x)$$

for x in $\mathcal{P}_L^s$. Since $k^p = k$ in λ

$$\psi_{\lambda/\phi}(k\beta_1(\nu)(x^q + \ldots + \omega x) = \psi_{\lambda/\phi}(\beta_1(\nu)\,[(kx)^q + \ldots + \omega kx])$$

if x is in O_F. The left side is also equal to

$$\psi_{L/F}\left(\frac{\beta_1(\nu)\,P_{K/L}(x\varpi_K^t)}{\varpi_F^{1+n}\,\varpi_L^t}\right) = 1.$$

Thus $Q(k\beta_1(\nu))=0$. Since $\beta_1(\nu_1)=\beta_2(\nu_2) \pmod{\mathfrak{P}_L}$ implies $\nu_1=\nu_2$ we have found all the roots of $Q(y)=0$. Thus

$$\frac{\alpha^q}{\omega^q} \equiv \prod_{\nu\neq 1} k\beta_1(\nu) \equiv \prod_{\nu\neq 1} \beta_1(\nu) \pmod{\mathfrak{P}_L}.$$

Let M_μ be a set of representatives for the cosets of G_μ in G. Then

$$\prod_{\mu\in T} N_{F_\mu/F}\beta(\mu') = \prod_{\mu\in T} \prod_{\sigma\in M_\mu} \beta(\mu')^\sigma$$

is congruent to

$$\left\{\prod_{\nu\neq 1} \beta_1(\nu)\right\} \left\{\prod_{\mu\in T} \prod_{\sigma\in M_\mu} \alpha_\mu^\sigma \, \frac{\varpi_L^t}{\varpi_L^{\sigma\, t}}\right\}^{-1}$$

modulo $\mathfrak{P}_L$. To verify the identity (14.3) we have to show that

$$\left\{\prod_{\mu} \prod_{\sigma\in M_\mu} \alpha_\mu^\sigma \, \frac{\varpi_L^t}{\varpi_L^{\sigma\, t}}\right\} \left\{\prod_{\mu} \gamma_\mu\right\} \equiv \delta^q \pmod{\mathfrak{P}_K}.$$

Since

$$\gamma_\mu = \left\{\prod_{\sigma\in M_\mu} \frac{\varpi_L^{\sigma\, t}}{\alpha_\mu^\sigma}\right\} \varpi_F^{-t\frac{[F_\mu:F]}{k}}$$

the congruence reduces to

$$\frac{\varpi_L^{t(q-1)}}{\varpi_F^{t\frac{(q-1)}{k}}} \equiv \delta^q \pmod{\mathfrak{P}_K}$$

which is valid because the left side is $N_{K/L}\delta$ and

$$N_{K/L}\delta \equiv \delta^q \pmod{\mathfrak{P}_K}.$$

If $m=1$ then $m(\chi_{F_\mu/F})\leq 1$ and we can take $\beta(\mu'\chi_{F_\mu/F})=\beta(\mu')$. Then

$$\Delta_2(\mu', \psi_{F_\mu/F}, \varpi_F^{1+n}\varpi_{F_\mu}^t)$$

is equal to

$$\chi_F(N_{F_\mu/F}(\beta(\mu')))\, \Delta_2(\mu'\chi_{F_\mu/F}, \psi_{F_\mu/F}, \varpi_F^{1+n}\varpi_{F_\mu}^t).$$

Lemma 9.4 implies that

$$\Delta_3(\mu', \psi_{F_\mu/F}, \varpi_F^{1+n}\varpi_{F_\mu}^t) = \Delta_3(\mu'\chi_{F_\mu/F}, \psi_{F_\mu/F}, \varpi_F^{1+n}\varpi_{F_\mu}^t).$$

If x belongs to O_E then

$$\psi_{E/F}\left(\frac{x}{\varpi_E^{1+n'}}\right) = \psi_\phi(\omega_1 x).$$

If χ_ϕ is the character of ϕ^* determined by χ_F then

$$\Delta_1(\chi_F, \psi_F, \varpi_F^{1+n}) = A[-\tau(\chi_\phi, \psi_\phi)]$$

and

$$\Delta_1(\chi_{E/F}, \psi_{E/F}, \varpi_E^{1+n'}) = \chi_\phi(\omega_1^q)\ A[-\tau(\chi_\phi^q, \psi_\phi)].$$

The right side of this expression is equal to

$$\chi_\phi(\omega_1^q \alpha^{-q})\ A[-\tau(\chi_\phi, \psi_\phi)].$$

The identity (14.3) now shows that $\rho = 1$ when $m = 1$.

Suppose that

$$1 < m < \frac{t}{[G_0 : G_1]} + 1.$$

Let β be a given choice of $\beta(\chi_F)$. Then

$$\beta(\chi_{E/F}) \equiv P^*_{E/F}(\beta, \varpi_E^{m'+n'}, \varpi_F^{m+n}) \pmod{\mathfrak{P}_E^{d'}}$$

if $m' = 2d' + \varepsilon'$. On the other hand

$$\psi_{L/F}(m-1) + 1 + n(\psi_{L/F}) = [G_0 : G_1](m-1) + 1 + [G : G_0]n + [G_0 : G_1] - 1$$

which equals $[G_0 : G_1](m+n)$ and Lemmas 8.3, 8.4 and 8.7 imply that

$$P^*_{L/F}(\beta, \varpi_F^{m+n}, \varpi_F^{m+n}) \equiv \beta \pmod{\mathfrak{P}_L^{d_1}}$$

if

$$\psi_{L/F}(m-1) + 1 = 2d_1 + \varepsilon_1.$$

If

$$\psi_{K/F}(m-1) + 1 = 2d_1' + \varepsilon_1'$$

then

$$P^*_{K/E}(\beta(\chi_{E/F}, \varpi_E^{m'+n'}, \varpi_E^{m'+n'}) \equiv \beta(\chi_{E/F}) \pmod{\mathfrak{P}_K^{d_1'}}.$$

Thus

$$\beta(\chi_{E/F}) \equiv P^*_{K/F}(\beta, \varpi_E^{m'+n'}, \varpi_F^{m+n}) \pmod{\mathfrak{P}_K^{d_1'}}.$$

Let

$$v = t + 1 - (\psi_{L/F}(m-1) + 1) = t - [G_0 : G_1]\,(m-1).$$

If

$$\gamma = \frac{\varpi_L^{t-v}}{\varpi_F^{m-1}}$$

and

$$\gamma' = \frac{\varpi_E^{m'+n'}\varpi_K^v}{\varpi_F^{1+n}\varpi_L^t}$$

then

$$P^*_{K/F}(\beta, \varpi_E^{m'+n'}, \varpi_F^{m+n}) \equiv P^*_{K/L}(\beta, \varpi_E^{m'+n'}, \varpi_F^{m+n}) \pmod{\mathfrak{P}_K^{d_1'}}$$

is congruent to

$$\gamma' P^*_{K/L}(\gamma\beta, \varpi_F^{1+n}\varpi_L^t\varpi_K^{-v}, \varpi_F^{1+n}\varpi_L^{t-v})$$

modulo $\mathfrak{P}_K^{d_1'}$.

It is clear that

$$\Delta_2(\chi_{E/F},\psi_{E/F},\varpi_E^{m'+n'}) \sim_p \chi_F^{-1}(N_{E/F}(\beta(\chi_{E/F})))$$

and that

$$\Delta_2(\mu',\psi_{F_\mu/F},\varpi_F^{n+1}\varpi_{F_\mu}^t) \sim_p 1.$$

If we choose

$$\beta(\mu'\chi_{F_\mu/F}) = \beta(\mu') + \beta\,\frac{\varpi_{F_\mu}^t}{\varpi_F^{m-1}}$$

then

$$\Delta_2(\mu'\chi_{F_\mu/F},\psi_{F_\mu/F},\varpi_F^{n+1}\varpi_{F_\mu}^t) \sim_p \chi_F^{-1}\left(N_{F_\mu/F}\left(\beta(\mu') + \beta\ \frac{\varpi_{F_\mu}^t}{\varpi_F^{m-1}}\right)\right).$$

Moreover

$$\Delta_2(\chi_F,\psi_F,\varpi_F^{m+n}) \sim_p \chi_F^{-1}(\beta).$$

Let

$$\Delta_2(\chi_{E/F},\psi_{E/F},\varpi_E^{m'+n'})\ \prod\nolimits_\mu \Delta_2(\mu',\psi_{F_\mu/F},\varpi_F^{n+1}\varpi_{F_\mu}^t)$$

equal

$$\tau\Delta_2(\chi_F,\psi_F,\varpi_F^{m+n})\left\{\prod\nolimits_\mu \Delta_2(\mu'\chi_{F_\mu/F},\psi_{F_\mu/F},\varpi_F^{n+1}\varpi_{F_\mu}^t)\right\}\left\{\prod\nolimits_\mu \chi_F(\gamma_\mu)\right\}.$$

Since

$$\chi_F(u) \sim_p 1$$

if $u \in U_F^1$, all we need do to show that $\tau \sim_p 1$ is prove that

$$\beta\prod\nolimits_\mu N_{F_\mu/F}\left(\beta(\mu') + \beta\frac{\varpi_{F_\mu}^t}{\varpi_F^{m-1}}\right)$$

is congruent to

$$N_{E/F}(\beta(\chi_{E/F}))\ \prod\nolimits_\mu \gamma_\mu$$

modulo $\mathfrak{P}_F$.

As before we choose $\beta(\mu) = \alpha_\mu(\beta(\mu')$. If $\nu = \mu^\sigma$ a possible choice for $\beta(\nu)$ is

$$\alpha_\mu^\sigma\beta(\mu')^\sigma\ \frac{\varpi_L^t}{\varpi_L^{\sigma\,t}}.$$

We can also choose

$$\beta(\mu\chi_{L/F}) = \alpha_\mu\beta(\mu') + \beta\ \frac{\varpi_L^t}{\varpi_F^{m-1}} = \alpha_\mu\left(\beta(\mu') + \beta\ \frac{\varpi_{F_\mu}^t}{\varpi_F^{m-1}}\right).$$

Then a possible choice for $B(\mu^\sigma\chi_{L/F})$ is

$$\alpha_\mu^\sigma\left\{\beta(\mu') + \beta\ \frac{\varpi_{F_\mu}^t}{\varpi_F^{m-1}}\right\}^\sigma\ \frac{\varpi_L^t}{\varpi_L^{\sigma\,t}} = \alpha_\mu^\sigma(\beta(\mu')^\sigma\ \frac{\varpi_L^t}{\varpi_L^{\sigma\,t}} + \beta\ \frac{\varpi_L^t}{\varpi_F^{m-1}}.$$

We apply Lemma 8.10 with F replace by L,

$$\delta=\varpi_F^{1+n}\varpi_L^t$$

and $\varepsilon_1=\varpi_K^v$. It implies that

$$N_{K/L}\ \left(\frac{\beta(\chi_{E/F})}{\gamma'}\right)$$

is congruent to

$$\gamma_\beta\prod\nolimits_{\mu\in T}\prod\nolimits_{\sigma\in M_\mu}\ \left\{\alpha_\mu^\sigma\left(\beta(\mu')+\beta\ \frac{\varpi_{F_\mu}^t}{\varpi_F^{m-1}}\right)^\sigma\ \frac{\varpi_L^t}{\varpi_L^{\sigma\,t}}\right\}$$

modulo $\mathfrak{P}_L$. The last expression is equal to

$$\gamma_\beta\left\{\prod\nolimits_{\mu\in T}N_{F_\mu/F}\left(\beta(\mu')+\beta\ \frac{\varpi_{F_\mu}^t}{\varpi_F^t}\right)\right\}\ \left\{\prod\nolimits_{\mu\in T}\prod\nolimits_{\sigma\in M_\mu}\alpha_\mu^\sigma\ \frac{\varpi_L^t}{\varpi_L^{\sigma\,t}}\right\}$$

and we have to show that

$$\gamma N_{K/L}(\gamma')\ \left\{\prod\nolimits_\mu\gamma_\mu\right\}\ \left\{\prod\nolimits_{\mu\in T}\prod\nolimits_{\sigma\in M_\mu}\alpha_\mu^\sigma\ \frac{\varpi_L^t}{\varpi_L^{\sigma\,t}}\right\}$$

is congruent to 1 modulo $\mathfrak{P}_L$. First of all

$$N_{K/L}(\gamma')=\varpi_F^{m'+n'-q(1+n)}\varpi_L^{-qt+v}=\gamma^{-1}\ \frac{\varpi_F^{\frac{(q-1)t}{k}}}{\varpi_L^{(q-1)t}}.$$

Since

$$\gamma_\mu=\left\{\prod\nolimits_{\sigma\in M_\mu}\ \frac{\alpha_\mu^\sigma}{\varpi_L^{\sigma\,t}}\right\}^{-1}\varpi_F^{-t\frac{[F_\mu:F]}{k}}$$

the required relation follows.

Define η by setting

$$\eta\Delta_3\left(\chi_{E/F},\psi_{E/F},\varpi_E^{m'+n'}\right)\prod\nolimits_{\mu\in T}\Delta_3\left(\mu',\psi_{F_\mu/F},\varpi_F^{1+n}\varpi_{F_\mu}^t\right)$$

equal to

$$\Delta_3(\chi_F,\psi_F,\varpi_F^{m+n})\ \prod\nolimits_{\mu\in T}\Delta_3\left(\mu'\chi_{F_\mu/F},\psi_{F_\mu/F},\varpi_F^{1+n}\varpi_{F_\mu}^t\right).$$

We now know that $\eta\sim_p\rho$. We shall show that $\eta\sim_p 1$. This will prove not only the assertion of Lemma 14.2 but also that of Lemma 14.3, provided of course that

$$m-1<\frac{t}{[G_0:G_1]}.$$

Lemmas 9.2 and 9.3 imply directly that $\eta\sim_p 1$ if p is 2.

Suppose p is odd. Lemma 9.4 implies that

$$\Delta_3(\mu', \psi_{F_\mu/F}, \varpi_F^{1+n}\varpi_{F_\mu}^t) \sim_p \Delta_3(\mu'\chi_{F_\mu/F}, \psi_{F_\mu/F}, \varpi_F^{1+n}\varpi_{F_\mu}^t).$$

Since $m' = m$ all we need do is show that

$$\Delta_3(\chi_{E/F}, \psi_{E/F}, \varpi_E^{m'+n'}) \sim_p \Delta_3(\chi_F, \psi_F, \varpi_F^{m+n})$$

when m is odd. Let $\phi = O_F/\mathfrak{P}_F = O_E/\mathfrak{P}_E$. Let $\beta' = \beta(\chi_{E/F})$ and let $\beta = \beta(\chi_F)$. If ψ'_ϕ is the character of ϕ defined by

$$\psi'_\phi(x) = \psi_F\left(\frac{\beta\, x}{\varpi_F^{n+1}}\right)$$

and ψ''_ϕ is the character of ϕ defined by

$$\psi''_\phi(x) = \psi_{E/F}\left(\frac{\beta' x}{\varpi_E^{n'+1}}\right)$$

and if $\psi''_\phi(x) = \psi'_\phi(\delta x)$ then, by Lemmas 9.2 and 9.3, all we have to do is show that δ is a square in ϕ. If

$$\omega_1 = S_{E/F}\left(\frac{\varpi_F^{n+1}}{\varpi_E^{n'+1}}\right)$$

then $\delta = \omega_1 \, \frac{\beta'}{\beta}$ in ϕ. To show that δ is a square we show that δ^q is a square.

$$\delta^q \equiv N_{E/F}\alpha \equiv \beta^{1-q}\, \frac{N_{E/F}(\beta')}{\beta}\omega_1^q.$$

We saw that

$$\frac{N_{E/F}(\beta')}{\beta} = \left\{\prod\nolimits_\mu \gamma_\mu\right\}^{-1} \left\{\prod\nolimits_\mu N_{F_\mu/F}\left(\beta(\mu') + \beta\, \frac{\varpi_{F_\mu}^t}{\varpi_F^{m-1}}\right)\right\}$$

in ϕ. But

$$\beta\,\frac{\varpi_{F_\mu}^t}{\varpi_F^{m-1}} \equiv 0 \pmod{\mathfrak{P}_L}$$

because $t > [G_0 : G_1](m-1)$. We also saw that

$$\left\{\prod\nolimits_\mu \gamma_\mu\right\}^{-1} \left\{\prod\nolimits_\mu N_{F_\mu/F}\beta(\mu')\right\} = \frac{\alpha^q}{\varpi_1^q}$$

in ϕ. Since β^{1-q} is clearly a square, we need only check that α is a square. The character

$$x \longrightarrow \psi_\phi\ (x^q - \alpha x)$$

is identically 1, so that the kernel of the map

$$x \longrightarrow x^q - \alpha x$$

is non-trivial. Thus $\alpha = x^{q-1}$ for some x in ϕ.

Now suppose that

$$m - 1 \geq \frac{t}{[G_0 : G_1]}.$$

We have to show that the complex number σ defined at the beginning of the proof satisfies $\sigma \sim_{2p} 1$. To prove Lemma 14.3 we will have to show that $\sigma \sim_p 1$ if $[G : G_1]$ is a power of 2.

Given $\beta = \beta(\chi_F)$ we may choose $\beta(\chi_{L/F}) = \beta(\chi_{F_\mu/F}) = \beta$. Moreover

$$\beta(\chi_{E/F}) \equiv P^*_{E/F}(\beta, \varpi_F^{m+n}, \varpi_F^{m+n}) \pmod{\mathfrak{P}_E^{d'}}$$

if $m' = m(\chi_{E/F}) = 2d' + \varepsilon'$. By Lemmas 8.3, 8.4 and 8.7

$$P^*_{K/F}(\beta, \varpi_F^{m+n}, \varpi_F^{m+n}) \equiv P^*_{K/E}(\beta(\chi_{E/F}), \varpi_F^{m+n}, \varpi_F^{m+n}) \equiv \beta(\chi_{E/F})$$

modulo $\mathcal{P}_K^{d_1'}$ if

$$\psi_{K/F}(m-1) + 1 = 2d_1' + \varepsilon_1'.$$

Thus

$$\beta(\chi_{E/F}) \equiv P^*_{K/L}(\beta, \varpi_F^{m+n}, \varpi_F^{m+n}) \pmod{\mathfrak{P}_K^{d_1'}}.$$

If

$$\psi_{F_\mu/F}(m-1) + 1 = 2d_\mu + \varepsilon_\mu$$

and

$$\psi_{F_\mu/F}\left(\frac{\alpha(\mu')x}{\varpi_F^{m+n}}\right) = \mu'(1+x)$$

for x in $\mathfrak{P}_{F_\mu}^{d_\mu + \varepsilon_\mu}$ we may take

$$\beta(\mu'\chi_{F_\mu/F}) = \beta + \alpha(\mu').$$

If

$$\psi_{L/F}(m-1) + 1 = 2d_1 + \varepsilon_1$$

then

$$\mu(1+x) = \psi_{L/F}\left(\frac{\alpha(\mu')x}{\varpi_F^{m+n}}\right)$$

for x in $\mathfrak{P}_L^{d_1+\varepsilon_1}$. If $\nu = \mu^\sigma$ then

$$\nu(1+x) = \psi_{L/F}\left(\frac{\alpha(\mu')^\sigma x}{\varpi_F^{m+n}}\right)$$

for x in $\mathfrak{P}_L^{d_1+\varepsilon_1}$. Lemma 8.2 implies that

$$N_{E/F}(\beta(\chi_{E/F})) = N_{K/L}(\beta(\chi_{E/F}))$$

is congruent to

$$\beta \prod\nolimits_{\mu \in T} \prod\nolimits_{\sigma \in M_\mu} (\beta + \alpha(\mu')^\sigma)$$

modulo $\mathfrak{P}_L$. The last expression is equal to

$$\beta \prod_{\mu \in T} N_{F_\mu/F}(\beta + \alpha(\mu')).$$

Moreover

$$\Delta_2(\chi_F, \psi_F, \varpi_F^{m+n}) \sim_p \chi_F^{-1}(\beta)$$
$$\Delta_2(\mu', \psi_{F_\mu/F}, \varpi_F^{1+n}\varpi_{F_\mu}^t) \sim_p 1$$
$$\Delta_2(\chi_{E/F}, \psi_{E/F}, \varpi_F^{m+n}) \sim_p \chi_F^{-1}(N_{E/F}(\beta(\chi_{E/F})))$$
$$\Delta_2(\mu'\chi_{F_\mu/F}, \psi_{F_\mu/F}, \varpi_F^{m+n}) \sim_p \chi_F^{-1}(N_{F_\mu/F}(\beta + \alpha(\mu'))).$$

Define τ by demanding that

$$\Delta_3(\chi_{E/F}, \psi_{E/F}, \varpi_F^{m+n}) \prod_\mu \Delta_3(\mu', \psi_{F_\mu/F}, \varpi_F^{1+n}\varpi_{F_\mu}^t)$$

be equal to

$$\tau\, \Delta_3(\chi_F, \psi_F, \varpi_F^{m+n}) \prod_\mu \Delta_3(\mu', \chi_{F_\mu/F}, \psi_{F_\mu/F}, \varpi_F^{m+n}).$$

Since $\chi_F(u) \sim_p 1$ if $u \in U_F^1$ the preceding discussion shows that $\sigma \sim_p \tau$. Lemmas 9.2 and 9.3 show that $\tau \sim_{2p} 1$. Lemma 14.2 is now completely proved. To prove Lemma 14.3 we have to show that $\tau \sim_p 1$ if $[G : G_1]$ is a power of 2. We may suppose that p is odd.

There are a number of possibilities.

(i.a) t is even and m is odd. $[G_0 : G_1]$ must be odd and hence 1, for we are now assuming that $[G : G_1]$ is a power of 2. Since

$$m(\chi_{F_\mu/F}) = [G_0 : G_1]\,(m-1) + 1$$

and

$$m(\chi_{E/F}) = [G_1 : 1]\,(m-1) - \frac{([G_1 : 1] - 1)t}{[G_0 : G_1]} + 1$$

both $m(\chi_{F_\mu/F})$ and $m(\chi_{E/F})$ are odd.

(i.b) t is even and m is even. Again $[G_0 : G_1]$ is 1. This time both $m(\chi_{F_\mu/F})$ and $m(\chi_{E/F})$ are even.

(ii.a) t is odd and m is odd. Then $m(\chi_{F_\mu/F})$ is odd. If

$$\frac{[G_1 : 1] - 1}{[G_0 : G_1]}$$

is even $m(\chi_{E/F})$ is odd. Otherwise it is even.

(ii.b) t is odd and m is even. If $[G_0 : G_1]$ is odd, that is 1, then $m(\chi_{F_\mu/F})$ is odd and $m(\chi_{E/F})$ is even. If $[G_0 : G_1]$ is even then $m(\chi_{F_\mu/F})$ is odd and $m(\chi_{E/F})$ is even or odd according as

$$\frac{[G_1 : 1] - 1}{[G_0 : G_1]}$$

is even or odd.

If t is odd then clearly

$$\prod_\mu \Delta_3(\mu', \psi_{F_\mu/F}, \varpi_F^{1+n}\varpi_{F_\mu}^t) \sim_p 1.$$

We are going to show that this is also true if t is even. Then L/F, and hence F_μ/F, is unramified. Let $\phi_\mu = O_{F_\mu}/\mathfrak{P}_{F_\mu}$. If

$$\psi_{\phi_\mu}(x) = \psi_{F_\mu/F}\left(\frac{\beta(\mu')x}{\varpi_F^{1+n}}\right)$$

and if φ_{ϕ_μ} is a nowhere vanishing function on ϕ_μ satisfying

$$\varphi_{\phi_\mu}(x+y) = \varphi_{\phi_\mu}(x)\,\varphi_{\phi_\mu}(y)\psi_{\phi_\mu}(xy)$$

then

$$\Delta_3(\mu', \psi_{F_\mu/F}, \varpi_F^{1+n}\varpi_{F_\mu}^t) \sim_p A[-\sigma(\varphi_{\phi_\mu})].$$

If α belongs to ϕ_μ^* let $\nu_{\phi_\mu}(\alpha)$ equal +1 or -1 according as α is or is not a square in ϕ_μ. If $\phi = O_F/\mathfrak{P}_F$ then

$$\nu_{\phi_\mu}(\alpha) = \nu_\phi\ (N_{\phi_\mu/\phi}(\alpha)).$$

If

$$\psi_\phi(x) = \psi_F\left(\frac{x}{\varpi_F^{1+n}}\right)$$

then, according to paragraph 9,

$$\Delta_3(\mu', \psi_{F_\mu/F}, \varpi_F^{1+n}\varpi_{F_\mu}^t) \sim_p \nu_\phi(N_{F_\mu/F}(\beta(\mu')))\,\{A[-\sigma(\varphi_\phi)]\}^{[F_\mu:F]}$$

if φ_ϕ is any nowhere vanishing function on ϕ satisfying

$$\varphi_\phi(x+y) = \varphi_\phi(x)\,\varphi_\phi(x)\,\psi_\phi(xy).$$

Thus if a is the number of μ in T

$$\prod_\mu \Delta_3(\mu', \psi_{F_\mu/F}, \varpi_F^{1+n}\varpi_{F_\mu}^t)$$

is equal to

$$\eta(-1)^a\,\nu_\phi\,\left(\prod_\mu N_{F_\mu/F}(\beta(\mu'))\right)\,A[\sigma(\varphi_\phi)^{q-1}]$$

where $\eta \sim_p 1$ and $q = [G_1 : 1]$.

We saw in paragraph 9 that

$$A[\sigma(\varphi_\phi)^2] \sim_p \nu_\phi(-1)\ A[|\sigma(\varphi_\phi)|^2] = \nu_\phi(-1).$$

Since t is even $G_0 = G_1$ and $G/G_1 = G/G_0$ is abelian. If $\sigma \in G$

$$\{\mu \in S(K/L) \mid \mu = \mu^\sigma\}$$

is a subgroup of $S(K/L)$ invariant under G. It is necessarily either $S(K/L)$ or $\{1\}$. If σ is not in G_1 it is not $S(K/L)$. Thus G_μ, the isotropy group of μ, is G_1 for all μ in T and $F_\mu = L$. Moreover

$$\prod_\mu N_{F_\mu/F}(\beta(\mu')) = \prod_\mu \prod_{\sigma\in G/G_1} \beta(\mu')^\sigma.$$

We may regard $C = G_1$ as a vector space over the field with p elements. If $\sigma \in G/G_1$ and the order of σ divides $p-1$ then all the eigenvalues of the linear transformation $c \longrightarrow \sigma c\sigma^{-1}$ lie in the prime field. Since the linear transformation also has order dividing $p-1$ it is diagonalizable. Since G/G_1 is abelian and acts irreducibly on C the linear transformation is a multiple of the identity. In particular if σ_0 is the unique element of order 2 then $\sigma_0 c\sigma_0^{-1} = c^{-1}$ for all c. As a consequence $\mu^{\sigma_0} = \mu^{-1}$ and

$$\beta(\mu')^{\sigma_0} \equiv -\beta(\mu') \pmod{\mathfrak{P}_L}$$

if we choose, as we may since F_μ/F is unramified, $\varpi_{F_\mu} = \varpi_F$. If D is the group $\{1, \sigma_0\}$ and M is a set of representatives for the cosets of D in G/G_1 then

$$\prod_{\mu\in T} \prod_{\sigma\in G/G_1} \beta(\mu')^\sigma = \gamma\gamma^{\sigma_0}$$

if

$$\gamma = \prod_{\mu\in T} \prod_{\sigma\in M} \beta(\mu')^\sigma.$$

Clearly

$$\gamma\gamma^{\sigma_0} = (1-)^{\frac{q-1}{2}}\gamma^2 \pmod{\mathfrak{P}_L}.$$

If χ is the non-trivial character of D and

$$v : G/G_0 \longrightarrow D$$

is the transfer then

$$\gamma^\sigma = \chi(v(\sigma))^a\gamma$$

for all σ in G/G_0. $\nu_\phi(\gamma^2) = 1$ if and only if $\chi(v(\sigma))^a$ is 1 for all σ. If σ is a generator of G/G_0 then

$$v(\sigma) = \sigma^{\frac{[G:G_0]}{2}} = \sigma_0$$

so that $\nu_\phi(\gamma^2) = (-1)^a$. Putting all these facts together we see that

$$\prod_\mu \Delta_3(\mu', \psi_{F_\mu/F}, \varpi_F^{1+n}\varpi_{F_\mu}^t) \sim_p 1.$$

Observe that if we had taken ϖ_{F_μ} to be $\delta_\mu\varpi_F$ then $N_{F_\mu/F}\beta(\mu')$ would have to be multiplied by

$$\{N_{F_\mu/F}\delta_\mu\}^t$$

which is a square modulo $\mathfrak{P}_F$ because t is even. Thus the result is valid for all choices of ϖ_{F_μ}.

Eventually we will have to discuss the various possibilities separately. There are however a number of comments we should make first. If m is odd and $m(\chi_{F_\mu/F})$ is odd then

$$\Delta_3(\mu'\chi_{F_\mu/F}, \psi_{F_\mu/F}, \varpi_F^{m+n}) \sim_p \nu_{\phi_\mu}(\beta + \alpha(\mu'))\ A[-\sigma(\varphi_{\phi_\mu})]$$

if

$$\psi_{\phi_\mu}(x) = \psi_{F_\mu/F}\left(\frac{x}{\varpi_F^{1+n}}\right).$$

Observe that, because m is odd, we may take the number δ in Lemma 9.3 to be $\varpi_F^{\frac{m-1}{2}}$. Of course φ_{ϕ_μ} is any function on ϕ_μ which vanishes nowhere and satisfies

$$\varphi_{\phi_\mu}(x+y) = \varphi_{\phi_\mu}(x)\ \varphi_{\phi_\mu}(y)\psi_{\phi_\mu}(xy).$$

Applying Lemma 9.1 we see that

$$A[-\sigma(\varphi_{\phi_\mu})] \sim_p -\nu_\phi\left(k^{\frac{[F_\mu:F]}{k}}\right)\ A\left[\sigma(\varphi_\phi)^{\frac{[F_\mu:F]}{k}}\right]$$

if $k = [G_0 : G_1]$, if

$$\psi_\phi(x) = \psi_F\left(\frac{x}{\varpi_F^{1+n}}\right)$$

and if φ_ϕ bears the usual relation to ψ_ϕ. We use, of course, the relation

$$kS_{\phi_\mu/\phi}(x) = S_{F_\mu/F}(x).$$

Observe also that

$$\nu_{\phi_\mu}(\beta+\alpha(\mu')) = \nu_\phi(N_{\phi_\mu/\phi}(\beta+\alpha(\mu'))).$$

If m is odd

$$\Delta_3(\chi_F, \psi_F, \varpi_F^{m+n}) \sim_p -\nu_\phi(\beta)\ A[\sigma(\varphi_\phi)].$$

If both m and $m' = m(\chi_{E/F})$ are odd and if $\beta' = \beta(\chi_{E/F})$ then

$$\Delta_3(\chi_{E/F}, \psi_{E/F}, \varpi_F^{m+n}) \sim_p -\nu_\phi(\beta')\ A[\sigma(\varphi'_\phi)]$$

if φ'_ϕ bears the usual relation to the character

$$\psi'_\phi(x) = \psi_{E/F}\ \left(\frac{x}{\varpi_F^{1+n}\varpi_E^{\frac{(q-1)t}{k}}}\right).$$

There is a unit ε in O_K such that $\varpi_E = \varepsilon\varpi_K^q$. If $\sigma \in C$ then

$$\varpi_E^{\sigma-1} = \varepsilon^{\sigma-1}\varpi_K^{(\sigma-1)q} \equiv 1 \pmod{\mathfrak{P}_K}$$

because $t \geq 1$. Thus the multiplicative congruence

$$\varpi_E^q \equiv N_{E/F}\varpi_E = \varpi_F \quad (\operatorname{mod}^* \mathfrak{P}_E)$$

is satisfied and

$$\frac{1}{\varpi_E^{\frac{(q-1)t}{k}}} \equiv \frac{\varpi_F^{1+n}}{\varpi_E^{1+n'}} \quad (\operatorname{mod}^* \mathfrak{P}_E).$$

If

$$\omega_1 = S\left(\frac{\varpi_F^{1+n}}{\varpi_E^{1+n'}}\right)$$

as before, then

$$\psi'_\phi(x) = \psi_F\left(\frac{\omega_1 x}{\varpi_F^{1+n}}\right).$$

Since

$$\nu_\phi(\beta') = \nu_\phi(\beta')^q = \nu_\phi(N_{E/F}\beta')$$

we have

$$\Delta_3(\chi_{E/F}, \psi_{E/F}, \varpi_F^{m+n}) \sim_p -\nu_\phi(N_{E/F}\beta')\,\nu_\phi(\omega_1)\ \ A[\sigma(\varphi_\phi)].$$

Define η by demanding that

$$\Delta_3(\chi_{E/F}, \psi_{E/F}, \varpi_F^{m+n})$$

be equal to

$$\eta\Delta_3(\chi_F, \psi_F, \varpi_F^{m+n})\ \prod_\mu \Delta_3\left(\mu'\chi_{F_\mu/F}, \psi_{F_\mu/F}, \varpi_F^{m+n}\right).$$

We have to show that $\eta \sim_p 1$. If both t and m are even this is clear. If t is even and m is odd we are to show that

$$\nu_\phi(N_{E/F}\beta')\nu_\phi(\omega_1) \sim_p (-1)^a\ \nu_\phi(-1)^{\frac{q-1}{2k}}\nu_\phi(k)^{\frac{q-1}{k}}\ \nu_\phi(\beta)\prod_\mu \nu_\phi(N_{\phi_\mu/\phi}(\beta+\alpha(\mu')))$$

if a is the number of elements in T. Since t is even k is 1. As before

$$\beta\prod_\mu N_{\phi_\mu/\phi}(\beta+\alpha(\mu')) = \beta\prod_\mu\ \prod_{\sigma\in G/G_1}(\beta+\alpha(\mu')^\sigma)$$

is congruent to $N_{E/F}\beta'$ modulo $\mathfrak{P}_K$. All we need do is show that

$$\nu_\phi(\omega_1) = (-1)^a\ \nu_\phi(-1)^{\frac{q-1}{2}}.$$

Since t is even each γ_μ is a square in ϕ. Applying the identity (14.3) we see that

$$\nu_\phi(\omega_1) = \nu_\phi(\omega_1^q) = \nu_\phi(\alpha)\nu_\phi^{-1}\left(\prod_\mu N_{F_\mu/F}\beta(\mu')\right).$$

We have seen that α is a square in ϕ so that $\nu_\phi(\alpha) = 1$. We also saw that

$$\nu_\phi\left(\prod_\mu N_{F_\mu/F}\beta(\mu')\right) = (-1)^a\ \nu_\phi(-1)^{\frac{q-1}{2}}$$

when t is even. The required relation follows.

We suppose henceforth that t is odd. The discussion will be fairly complicated. Suppose first that m is also odd. Then

$$[G_0 : G_1](m-1) \neq t$$

and

$$m - 1 > \frac{t}{[G_0 : G_1]}$$

so that

$$\beta + \alpha(\mu') \equiv \beta \pmod{\mathfrak{P}_L}$$

and

$$\prod_\mu \Delta_3(\mu' \chi_{F_\mu/F}, \psi_{F_\mu/F}, \varpi_F^{m+n}) \sim_p (-1)^a \; \nu_\phi\left(k^{\frac{q-1}{k}}\right) \; \nu_\phi\left(\beta^{\frac{q-1}{k}}\right) \;\; A[\sigma(\varphi_\phi)]^{\frac{q-1}{k}}.$$

Thus if $\frac{q-1}{k}$ is odd we have to show that

$$(-1)^{a+1}\,\nu_\phi(k)\;\nu_\phi(-1)^{\frac{q-1}{2k}+\frac{1}{2}} \sim_p 1 \tag{14.4}$$

and if $\frac{q-1}{k}$ is even we have to show that

$$\nu_\phi(\omega_1) \sim_p (-1)^a\,\nu_\phi(-1)^{\frac{q-1}{2k}}. \tag{14.5}$$

Now suppose m is even. If $[G_0 : G_1]$ is 1 there is nothing to prove. If $k = [G_0 : G_1]$ is even then

$$m - 1 > \frac{t}{[G_0 : G_1]}$$

and

$$\beta + \alpha(\mu') \equiv \beta \pmod{\mathfrak{P}_L}.$$

If

$$\psi'_{\phi_\mu}(x) = \psi_{F_\mu/F}\left(\beta \frac{\varpi_{F_\mu}^{k(m-1)} x}{\varpi_F^{m+n}}\right)$$

and φ'_{ϕ_μ} is a function on ϕ_μ which vanishes nowhere and satisfies

$$\varphi'_{\phi_\mu}(x+y) = \varphi'_{\phi_\mu}(x)\,\varphi'_{\phi_\mu}(y)\,\psi'_{\phi_\mu}(xy)$$

then

$$\Delta_3(\mu' \chi_{F_\mu/F}, \psi_{F_\mu/F}, \varpi_F^{m+n}) \sim_p \;\; A[-\sigma(\varphi'_{\phi_\mu})].$$

If

$$\varepsilon_\mu \varpi_F^{m-1} = \varpi_{F_\mu}^{k(m-1)}$$

then ε_μ is a unit and

$$\psi_{\phi_\mu}(x) = \psi_{\phi_\mu/\phi}(k\beta\varepsilon_\mu x)$$

if, as before,

$$\psi_\phi(x) = \psi_F\left(\frac{x}{\varpi_F^{1+n}}\right).$$

By Lemma 9.1, $A[-\sigma(\varphi_{\phi_\mu})]$ is equal to

$$-\nu_\phi\left(k^{\frac{[F_\mu:F]}{k}}\right) \;\; \nu_\phi\left(\beta^{\frac{[F_\mu:F]}{k}}\right) \; \nu_\phi(N_{\phi_\mu/\phi}\varepsilon_\mu) \;\; A[\sigma(\varphi_\phi)]^{\frac{[F_\mu:F]}{k}}.$$

If $\frac{q-1}{k}$ is even we have to show that

$$(-1)^a\,\nu_\phi\left(\prod_\mu N_{\phi_\mu/\phi}\varepsilon_\mu\right) \;\; \nu_\phi(-1)^{\frac{q-1}{2k}} \sim_p 1 \tag{14.6}$$

If $\frac{q-1}{k}$ is odd then $m' = m(\chi_{E/F})$ is odd. If

$$\psi''_\phi(x) = \psi_{E/F}\left(\beta' \frac{\varpi_E^{m'-1} x}{\varpi_F^{m+n}}\right)$$

and φ''_ϕ bears the usual relation to ψ''_ϕ then

$$\Delta_3(\chi_{E/F}, \psi_{E/F}, \varpi_F^{m+n}) \sim_p \ A[-\sigma(\varphi''_\phi)].$$

Now $\nu_\phi(\beta') = \nu_\phi(\beta')^q$ and

$$(\beta')^q \equiv N_{E/F}\beta'$$

which in turn is congruent to

$$\beta \prod\nolimits_{\mu\in T} \ \prod\nolimits_{\sigma\in M_\mu} (\beta + \alpha(\mu')^\sigma) \equiv \beta^q$$

modulo $\mathfrak{P}_K$. Let

$$\varepsilon_1 \varpi_F^{m+n} = \varpi_E^{q(m+n)}$$

and, as before,

$$\omega_1 = S_{E/F}\left(\frac{\varpi_F^{1+n}}{\varpi_E^{1+n'}}\right)$$

then

$$A[-\sigma(\varphi''_\phi)] \sim_p \ \nu_\phi(\omega_1)\,\nu_\phi(\varepsilon_1)\,\nu_\phi(\beta)\ A[-\sigma(\varphi_\phi)].$$

We saw that

$$\varpi_E^q \equiv \varpi_F \pmod{^*\,\mathfrak{P}_E}$$

so that

$$\varepsilon_1 \equiv 1 \pmod{\mathfrak{P}_E}.$$

Thus we have to show that

$$\nu_\phi(\omega_1) \sim_p (-1)^{a+1}\,\nu_\phi(k)\,\nu_\phi(-1)^{\frac{q-1}{2k}-\frac{1}{2}}\ \nu_\phi\ \left(\prod\nolimits_\mu N_{\phi_\mu/\phi}\varepsilon_\mu\right). \tag{14.7}$$

The four identities (14.4), (14.5), (14.6), and (14.7) look rather innocuous. However to prove them is not an entirely trivial matter. We first consider the case that G/G_1 is abelian. If $\sigma_0 \in G/G_1$ is of order 2, the argument used before shows that $\sigma_0 c \sigma_0^{-1} = c^{-1}$ for all c in C. Since the representation of G/G_1 on C is faithful G/G_1 has only one element of order 2 and is therefore cyclic. In this case $F_\mu = L$ for all μ and $a = \frac{q-1}{[G:G_1]}$. We may choose $\varpi_{F_\mu} = \varpi_L$. If

$$N_{L/F}\varpi_L = \gamma\varpi_F^{[G:G_0]}$$

then $\gamma_\mu = \gamma^t$ and

$$\prod\nolimits_\mu \ \gamma_\mu = \gamma^{at}.$$

If $[G_0 : G_1] = 1$ we may choose $\varpi_L = \varpi_F$ so that $\gamma = 1$. The argument used before shows that

$$\nu_\phi\left(\prod_{\mu\in T}\prod_{\sigma\in G/G_1}\beta(\mu')^\sigma\right) = (-1)^a\,\nu_\phi(-1)^{\frac{q-1}{2}}.$$

The identity (14.3) shows that

$$\nu_\phi(\omega_1) = (-1)^a\,\nu_\phi(-1)^{\frac{q-1}{2k}}.$$

The identity (14.5) which is the only one of concern here becomes

$$\nu_\phi(-1)^{\frac{q-1}{2}} = \nu_\phi(-1)^{\frac{q-1}{2k}}$$

which is clear because $k = [G_0 : G_1] = 1$.

Now take $[G : G_0] = 1$. We may choose $\varpi_E = N_{K/E}\varpi_K$ so that $\varpi_F = N_{L/F}\varpi_L$ and γ is again 1. It is perhaps worth pointing out these special choices are not inconsistent with any choices yet made in this paragraph. This is necessary because the arguments appearing in the functions Δ_2 must be the same as those appearing in the functions Δ_3. We previously defined

$$\delta = \frac{\varpi_F^{1+n}}{\varpi_E^{1+n'}}\cdot\frac{\varpi_L^t}{\varpi_K^t}$$

and showed that

$$N_{K/L}\delta = \frac{\varpi_L^{t(q-1)}}{\varpi_F^{\frac{t(q-1)}{k}}}.$$

Observe that

$$\frac{\varpi_L^k}{\varpi_F} = \prod_{\sigma\in G/G_1}\varpi_L^{1-\sigma} \equiv \prod\theta_0(\sigma)^{-1} \equiv -1 \pmod{\mathfrak{P}_L}$$

because

$$\{\theta_0(\sigma) \mid \sigma\in G/G_1\}$$

is just the set of kth roots of unity in ϕ and k is a power of 2. It is not 1 because

$$[G_0 : G_1] = [G : G_1] > 1.$$

Since

$$\delta^q \equiv N_{K/L}\delta \pmod{\mathfrak{P}_K}$$

we have

$$\nu_\phi(\delta) = \nu_\phi(-1)^{\frac{q-1}{k}}.$$

If as before

$$\psi_{L/F}\left(\frac{\beta_1(\nu)x}{\varpi_F^{1+n}\varpi_L^t}\right) = \nu(1+x)$$

for x in $\mathfrak{P}_L^s$ and ν in $S(K/L)$ then, as we saw when proving the identity (14.3),

$$\omega_1^q \equiv \delta^q\alpha^q\left\{\prod_{\nu\neq 1}\beta_1(\nu)\right\} \pmod{\mathfrak{P}_L}.$$

Thus
$$\nu_\phi(\omega_1) = \nu_\phi(-1)^{\frac{q-1}{k}} \prod\nolimits_{\nu\neq 1} \nu_\phi(\beta_1(\nu)).$$

We can choose $\frac{q-1}{p-1}$ elements ν_i in $S(K/L)$ so that every non-trivial element of $S(K/L)$ is of the form $\nu_i^j,\ 0<j<p$. Then

$$\prod\nolimits_{\nu\neq 1} \nu_\phi(\beta_1(\nu)) = \nu_\phi\left(\prod\nolimits_{i=1}^{\frac{q-1}{p-1}} \prod\nolimits_{j=1}^{p-1} j\beta(\nu_i)\right) = \nu_\phi(-1)^{\frac{q-1}{p-1}}$$

because
$$\nu_\phi(\beta(\nu_i))^{p-1} = 1.$$

When m is even
$$\nu_\phi(\varepsilon_\mu) = \nu_\phi\ \left(\frac{\varpi_L^k}{\varpi_F}\right) = \nu_\phi(-1).$$

Since $a = \frac{q-1}{k}$ the identities (14.4), (14.5), (14.6) and (14.7) become

$$\nu_\phi(k)\,\nu_\phi(-1)^{\frac{q-1}{2k}+\frac{1}{2}} = 1 \tag{14.4$'$}$$

$$\nu_\phi(-1)^{\frac{q-1}{p-1}} = \nu_\phi(-1)^{\frac{q-1}{2k}} \tag{14.5$'$}$$

$$\nu_\phi(-1)^{\frac{q-1}{2k}} = 1 \tag{14.6$'$}$$

$$\nu_\phi(-1)^{\frac{q-1}{k}}\nu_\phi(-1)^{\frac{q-1}{p-1}} = \nu_\phi(k)\ \nu_\phi(-1)^{\frac{q-1}{2k}+\frac{1}{2}}\,\nu_\phi(-1)^{\frac{q-1}{k}}. \tag{14.7$'$}$$

If $p\equiv 1 \pmod 4$ the identities (14.5′) and (14.6′) are clearly valid. Moreover for (14.5′) and (14.6′) the number $\frac{q-1}{k}$ is even. Since k is a positive power of 2, q is an even power of p if $p\equiv 3 \pmod 4$. If $q = p^{2f}$ then
$$\frac{q-1}{p-1} = 1 + p + \ldots + p^{2f-1} \equiv 0 \pmod 4$$

and the left side of (14.5′) is 1. If $\frac{q-1}{2k}$ is even (14.5′) and (14.6′) are now clear. If it is odd, 4 divides k because 8 divides $q-1$. But $\{\theta_0(\sigma)\mid \sigma\in G_0/G_1\}$ is the set of kth roots of unity in $O_L/\mathfrak{P}_L = \phi$ so -1 is a square in $\phi, \nu_\phi(-1)=1$, and the relations are valid in this case too. The relations (14.4′) and (14.7′) are obvious if the degree of ϕ over the prime field ϕ_0 is even. Since $\phi^\times$ contains the kth roots of unity and k is a power of 2 the degree can be odd only if k divides $p-1$. Since

$$\frac{q-1}{k} = \frac{q-1}{p-1}\cdot\frac{p-1}{k}$$

and $\frac{q-1}{k}$ is now odd $\frac{p-1}{k}$ must also be odd and by quadratic reciprocity

$$\nu_\phi(k) = \nu_{\phi_0}(k) = \nu_{\phi_0}(-1)\,\nu_{\phi_0}\left(\frac{p-1}{k}\right) = \nu_{\phi_0}(-1)\,\nu_{\phi_0}(-1)^{\frac{p-1}{2k}-\frac{1}{2}}$$

because
$$p\equiv 1\left(\operatorname{mod}\frac{p-1}{k}\right).$$

If $p \equiv 1 \pmod 4$ the two relations are now clear. If $p \equiv 3 \pmod 4$ and $q = p^f$

$$\frac{q-1}{p-1} = 1 + p + \ldots + p^{f-1}$$

must be odd. It is therefore congruent to 1 modulo 4. (14.4′) becomes

$$\nu_{\phi_0}(-1)\ \nu_{\phi_0}(-1)^{\frac{p-1}{k}} = 1$$

and (14.7′) becomes

$$\nu_{\phi_0}(-1) = \nu_{\phi_0}(-1).$$

There is no question that both these relations are valid.

We have still to treat the case that G/G_1 is abelian while neither $[G : G_0]$ nor $[G_0 : G_1]$ is 1. Then

$$N_{F_\mu/F}\beta(\mu') \equiv \left\{\prod\nolimits_{\sigma\in G/G_0} \beta(\mu')\right\}^k \pmod{\mathfrak{P}_{F_\mu}}$$

is a square in ϕ and the identity (14.3) implies that

$$\nu_\phi(\omega_1) = \nu_\phi(\gamma^a)$$

$C_F/N_{L/F}C_L$ is cyclic of order $[G : G_1]$. It has a generator which contains an element of the form $\gamma_1\varpi_F$. Moreover the coset of

$$(\gamma_1\varpi_F)^{[G:G_0]}\ N_{L/F}\varpi_L^{-1} = \gamma_1^{[G:G_0]}\gamma^{-1}$$

is a generator of $U_F/U_F \cap N_{L/F}C_L$. The order of this group is a power of 2 and p is odd so every element of $U_F \cap N_{L/F}C_L$ is a square. Consequently γ cannot be a square and $\nu_\phi(\gamma) = -1$. If m is even and F' is the fixed field of G_0 then

$$\varepsilon_\mu = \left(\frac{\varpi_L^k}{\varpi_F}\right)^{m-1} = \left(\frac{N_{L/F'}\varpi_L}{\varpi_F}\right)^{m-1} \left(\prod\nolimits_{\sigma\in G_0/G_1} \varpi_L^{1-\sigma}\right)^{m-1}$$

which is congruent to

$$-\left(\frac{N_{L/F'}\varpi_L}{\varpi_F}\right)^{m-1}$$

modulo $\mathfrak{P}_L$. Since $[F' : F]$ is even

$$N_{\phi_\mu/\phi}\,\varepsilon_\mu = N_{F'/F}\,\varepsilon_\mu = \left(\frac{N_{L/F}\varpi_L}{\varpi_F^{[G:G_0]}}\right)^{m-1} = \gamma^{m-1}$$

and

$$\nu_\phi(N_{\phi_\mu/\phi}\,\varepsilon_\mu) = \nu_\phi(\gamma) = -1.$$

Because

$$a = \frac{q-1}{[G:G_1]}$$

is integral, $\frac{q-1}{k}$ is even, and we need only worry about the identities (14.5) and (14.6). They both reduce to

$$\nu_\phi(-1)^{\frac{q-1}{2k}} = 1.$$

To prove this we show that $\frac{q-1}{2k}$ is even if $\nu_\phi(-1) = -1$. Since

$$k = [U_F : U_F \cap N_{L/F} C_L]$$

and this index must divide the order of ϕ^* the number $\nu_\phi(-1)$ is -1 only if $k = 2$. Of course p will be congruent to 3 modulo 4. Since 4 divides $q-1$, q is an even power of p and $q \equiv 1 \pmod 8$. Thus

$$\frac{q-1}{2k} = \frac{q-1}{4}$$

is even.

Now suppose that G/G_1 is not abelian. Let $\sigma \longrightarrow x(\sigma)$ be a given isomorphism of G_0/G_1 with $\mathbb{Z}/k\mathbb{Z}$ and let $x \longrightarrow \sigma(x)$ be its inverse. Let $\tau \longrightarrow \lambda(\tau)$ be that homomorphism of G/G_0 into the units of $\mathbb{Z}/k\mathbb{Z}$ which satisfies

$$x(\tau\sigma\tau^{-1}) = \lambda(\tau)\, x(\sigma).$$

There is precisely one element of order 2 in G_0/G_1, namely $\sigma\left(\frac{k}{2}\right)$, and it lies in the center of G/G_1. Since G/G_0 is cyclic, G/G_1 is non-abelian only if $k > 2$. Choose a fixed σ_0 in G which generates G/G_0 and set

$$\mu_0 = \lambda(\sigma_0)$$

and

$$y_0 = x(\sigma_0^{[G:G_0]}).$$

We shall sometimes regard C as a vector space over the field with p elements. If σ belongs to G/G_1 let $\pi(\sigma)$ be the linear transformation

$$c \longrightarrow \sigma c \sigma^{-1}.$$

The dual space will be identified with $S(K/L)$ and π^* will be the representation contragredient to π.

The relation

$$N_{F_\mu/F}\beta(\mu') \equiv \left\{\prod\nolimits_{\sigma \in G/G_\mu G_0} \beta(\mu')^\sigma\right\}^k$$

together with the identity (14.3) implies that

$$\nu_\phi(\omega_1) = \nu_\phi\left(\prod\nolimits_\mu \gamma_\mu\right).$$

Moreover if m is even and F'_μ is the fixed field of $G_\mu G_0$

$$\varepsilon_\mu = \left(\frac{\varpi_{F_\mu}^k}{\varpi_F}\right)^{m-1} = \left\{\frac{N_{F_\mu/F'_\mu}\varpi_{F_\mu}}{\varpi_F}\right\}^{m-1} \left\{\prod\nolimits_{\sigma \in G_0/G_1} \varpi_{F_\mu}^{1-\sigma}\right\}^{m-1}$$

which is congruent to

$$\left\{-\frac{N_{F_\mu/F'_\mu}\varpi_{F_\mu}}{\varpi_F}\right\}^{m-1}$$

modulo $\mathfrak{P}_{F_\mu}$. Since

$$\{N_{\phi_\mu/\phi}\,\varepsilon_\mu\}^t = N_{F'_\mu/F}\,\left\{-\frac{N_{F_\mu/F'_\mu}\varpi_{F_\mu}}{\varpi_F}\right\}^{(m-1)t}$$

which equals

$$(-1)^{t[\phi_\mu:\phi]}\ \gamma_\mu^{m-1}$$

and t is odd

$$\nu_\phi(N_{\phi_\mu/\phi}\,\varepsilon_\mu) = \nu_\phi(-1)^{[\phi_\mu:\phi]}\,\nu_\phi(\gamma_\mu).$$

These relations will be used frequently and without comment.

I want to discuss the case $[G:G_0]=2$ and $\mu_0 \equiv -1 \pmod 4$ first. Since

$$(-\mu_0)^2 = \mu_0^2 = \lambda(\sigma_0^2) \equiv 1 \pmod k$$

we must have

$$-\mu_0 \equiv 1 \pmod k$$

or, if $k>4$,

$$-\mu_0 \equiv \frac{k}{2}+1 \pmod k.$$

Then

$$\mu_0 \equiv -1 \pmod k$$

or

$$\mu_0 \equiv \frac{k}{2}-1 \pmod k.$$

Since

$$\mu_0 - 1 \equiv 2 \pmod 4$$

the centralizer of σ_0 in G_0/G_1 consists of the identity and $\sigma\left(\frac{k}{2}\right)$. Thus $x(\sigma_0^2)$ is 0 or $\frac{k}{2}$.

Suppose $\mu_0 \equiv -1 \pmod k$ and $x(\sigma_0^2) = \frac{k}{2}$. If σ belongs to G_0/G_1 then $\sigma_0\sigma\sigma_0^{-1} = \sigma^{-1}$ and $(\sigma_0\sigma)^2 = \sigma_0^2$. Thus $\sigma\left(\frac{k}{2}\right)$ is the only element of order 2 in G/G_1. If σ belongs to G/G_1 then σ has a non-trivial fixed point in $S(K/L)$ if and only if $\pi(\sigma)$ has 1 as an eigenvalue. If $\sigma \neq 1$ there is an integer n such that σ^n has order 2. Then $\pi(\sigma^n)$ also has 1 as an eigenvalue. Thus if any non-trivial element of G/G_1 has a non-trivial fixed point there is an element τ of order 2 such that $\pi(\tau)$ has 1 as an eigenvalue. The usual argument shows that

$$\pi\left(\sigma\left(\frac{k}{2}\right)\right) = -I$$

so that, in the case under consideration, only the identity has fixed points. Then

$$a = \frac{q-1}{[G:G_1]}.$$

In particular $\frac{q-1}{k}$ is even. We choose $\varpi_{F_\mu} = \varpi_L$ and let

$$\gamma\varpi_F^{[G:G_0]} = N_{L/F}\varpi_L.$$

Only identities (14.5) and (14.6) are to be considered. (14.5) reduces to

$$\nu_\phi(\gamma)^{at} = (-1)^a\, \nu_\phi(-1)^{\frac{q-1}{2k}}$$

and (14.6) reduces to

$$(-1)^a\, \nu_\phi(-1)^{a[G:G_0]}\, \nu_\phi(\gamma)^{at}\, \nu_\phi(-1)^{\frac{q-1}{2k}} = 1.$$

Since $[G : G_0]$ is even they are equivalent. Suppose ϕ has r elements. If $x \in \lambda = O_L/\mathfrak{P}_L$ then $x^{\sigma_0} = x^{r^f}$ for some f. If σ belongs to G_0/G_1 then

$$\theta_0(\sigma)^{\mu_0 r^f} = \theta_0(\sigma_0\sigma\sigma_0^{-1})^{r^f} \equiv \left(\frac{\varpi_L^{\sigma_0\sigma}}{\varpi_L^{\sigma_0}}\right)^{r^f\sigma_o^{-1}} \equiv \theta_0(\sigma).$$

Thus

$$\mu_0^{r^f} \equiv 1 \pmod k$$

and

$$r \equiv -1 \pmod 4$$

so that $\nu_\phi(-1) = -1$. Since, in the present case,

$$a = \frac{q-1}{2k}$$

the identities become

$$\nu_\phi(\gamma)^{at} = 1.$$

The map

$$\tau_{L/F} : W_{L/F} \longrightarrow C_F$$

determines a map of G/G_1 onto $C_F/N_{L/F}C_L$. The image of σ_0 contains an element of the form $\gamma_1\varpi_F$ where γ_1 is a unit. The image of σ_0^2 is 1 because the commutator subgroup contains

$$\{\sigma((\mu_0 - 1)x)\} = \{\sigma(x) \mid x \equiv 0 \pmod 2)\}$$

and in particular contains σ_0^2. Since $[G : G_0] = 2$ the number $\gamma\gamma_1^{-2}$ lies in $U_F \cap N_{L/F}C_L$. The index of the commutator subgroup of G/G_1 in G/G_1 is 4 so

$$[U_F : U_F \cap N_{L/F}C_L] = 2.$$

Consequently $\gamma\gamma_1^{-2}$ and γ are both squares and $\nu_\phi(\gamma) = 1$.

Now suppose $\mu_0 \equiv -1 \pmod k$ and $x(\sigma_0^2) = 0$. Every element of the form $\sigma_0\sigma,\ \sigma \in G_0/G_1$, has order 2. If $\pi(\sigma_0\sigma) = -I$ then $\sigma_0\sigma$ lies in the center of G/G_1 which is impossible. Thus $\pi(\sigma_0\sigma)$ has 1 as an eigenvalue. If $\tau \in G_0/G_1$ then

$$\tau^{-1}\sigma_0\sigma\tau = \sigma_0\sigma\tau^2$$

so there are two conjugacy classes in the set $\sigma_0 G_0/G_1$. One has σ_0 as representative and the other has $\sigma_1 = \sigma_0\sigma(1)$.

Let V be a non-trivial subspace of $S(K/L)$ invariant and irreducible under the action of G_0/G_1. Suppose first that V is also invariant under $\pi^*(\sigma_0)$ so that $V = S(K/L)$. Choose $v_0 \neq 0$ so that

$\pi^*(\sigma_0)v_0 = v_0$. Let λ' be the field obtained by adjoining the kth roots of unity to the prime field. Certainly $\lambda' \subseteq \lambda$ and, since

$$\theta_0(\sigma)^{\sigma_0} = \theta_0(\sigma_0^{-1}\sigma\sigma_0),$$

λ' is not contained in ϕ. Let $\phi' = \phi \cap \lambda'$. We may regard $\{1, \sigma_0\}$ as $\mathfrak{G}(\lambda'/\phi')$. The map φ which sends σ in G_0/G_1 to $(\theta_0^{-1}(\sigma), 1)$ and $\sigma\sigma_0$ to $(\theta_0^{-1}(\sigma), \sigma_0)$ is an isomorphism of G/G_1 with the semi-direct product of the kth roots of unity in λ' and $\mathfrak{G}(\lambda'/\phi')$. There is a unique map, again denoted by φ, of V onto λ' such that $\varphi(v_0) = 1$ while

$$\varphi(\pi^*(\tau)v) = \varphi(\tau)\varphi(v)$$

for τ in G/G_1. Of course the kth roots of unity act on λ' by left multiplication. The Galois group acts by $\sigma_0\alpha = \alpha^{\sigma_0^{-1}}$. Putting the actions together we get an action of the semi-direct product. To study the action of G/G_1 on V we study the equivalent action of the semi-direct product in λ'.

It is best to consider a more general situation. Suppose ϕ' is a finite field with p^f elements, λ' is an extension of ϕ' with p^ℓ elements and Γ is the semi-direct product of the group of kth roots of unity, where k divides $p^\ell - 1$, and $\mathfrak{G}(\lambda'/\phi')$. Γ acts on λ' as before. Let $\ell = nf$. If $0 \le j_1 < n, j = (j_1, n)$, and ρ is the automorphism $x \longrightarrow x^{p^f}$ of λ'/ϕ' then the number of elements of λ' fixed by a member of Γ of the form (α, ρ^{j_i}) where α is a kth root of unity is the same as the number of elements fixed by some other member of the form (β, ρ^{-j}). Indeed if

$$b\,\frac{j_1}{j} \equiv -1 \left(\mathrm{mod}\,\frac{n}{j}\right)$$

and b is prime to the order of (α, ρ^{j_1}) we can take

$$(\beta, \rho^{-j}) = (\alpha, \rho^{j_1})^b.$$

Let θ be a generator of the multiplicative group of λ'. The equation

$$\beta\,\theta^{m\rho^j} = \theta^m$$

can be solved for β if and only if $\theta^{m(p^{jf}-1)}$ has order dividing k, that is, if and only if $p^\ell - 1$ divides $km(p^{jf} - 1)$ or, if

$$u = \frac{p^\ell - 1}{k}$$

if and only if u divides $m(p^{jf} - 1)$. Let $u(j)$ be the greatest common divisor of u and $p^{jf} - 1$. u divides $m(p^{jf} - 1)$ if and only if $\frac{u}{u(j)}$ divides m. The number of such m with $0 \le m < p^\ell - 1$ is

$$\frac{u(j)}{u}\,(p^\ell - 1) = u(j)k.$$

Once m and j are chosen α is determined. The number of non-zero x in λ' which are fixed by some (β, ρ^{-j}) where j divides n but by no (β, ρ^{-i}) where i properly divides j is

$$\sum\nolimits_{i|j}\ \mu\left(\frac{j}{i}\right)\ u(i)k$$

if $\mu(\cdot)$ is the Möbius function. The number of orbits formed by such x is

$$\frac{1}{jk} \sum_{i|j} \mu\left(\frac{j}{i}\right) u(i)k$$

so that the total number of orbits of Γ in the multiplicative group of $\mathcal{X}'$ is

$$a = \sum_{i|n} \sum_{j\left|\frac{n}{i}\right.} \frac{\mu(j)}{ij} u(i)$$

which equals

$$\sum_{i|n} \prod_{\pi\left|\frac{n}{i}\right.} \left(1 - \frac{1}{\pi}\right) \frac{u(i)}{i}.$$

The product is over primes.

Lemma 14.7

If $\frac{p^\ell-1}{k}$ is odd then

$$(-1)^{a+1} \nu_{\phi'}(k)\ \nu_{\phi'}(-1)^{\frac{p^\ell-1}{2k}+\frac{1}{2}} = 1.$$

The identity of the lemma is equivalent to

$$(-1)^{a+1} \nu_{\phi'}(u)\ \nu_{\phi'}(-1)^{\frac{u-1}{2}} = 1$$

because

$$\nu_{\phi'}(k) = \nu_{\phi'}(-1)\ \nu_{\phi'}(u).$$

By the law of quadratic reciprocity the left side of the identity is equal to

$$(-1)^{a+1}\ (p^f|u)$$

if $(p^f|u)$ is Jacobi's symbol. If $u = 1$ there is only one orbit so

$$(-1)^{a+1} = 1.$$

Of course $(p^f|1) = 1$ so the identity is clear in this case.

We prove it in general by induction on the number of prime factors of u. Let π_0 be a prime factor of u and let $u = \pi_0^x v$ with v prime to π_0. Let $v(j)$ be the analogue of $u(j)$. Then $u(j) = \pi_0^{x(j)} v(j)$. Leb b be the analogue of a. Then

$$\nu = a - b = \sum_{i|n} \prod_{\pi\left|\frac{n}{i}\right.} \left(1 - \frac{1}{\pi}\right) \frac{v(i)}{i} (\pi_0^{x(i)} - 1).$$

Observe that π_0 and all $v(i)$ are odd. To prove the lemma by induction we must show that

$$(-1)^\nu\ (p^f \mid \pi_0^x) = 1. \tag{14.8}$$

Let

$$n = 2^y n_1$$

with n_1 odd. There are two possibilities to be considered.

(i)
$$\pi_0 \equiv 1 \pmod{2^{y+1}}.$$

Since the order of p^f modulo π_0 divides n the quotient of $\pi_0 - 1$ by this order is even and p^f is a quadratic residue of π_0. Also if i divides n

$$\frac{\pi_0^{x(i)} - 1}{i}$$

is divisible, in the 2-adic field, by 4 if 2 divides $\frac{n}{i}$ and is always divisible by 2. Thus ν is even and (14.8) is valid.

(ii)
$$\pi_0 = 1 + 2^c w$$

with $c \leq y$ and w odd. Let $i \neq n_1$ divide n_1 and consider

$$\sum\nolimits_{j=0}^{y} \prod\nolimits_{\pi \left| \frac{n}{2^j i}\right.} \left(1 - \frac{1}{\pi}\right) \; \frac{v(2^j i)}{2^j i} \; (\pi_0^{x(2^j i)} - 1). \tag{14.9}$$

If $x(2^y i) = 0$ the sum is zero. If $x(2^y i) \neq 0$ let z be the smallest integer for which $x(2^z i) \neq 0$. If $j < z$ then $x(2^j i) = 0$. If $j \geq z$

$$p^{2^j if} - 1 = \left(p^{2^z if} - 1\right) \left(\sum\nolimits_{d=0}^{2^{j-z}-1} \; p^{2^z cif}\right).$$

The residue of the sum modulo π_0 is 2^{j-z}. Thus

$$x(2^j i) = x(2^z i)$$

if $j \geq z$ and (14.9) is equal to

$$\frac{1}{i} \left\{\prod\nolimits_{\pi \left| \frac{n_1}{i}\right.} \left(1 - \frac{1}{\pi}\right)\right\} \left\{\frac{v(2^y i)}{2^y} + \sum\nolimits_{j=z}^{y-1} \; \frac{v(2^j i)}{2^{j+1}}\right\} \left(\pi_0^{x(2^y i)} - 1\right).$$

We write
$$\frac{v(2^y i)}{2^y} + \sum\nolimits_{j=z}^{y-1} \; \frac{v(2^j i)}{2^{j+1}}$$
as
$$\frac{v(2^z i)}{2^z} + \sum\nolimits_{j=z+1}^{y} \; \frac{v(2^j i) - v(2^{j-1} i)}{2^j}.$$

If k is replaced by $\frac{p^\ell - 1}{v}$ the number of elements of λ^* fixed by some $(\alpha, \rho^{-2^j i})$ but by no $(\alpha, \rho^{-2^{j-1} i})$ is
$$\{v(2^j i) - v(2^{j-1} i)\} \; \frac{p^\ell - 1}{v}.$$

The collection of such elements is invariant under the group obtained by replacing k by $\frac{p^\ell-1}{v}$ and ϕ' by the field with p^{if} elements. The isotropy group of each such point has a generator of the form $(\alpha, \rho^{-2^j i})$ and, therefore, has order $\frac{n}{2^j i}$ and index $\frac{2^j(p^\ell-1)}{v}$. Thus $\frac{2^j(p^\ell-1)}{v}$ divides

$$\{v(2^j i) - v(2^{j-1} i)\}\ \frac{p^\ell - 1}{v}$$

so that 2^j divides

$$v(2^j i) - v(2^{j-1} i).$$

Since $\frac{n_1}{i}$ is divisible by at least one prime, the expression (14.9) is congruent, in the 2-adic field, to

$$\frac{1}{i}\ \left\{\prod\nolimits_{\pi\left|\,\frac{n_1}{i}\right.} \left(1 - \frac{1}{\pi}\right)\right\}\ \frac{v(2^z i)}{2^z}\ \left(\pi^{x(2^y i)} - 1\right)$$

modulo 4. Since $z \le c$ and the product is not empty this is congruent, in the 2-adic field again, to 0 modulo 2. Thus ν is even or odd according as

$$\sum\nolimits_{j=0}^{y} \left\{\prod\nolimits_{\pi\left|\,2^{y-j}\right.} \left(1 - \frac{1}{\pi}\right)\right\}\ \frac{v(2^j n_1)}{2^j n_1}\ \left(\pi_0^{x(2^j n_1)} - 1\right)$$

is or is not divisible by 2 in the 2-adic field. Consequently

$$\nu \equiv \sum\nolimits_{j=0}^{y}\ \{\prod\nolimits_{\pi\,\left|\,2^{y-j}\right.} \left(1 - \frac{1}{\pi}\right)\right\}\ \frac{v(2^j n_1)}{2^j}\ (\pi_0^{x(2^j n_1)} - 1) \pmod 2.$$

Of course $x(2^y n_1) = x \ne 0$. Let z again be the smallest integer for $x(2^z n_1) \ne 0$. Then $z \le c$ and

$$x(2^j n_1) = x(2^z n_1)$$

if $j \ge z$. The sum above is equal to

$$\left\{\frac{v(2^z n_1)}{2^z} + \sum\nolimits_{j=z+1}^{y}\ \frac{v(2^j n_1) - v(2^{j-1} n_1)}{2^j}\right\}\quad (\pi_0^x - 1).$$

As before this is congruent modulo 2 to

$$\frac{v(2^z n_1)}{2^z}\quad (\pi_0^x - 1).$$

If $z < c$ this is even and the order of p modulo π_0 divides $\frac{\pi_0 - 1}{2}$ so that $(p|\pi_0) = 1$. If $z = c$ then

$$\frac{\pi_0^x - 1}{2^z} = \frac{1}{2^c}\ \sum\nolimits_{i=1}^{x} \binom{x}{i}\ (2^c w)^i \equiv x \pmod 2$$

so that $\nu \equiv x \pmod 2$. However the order of p^f modulo π_0 is divisible by 2^z so that it does not divide $\frac{\pi_0 - 1}{2}$ and

$$\left(p^f\ \mid\ \pi_0^x\right) = (-1)^x.$$

The relation (14.8) is now easily verified.

We return to the original problem. Since λ' is a quadratic extension of ϕ' and λ' is not contained in ϕ the degree of ϕ over ϕ' is odd. Since V and λ' have the same number of elements $q = p^\ell$. If $\frac{q-1}{k}$ is odd the relation (14.4) follows immediately from the equality

$$(-1)^{a+1}\,\nu_\phi(k)\,\nu_\phi(-1)^{\frac{q-1}{2k}+\frac{1}{2}} = (-1)^{a+1}\,\nu_{\phi'}(k)\,\nu_{\phi'}(-1)^{\frac{q-1}{2k}+\frac{1}{2}}$$

and the preceding lemma.

The number of μ in T with isotropy group of order 2 is $u(1)$ and the number of μ with trivial isotropy group is $\frac{u(2)-u(1)}{2}$. For points of the second type $[\phi_\mu : \phi] = 2$ and for points of the first type $[\phi_\mu : \phi] = 1$. Since, as we verified earlier,

$$\nu_\phi(\omega_1) = \nu_\phi\left(\prod\nolimits_\mu \gamma_\mu\right)$$

and

$$\nu_\phi(N_{\phi_\mu/\phi}\,\varepsilon_\mu) = \nu_\phi(-1)^{[\phi_\mu:\phi]}\,\nu_\phi(\gamma_\mu)$$

the identity (14.7) reduces to

$$u(1) \equiv 1 \pmod 2$$

which is true because $u(1)$ divides $u = \frac{p^\ell-1}{k}$ which, when (14.7) is under consideration, is odd by assumption.

The identity (14.5) may be formulated as

$$\nu_\phi\left(\prod\nolimits_\mu \gamma_\mu\right) = (-1)^a\,\nu_\phi(-1)^{\frac{q-1}{2k}}$$

and (14.6) as

$$\nu_\phi\left(\prod\nolimits_\mu \gamma_\mu\right)\;\nu_\phi(-1)^{\sum_\mu [\phi_\mu:\phi]} = (-1)^a\,\nu_\phi(-1)^{\frac{q-1}{2k}}.$$

For these two identities $\frac{q-1}{k}$ is even. Again

$$\sum [\phi_\mu : \phi] \equiv u(1) \pmod 2.$$

But

$$u(2) = u = \frac{p^\ell - 1}{k} = \frac{q-1}{k}$$

and

$$2a = u(1) + u(2)$$

so $u(1)$ is even. It will be enough to verify (14.5).

We may choose T so that if μ is in T then its isotropy group is trivial or contains one of σ_0 or σ_1. If σ_0 lies in the isotropy group of μ and ν in the orbit of μ corresponds to θ^m in λ' then

$$\alpha^2\theta^{m\rho} = \theta^m$$

for some kth root of unity α. This is possible if and only if $p^\ell - 1$ divides $\frac{km}{2}(p^f - 1)$ or $2u$ divides $m(p^f - 1)$. This is the same as requiring that $\frac{2u}{u(1)}$ divide $\frac{m(p^f-1)}{u(1)}$. The number u is even. We have already observed that if r is the number of elements in ϕ so that $x^{\sigma_0} = x^r$ for x in ϕ then

$$\mu_0 r \equiv 1 \pmod k$$

and in particular

$$\mu_0 r \equiv 1 \pmod 4.$$

Since $[\phi : \phi']$ is odd and $\mu_0 \equiv -1 \pmod 4$ the highest power of 2 dividing $p^f - 1$ is 2. Thus $\frac{2u}{u(1)}$ and $\frac{p^f-1}{u(1)}$ are relatively prime so that $\frac{2u}{u(1)}$ divides $\frac{m(p^f-1)}{u(1)}$ if and only if $\frac{2u}{u(1)}$ divides m. There are $\frac{u(1)k}{2}$ such m with $0 \le m < p^\ell - 1$. The corresponding characters ν fall into $\frac{u(1)}{2}$ orbits. Thus there are $\frac{u(1)}{2}$ elements in T whose isotropy group contains σ_0 and $\frac{u(1)}{2}$ whose isotropy group contains σ_1. Let L_0 be the fixed field of σ_0 and L_1 the fixed field of σ_1. Let ϖ_{L_0} and ϖ_{L_1} generate $\mathfrak{P}_{L_0}$ and $\mathfrak{P}_{L_1}$ respectively and let

$$\begin{aligned} N_{L_0/F}\varpi_{L_0} &= \gamma_0\, \varpi_F \\ N_{L_1/F}\varpi_{L_1} &= \gamma_1 \varpi_F \\ N_{L/F}\varpi_L &= \gamma \varpi_F^2. \end{aligned}$$

We have to show that

$$\nu_\phi\left(\gamma_0^{\frac{u(1)}{2}}\ \gamma_1^{\frac{u(1)}{2}}\ \gamma^{\frac{u(2)-u(1)}{2}}\right) = (-1)^a\, \nu_\phi(-1)^{\frac{q-1}{2k}}.$$

First we prove a lemma, special cases of which we have already seen.

Lemma 14.8

Suppose L/F is normal but non-abelian and $[L : F]$ is a power of 2. Suppose $H = \mathfrak{G}(L/F)$ and the first ramification group H_1 is $\{1\}$ but $[H : H_0] > 1$ and $[H_0 : H_1] > 1$. Let ϖ_L generate the prime ideal of O_L, let ϖ_F generate the prime ideal of O_F, and let

$$N_{L/F}\, \varpi_L = \gamma \varpi_F^{[H:H_0]}.$$

Then γ is a square in U_F.

The hypotheses imply that the residue field has odd characteristic. Let A be the fixed field of H_0 and L' be the fixed field of the commutator subgroup of H. Then $A \subseteq L'$ and if

$$\varpi_{L'} = N_{L/L'}\varpi_L$$

then

$$N_{L'/F}\varpi_{L'} = \gamma \varpi_F^{[A:F]}.$$

Of course $[A : F] = [H : H_0]$. Since H is nilpotent but not abelian L' cannot be a cyclic extension. If γ is not a square in U_F then γ^{-1} generates $U_F/U_F \cap N_{L'/F}C_L$. Since

$$\varpi_F^{[A:F]} \equiv \gamma^{-1} \pmod{N_{L'/F}C_{L'}}.$$

ϖ_F would then generate $C_F/N_{L'/F}C_{L'}$ which is impossible.

Returning to the problem at hand, we observe that the quotient of G/G_1 by the squares in G_0/G_1 is a group of order 4 in which every square is 1. The fixed field F' of this group is the composite of all quadratic extensions of F. $F_0 = F' \cap L_0$ and $F_1 = F' \cap L_1$ are the two different ramified quadratic extensions of F. Define

$$\varpi_{F_0} = N_{L_0/F_0}\varpi_{L_0}$$

and

$$\varpi_{F_1} = N_{L_1/F_1}\varpi_{L_1}.$$

Then

$$N_{F_0/F}\varpi_{F_0} = \gamma_0\varpi_F$$

and

$$N_{F_1/F}\varpi_{F_1} = \gamma_1\varpi_F.$$

We need to show that

$$\nu_\phi(\gamma_0\gamma_1) = \nu_\phi\left(\frac{\gamma_0}{\gamma_1}\right) = -1.$$

If not, $\frac{\gamma_0}{\gamma_1}$ is a square and thus in $N_{F_1/F}C_{F_1}$. Then $\gamma_0\varpi_F$ belongs to

$$N_{F_0/F}C_{F_0} \cap N_{F_1/F}C_{F_1} = N_{F'/F}C_{F'}.$$

This is impossible because F' contains an unramified extension.

We observed before that since

$$\mu_0 = \lambda(\sigma_0) \equiv -1 \pmod 4$$

the number $\nu_\phi(-1)$ is -1. The identity (14.5) reduces to

$$(-1)^{\frac{u(1)}{2}} = (-1)^a\,(-1)^{\frac{q-1}{2k}}.$$

Since

$$a = \frac{u(1)}{2} + \frac{u(2)}{2}$$

and

$$u(2) = \frac{q-1}{k}$$

this relation is clearly valid.

We continue to suppose that $\mu_0 \equiv -1 \pmod k$ and that $\sigma_0^2 = 1$ but now we suppose that V is not invariant under $\pi^*(\sigma_0)$. Since $\pi^*(\sigma_0)V \cap V$ and $\pi^*(\sigma_0)V + V$ are both invariant under G/G_1 the first is 0 and the second is $S(K/L)$ so that $S(K/L)$ is the direct sum $V \oplus \pi^*(\sigma_0)V$. Let V have p^ℓ elements so that $q = p^{2\ell}$. If λ' is again the field generated over the prime field by the kth roots of unity λ' has p^ℓ elements. If $\phi' = \lambda' \cap \phi$ has p^f elements then $p^\ell = p^{2f}$ so that $p^\ell \equiv 1 \pmod 8$. Also k divides $p^\ell - 1$ so that

$$\frac{q-1}{k} = \left(\frac{p^\ell - 1}{k}\right)\,(p^\ell + 1)$$

is even.

If $\sigma \in G_0/G_1$ the non-zero fixed points of $\sigma_0\sigma$ are the elements of the form

$$v \oplus \pi^*(\sigma_0\sigma)v$$

with $v \neq 0$. There are $(p^\ell - 1)k$ of them altogether and they fall into $p^\ell - 1$ orbits. The remaining

$$(p^{2\ell} - 1) - (p^\ell - 1)k$$

elements fall into

$$\frac{1}{2k}\,\{(p^{2\ell} - 1) - (p^\ell - 1)k\}$$

orbits. Thus

$$a = \frac{p^\ell - 1}{2} + \frac{p^{2\ell} - 1}{2k}.$$

Since, for the same reasons as before, $\nu_\phi(-1) = -1$ the identity (14.5) becomes

$$\nu_\phi\left(\prod\nolimits_\mu \gamma_\mu\right) = (-1)^{\frac{p^\ell - 1}{2}} \tag{14.10}$$

while (14.6) becomes

$$\nu_\phi\left(\prod\nolimits_\mu \gamma_\mu\right)\ \nu_\phi(-1)^{\Sigma[\phi_\mu:\phi]} = (-1)^{\frac{p^\ell - 1}{2}}.$$

Since

$$\sum\,[\phi_\mu : \phi] \equiv p^\ell - 1 \equiv 0 \pmod 2$$

only (14.5) need be proved. (14.4) and (14.7) are not to be considered because $\frac{q-1}{k}$ is even.

We proceed as before. The points in T can be chosen so that their isotropy groups are either trivial or contain σ_0 or σ_1. $\frac{p^\ell - 1}{2}$ will have isotropy groups containing σ_0 and $\frac{p^\ell - 1}{2}$ will have isotropy groups containing σ_1. The argument used above shows that the left side of (14.10) is equal to

$$(-1)^{\frac{p^\ell - 1}{2}}$$

as desired.

Now suppose $k \geq 8$ and

$$\mu_0 = \lambda(\sigma_0) \equiv \frac{k}{2} - 1 \pmod k.$$

We are of course still supposing that $[G : G_0] = 2$. If σ belongs to G_0/G_1 then

$$\sigma\sigma_0\sigma^{-1} = \sigma_0\sigma^{\frac{k}{2} - 2}$$

and

$$(\sigma_0\sigma)^2 = \sigma_0^2\sigma^{\frac{k}{2}}.$$

Thus

$$x((\sigma_0\sigma)^2) = x(\sigma_0^2) + \frac{k}{2}\,x(\sigma).$$

Since $x(\sigma_0^2)$ is 0 or $\frac{k}{2}$, we can make the sum on the right 0. Replacing σ_0 by $\sigma_0\sigma$ if necessary, we suppose that $\sigma_0^2 = 1$. Then $(\sigma_0\sigma)^2 = 1$ if and only if

$$\frac{k}{2}\, x(\sigma) \equiv 0 \pmod k$$

which is so if and only if $\sigma_0\sigma$ is conjugate to σ.

Take V in $S(K/L)$ as before. If V is invariant under $\pi^*(\sigma_0)$ and λ' with p^ℓ elements and ϕ' with p^f elements have the same meaning as before then

$$p^f = \frac{k}{2} - 1 + wk$$

for some integer w so that

$$q - 1 = p^{2f} - 1 = k \cdot \frac{k}{4} - k + 2wk\left(\frac{k}{2} - 1\right) + (wk)^2$$

and

$$\frac{q-1}{k} \equiv \frac{k}{4} - 1 \pmod 2$$

is odd. Thus the identities (14.5) and (14.6) are not to be considered. The identities (14.4) and (14.7) follow from Lemma 14.7 exactly as above.

Suppose then $S(K/L)$ is the direct sum $V \oplus \pi^*(\sigma_0)V$. If V has p^ℓ elements then $q = p^{2\ell}$ and

$$\frac{q-1}{k} = \frac{p^\ell - 1}{k}\,(p^\ell + 1)$$

is even because k divides $p^\ell - 1$. The non-zero elements of $S(K/L)$ which are fixed points of some $\sigma_0\sigma$ with σ a square in G_0/G_1 are the elements

$$v \oplus \pi^*(\sigma_0\sigma)v$$

with $v \neq 0$. There are $(p^\ell - 1)\,\frac{k}{2}$ such elements and they fall into $\frac{p^\ell-1}{2}$ orbits. The remaining

$$(p^{2\ell} - 1) - (p^\ell - 1)\,\frac{k}{2}$$

non-zero elements have trivial isotropy group and fall into

$$\frac{1}{2k}\,\left\{(p^{2\ell} - 1) - (p^\ell - 1)\,\frac{k}{2}\right\}$$

orbits. Thus

$$a = \frac{p^{2\ell} - 1}{2k} + \frac{p^\ell - 1}{4}.$$

Since, as before, $\nu_\phi(-1) = -1$ the identity (14.5) becomes

$$\nu_\phi\left(\prod\nolimits_\mu \gamma_\mu\right) = (-1)^{\frac{p^\ell-1}{4}} \tag{14.11}$$

while (14.6) becomes
$$\nu_\phi\left(\prod\nolimits_\mu \gamma_\mu\right)\,(-1)^{\Sigma[\phi_\mu:\phi]}=(-1)^{\frac{p^\ell-1}{4}}.$$
Again
$$\sum\,[\phi_\mu:\phi]\equiv\frac{p^\ell-1}{2}\equiv 0\pmod 2$$
so that it is enough to prove (14.11). The identities (14.4) and (14.7) need not be considered.

If λ' and ϕ' are defined as before and ϕ' has p^f elements then λ' has $p^\ell=p^{2f}$ elements so that

$$p^\ell\equiv 1\pmod 8$$

and $\frac{p^\ell-1}{4}$ is even. We may suppose that each μ in T either has trivial isotropy group or is fixed by σ_0. Lemma 14.8 shows that those μ with trivial isotropy group contribute nothing to the left side of (14.11). If L_0 is the fixed field of σ_0 and
$$N_{L_0/F}\varpi_{L_0}=\gamma_0\varpi_F$$
the left side of K is
$$\nu_\phi(\gamma_0)^{\frac{p^\ell-1}{2}}$$
which is 1. The truth of the identity is now clear.

We return to the general case so that $[G:G_0]$ may be greater than 2 and μ_0 may be congruent to 1 modulo 4. Of course $[G:G_0]$ is still even. Let

$$\lambda_0=\lambda\left(\sigma_0^{\frac{1}{2}\,[G:G_0]}\right)$$

so that
$$\lambda_0=\mu_0^{\frac{1}{2}\,[G:G_0]}.$$
If $[G:G_0]>2$ then
$$\lambda_0\equiv 1\pmod 4.$$
If $[G:G_0]=2$ then $\lambda_0=\mu_0$. Since the case that $[G:G_0]=2$ and $\mu_0\equiv -1\pmod 4$ is completely settled we may suppose that $\lambda_0\equiv 1\pmod 4$. Set

$$\tau_0=\sigma_0^{\frac{1}{2}\,[G:G_0]}.$$

Any element of G/G_1 which does not lie in G_0/G_1 and whose square is 1 is of the form $\sigma(x)\tau_0$. If

$$\sigma_0^{[G:G_0]}=\sigma(y_0)$$

then
$$(\sigma(x)\tau_0)^2=\sigma((\lambda_0+1)x)\tau_0^2=\sigma(y_0+(\lambda_0+1)x).$$
Since G/G_1 is not cyclic y_0 is even. Since

$$\lambda_0+1\equiv 2\pmod 4$$

there are exactly two solutions of the equation

$$y_0 + (\lambda_0 + 1)x \equiv 0 \pmod{k}.$$

Let x_0 be one of them. Then $x_0 + \frac{k}{2}$ is the other. We may suppose that k does not divide x_0. Set

$$\rho_0 = \sigma(x_0)\tau_0.$$

We observed before that if $\sigma \neq 1$ belongs to G/G_1 and $\pi^*(\sigma)$ has a non-zero fixed point then some power of σ is of order 2 and has a non-zero fixed point. Since $\sigma\left(\frac{k}{2}\right)$ has no non-zero fixed point this power must be ρ_0 or $\sigma\big(\frac{k}{2}\big)\rho_0$. Since $\sigma\big(\frac{k}{2}\big)$ lies in the center of G/G_1, σ must lie in the centralizer of ρ_0.

The group

$$\left\{1, \sigma\left(\frac{k}{2}\right), \rho_0, \sigma\left(\frac{k}{2}\right)\rho_0\right\}$$

is of order 4 and every element in it is of order 2 so it cannot be contained in the center of G/G_1. However it is a normal subgroup and its centralizer H^* has index 2 in G/G_1. G/G_1 may be identified with H. Every element σ of H such that $\pi^*(\sigma)$ has a non-zero fixed point lies in H^*. $S(K/L)$ is the direct sum of V and W where

$$V = \{v \mid \pi^*(\rho_0)v = v\}$$
$$W = \{w \mid \pi^*(\rho_0)w = -w\}.$$

If σ in H does not belong to H^* then $\pi^*(\sigma)V = W$ and $\pi^*(\sigma)W = V$. The number of non-zero orbits of H in $V \cup W$ is the same as the number a' of non-zero orbits of H^* in V. If V has p^ℓ elements so that $q = p^{2\ell}$ the number of non-zero orbits of H in $V \oplus W - (V \cup W)$ is

$$a'' = \frac{(p^\ell - 1)^2}{[G : G_1]} = \frac{p^\ell - 1}{k} \cdot \frac{p^\ell - 1}{[G : G_0]}.$$

The action of H^* on V must be irreducible although it is not faithful. However the action of $H^* \cap H_0 = H_0^*$ is faithful.

Let F' be the fixed field of H^* in L or, what is the same, of H^*C in K. Let $C^1 \subseteq C$ be the orthogonal complement of V and let H^1 be the subgroup of H which acts trivially on V. H^1C^1 is a normal subgroup of H^*C and its fixed field K' is normal over F'. If $H' = H^*/H^1$ and $C' = C/C^1$ then $G' = \mathfrak{G}(K'/F') = H'C'$. Moreover $H' \cap C' = \{1\}$ and $H' \neq \{1\}$ because $\sigma\left(\frac{k}{2}\right)$ does not lie in H^1. Since the action of H' on C' is faithful and irreducible C' is contained in every non-trivial normal subgroup of G'. To complete the proof of the four identities (14.4), (14.5), (14.6), and (14.7) we use induction on $[K : F]$.

Let k' be the order of H_0' and let $\phi' = O_{F'}/\mathfrak{P}_{F'}$. If K/F is replaced by K'/F' the identity (14.4) becomes

$$(-1)^{a'+1}\,\nu_{\phi'}(k')\,\nu_{\phi'}(-1)^{\frac{p^\ell-1}{2k'}+\frac{1}{2}} = 1. \tag{14.4$''$}$$

T is to be replaced by T', a set of representatives for the non-zero orbits of H' or H^* in V, which may be identified with the character group of C'. We may suppose that T' is a subset of T. Because $H_0' \neq \{1\}$ the identity (14.5) for the field K'/F' may be written as

$$\nu_{\phi'}\left(\prod\nolimits_{\mu \in T'} \gamma'_\mu\right) = (-1)^{a'}\,\nu_{\phi'}(-1)^{\frac{p^\ell-1}{2k'}}. \tag{14.5$''$}$$

Of course
$$N_{F_\mu/F'}(\varpi_{F_\mu}^t) = \gamma'_\mu \varpi_{F'}^{\frac{t[F_\mu:F']}{k'}}.$$
Recall that t is odd. By Proposition IV.3 of Serre's book, t has the same significance for K'/F' as it had for K/F. The identity (14.6) may be written as
$$(-1)^{a'}\,\nu_{\phi'}\,\left(\prod\nolimits_{\mu\in T'}\gamma'_\mu\right)\,\nu_{\phi'}(-1)^{\Sigma_{\mu\in T'}[\phi_\mu:\phi']}\,\nu_{\phi'}(-1)^{\frac{p^\ell-1}{2k'}} = 1. \tag{14.6$''$}$$
and (14.7) as
$$(-1)^{a'+1}\,\nu_{\phi'}(k')\,\nu_{\phi'}(-1)^{\frac{p^\ell-1}{2k'}-\frac{1}{2}}\,\nu_{\phi'}(-1)^{\Sigma_{\mu\in T'}\,[\phi_\mu:\phi']} = 1 \tag{14.7$''$}$$
Assuming (14.4$''$), (14.5$''$), (14.6$''$), and (14.7$''$) we are going to prove (14.4), (14.5), (14.6), and (14.7).

Since H'_0 is isomorphic to H_0^* either $k' = k$ or $k' = \frac{k}{2}$. Suppose first that $\frac{q-1}{k}$ is odd. Then $k' = \frac{k}{2}$ for if not
$$\frac{q-1}{k} = \left(\frac{p^\ell-1}{k}\right)\,(p^\ell+1)$$
would be even. Thus $H_0 = G_0/G_1$ is not contained in H^* and F'/F is ramified so that $\phi' = \phi$. Since
$$\frac{q-1}{k} = \left(\frac{p^\ell-1}{k'}\right)\,\frac{(p^\ell+1)}{2}$$
the number $\frac{p^\ell-1}{k'}$ is odd. To prove (14.4) we have to show that
$$(-1)^{a''}\,\nu_\phi(2)\,\nu_\phi(-1)^\delta = 1$$
if
$$\delta = \frac{p^{2\ell}-1}{2k} - \frac{p^\ell-1}{k} = \frac{p^\ell-1}{k}\,\left\{\frac{p^\ell+1}{2}-1\right\}.$$
Since G_0/G_1 is not contained in H^*, τ_0 does not commute with G_0/G_1 and the map λ of G/G_0 into the units of $\mathbb{Z}/k\,\mathbb{Z}$ is faithful. Thus
$$\lambda_0 \not\equiv 1 \pmod{k}.$$
But
$$\lambda_0 \equiv 1 \pmod 4$$
so that $k \geq 8$. In general if $k \geq 4$, the group of units of $\mathbb{Z}/k\,\mathbb{Z}$ is the product of $\{1,-1\}$ and
$$\{\alpha \mid \alpha \equiv 1 \pmod 4\}.$$
If
$$\alpha = 1 + 2^b x$$
with x odd and $4 \leq 2^b \leq k$ then
$$\alpha^2 = 1 + 2^{b+1} y$$
with y odd. One shows easily by induction that the order of α is $2^{-b}k$ so that
$$\{\alpha \mid \alpha \equiv 1 \pmod 4\}$$

is cyclic of order $\frac{k}{4}$. This implies in the particular case under consideration that $[G:G_0]$ divides $\frac{k}{4}$. Write

$$a'' = \left(\frac{p^\ell - 1}{k'}\right)\left(\frac{p^\ell - 1}{2[G:G_0]}\right).$$

a'' is odd if and only if

$$2[G:G_0] = k'.$$

We consider various cases separately. As before $\mu_0 = \lambda(\sigma_0)$. If ϕ has p^f elements then

$$\mu_0 p^f \equiv 1 \pmod 8$$

(i)

$$\mu_0 \equiv 1 \pmod 8.$$

Then

$$\nu_\phi(2) = \nu_\phi(-1) = 1$$

and the order of μ_0 in the units of $\mathbb{Z}/k\,\mathbb{Z}$ which is equal to $[G:G_0]$ divides $\frac{k}{8}$. Thus a'' is even. The identity (14.4) follows.

(ii)

$$\mu_0 \equiv 3 \pmod 8.$$

Then

$$\nu_\phi(2) = \nu_\phi(-1) = -1.$$

Since $\mu_0 \equiv 3 \pmod 8$ the numbers μ_0 and λ_0 are different. Thus λ_0 is a square and hence congruent to 1 modulo 8. Then $k > 8$ and

$$p^\ell \equiv 1 \pmod 8.$$

Then

$$\delta \equiv \frac{p^\ell + 1}{4} - \frac{1}{2} \equiv 0 \pmod 2.$$

Since $\mu_0 \neq \lambda_0$ the index $[G:G_0]$ is not 2. Thus the order of μ_0 is at least 4 and is therefore the order of $-\mu_0$. Since $-\mu_0 \equiv 5 \pmod 8$ its order is $\frac{k}{4}$ and

$$[G:G_0] = \frac{k}{4}.$$

Consequently a'' is odd. Again (14.4) is satisfied.

(iii)

$$\mu_0 \equiv 5 \pmod 8.$$

Then $\nu_\phi(2) = -1$ while $\nu_\phi(-1) = 1$. The order of μ_0 which equals $[G:G_0]$ is again $\frac{k}{4}$ so that a'' is odd and (14.4) is satisfied.

(iv)

$$\mu_0 \equiv 7 \pmod 8.$$

Then $\nu_\phi(2) = 1$ while $\nu_\phi(-1) = -1$. Again $k > 8$ and

$$\delta \equiv 0 \pmod 2.$$

The order of μ_0 is again at least 4 and therefore equal to the order of $-\mu_0$ and that divides $\frac{k}{8}$. Thus $[G : G_0]$ divides $\frac{k}{8}$ and a'' is even. (14.4) follows once more.

Since $\phi' = \phi$ all we need to prove (14.7) once (14.4) and (14.7$''$) are granted is show that

$$\sum\nolimits_{\mu \in T - T'} [\phi_\mu : \phi] \equiv 0 \pmod 2.$$

This is clear because, for these μ, $F_\mu = L$ and $\phi_\mu = O_L/\mathfrak{P}_L$ is of even degree over ϕ.

Finally we have to assume that $\frac{q-1}{k}$ is even and prove (14.5) and (14.6). First a lemma.

Lemma 14.9

If $\frac{q-1}{k}$ is even,

$$\lambda\left(\sigma_0^{\frac{1}{2}[G:G_0]}\right) \equiv 1 \pmod 4,$$

and G/G_0 acts faithfully on G_0/G_1, then

$$(-1)^a\, \nu_\phi(-1)^{\frac{q-1}{2k}} = 1.$$

Since the action is faithful G_0/G_1 is not contained in H^* and $k' = \frac{k}{2}$. As before $\lambda_0 \equiv 1 \pmod 4$ and $\lambda_0 \not\equiv 1 \pmod k$ together imply that $k \geq 8$ and $k' \geq 4$. Since k' divides $p^\ell - 1$,

$$p^\ell \equiv 1 \pmod 4$$

and $\frac{p^\ell+1}{2}$ is odd. Since

$$\frac{q-1}{k} = \left(\frac{p^\ell - 1}{k'}\right)\left(\frac{p^\ell + 1}{2}\right)$$

the number $\frac{p^\ell-1}{k'}$ is even.

If σ belongs to H^* and σ acts trivially on H_0^* then

$$\lambda(\sigma) \equiv 1 \left(\mathrm{mod}\, \frac{k}{2}\right)$$

so that

$$\lambda(\sigma^2) \equiv 1 (\mathrm{mod}\, k)$$

and σ^2 belongs to H_0. Thus σ belongs to $\rho_0 H_0 \cup H_0$. Since ρ_0 belongs to H^1 the image of σ in H' lies in H_0'. Thus G'/G_0' acts faithfully on G_0'/G_1'. If σ belongs to H^1 then σ acts trivially on H_0^* because the representation of H_0^* on V is faithful. Thus H^1 is contained in $\rho_0\, H_0 \cup H_0$ and is therefore just $\{\rho_0, 1\}$. Thus

$$[G' : G_0'] = [H' : H_0'] = [H^* : H_0^* H^1] = \frac{1}{2}\,[G : G_0].$$

Suppose that

$$(-1)^a\,\nu_{\phi'}(-1)^{\frac{p^\ell-1}{2k'}}=1. \tag{14.12}$$

Since $\phi'=\phi$ and, because $k'\geq 4$ divides $p^\ell-1$,

$$\frac{q-1}{2k}=\left(\frac{p^\ell-1}{2k'}\right)\left(\frac{p^\ell+1}{2}\right)\equiv\left(\frac{p^\ell-1}{2k'}\right)\pmod 2,$$

all we need do to establish the lemma is to show that

$$a''\equiv 0\pmod 2.$$

As before $[G:G_0]$ divides $\frac{k}{4}$. If

$$\frac{k}{4}=n[G:G_0]$$

then

$$a''=\frac{1}{k}\;\;\frac{(p^\ell-1)^2}{[G:G_0]}=n\left(\frac{p^\ell-1}{k'}\right)^2$$

is certainly even because $2k'$ divides $p^\ell-1$.

If $[G:G_0]\geq 4$ let

$$\lambda_0'=\lambda\left(\sigma_0^{\frac{1}{4}\,[G:G_0]}\right).$$

If

$$\lambda_0'\equiv 1\pmod 4$$

we may suppose that (14.12) is true by induction. If $[G:G_0]=4$ and

$$\lambda_0'\equiv 3\pmod 4$$

or if $[G:G_0]=2$ we must establish it directly.

Suppose first that $[G:G_0]=2$. If ϕ has p^f elements then

$$\lambda_0\equiv\mu_0\equiv p^f\equiv 1\pmod 4$$

so that $\nu_\phi(-1)=1$. It is clear that in this case

$$a'=\frac{p^\ell-1}{k'}.$$

a' is thus even and (14.12) is valid.

Now suppose $[G:G_0]=4$ so that $[G':G_0']=2$. If σ_0' generates G' modulo G_0' then λ_0' is the image of σ_0' in the group of units of $\mathbb{Z}/k'\,\mathbb{Z}$. We have already studied the case that $\lambda_0'\equiv 3\pmod 4$ intensively. Let

$$x:\sigma'\longrightarrow x(\sigma')$$

be the map of G_0'/G_1' onto $\mathbb{Z}/k'\,\mathbb{Z}$. If $\lambda_0' \equiv -1 \pmod{k'}$ and $x((\sigma_0')^2) = \frac{k'}{2}$ we showed, incidentally, that (14.12) is valid. If $\lambda_0' \equiv -1 \pmod{k'}$, $x((\sigma_0')^2) = 0$, and the action of H_0' on $S(K'/L')$ is reducible we saw that p^ℓ is a square $p^{2\ell'}$ and that the left side of (L) is

$$(-1)^{\frac{p^{\ell'}-1}{2}}.$$

But the field with $p^{\ell'}$ elements must contains the k'th roots of unity and $k' \equiv 0 \pmod 4$. Thus

$$p^{\ell'} - 1 \equiv 0 \pmod 4$$

and (14.12) is again valid. If $k' \geq 8$,

$$\lambda_0' \equiv \frac{k'}{2} - 1 \pmod{k'}$$

and the action of H_0' on $S(K'/L')$ is reducible, the left side of (14.12) is

$$(-1)^{\frac{p^{\ell'}-1}{4}}.$$

This time

$$p^{\ell'} - 1 \equiv 0 \pmod 8.$$

To complete the proof of the lemma we show that in the case under consideration the action of H_0' and $S(K'/L')$ or, what is the same, the action of H_0^* on V is reducible. If not the field generated over the prime field by the k'th roots of unity has p^ℓ elements. Thus

$$p^\ell \equiv 1 \pmod 4.$$

However as we have observed repeatedly, the number of elements in ϕ is congruent to 3 modulo 4. Thus ℓ is even. Let $\ell = 2\ell'$. Either $p^{\ell'} - 1$ or $p^{\ell'} + 1$ is congruent to 2 modulo 4. If $p^{\ell'} + 1 \equiv 2 \pmod 4$ then k' divides $p^{\ell'} - 1$ because

$$\frac{p^\ell - 1}{k'} = \left(\frac{p^{\ell'} - 1}{k'}\right)(p^{\ell'} + 1)$$

is even. Since k' cannot divide $p^{\ell'} - 1$ we have

$$p^{\ell'} \equiv 3 \pmod 4$$

and ℓ' is odd. Indeed it is 1 but that does not matter. Since k divides $p^\ell - 1$, the kth roots of unity are contained in the field with p^ℓ elements. Adjoining them to $\phi = O_F/\mathfrak{P}_F$ we obtain a quadratic extension because 4 does not divide ℓ. Therefore if σ belongs to G_0/G_1

$$\theta_0(\sigma) = \theta_0(\sigma)^{\sigma_0^{-2}} = \theta_0(\sigma)^{\lambda(\sigma_0^2)}$$

so that

$$\lambda(\sigma_0^2) \equiv 1 \pmod k.$$

This contradicts the assumption that G/G_0 acts faithfully on G_0/G_1.

Returning to the proof of (14.5), we suppose first that H_0 is not contained in H^* so that the action of G/G_0 on G_0/G_1 is faithful. Because of Lemma 14.9 the identity (14.5) is equivalent to

$$\nu_\phi\left(\prod\nolimits_{\mu\in T} N_{F_\mu/F}\,\gamma_\mu\right) = 1.$$

If μ belongs to T but not to T' then $F_\mu = L$ and, by Lemma 14.8,

$$\nu_\phi(N_{F_\mu/F}\,\gamma_\mu) = 1.$$

If μ belongs to T' then G_μ is contained in H^*C so that F_μ contains F'. Moreover we do not change F_μ if we replace K/F by K'/F'. Let $\varpi_{F'}$ generate $\mathfrak{P}_{F'}$ and take $\varpi_F = N_{F'/F}\varpi_{F'}$. If E' is the fixed-field of H^* we may suppose that

$$\varpi_{F'} = N_{E'/F'}\varpi_{E'}$$

and that

$$\varpi_E = N_{E'/E}\varpi_{E'}.$$

Then

$$\varpi_F = N_{E/F}\varpi_E$$

as required. Let

$$N_{F_\mu/F}, \varpi^t_{F_\mu} = \gamma'_\mu \varpi^{\frac{t[F_\mu:F']}{k'}}.$$

Then

$$\gamma_\mu = N_{F'/F}\,\gamma'_\mu.$$

Since F'/F is ramified γ_μ is a square in U_F and (14.5) is proved. To prove (14.6) we have to show that

$$\nu_\phi(-1)^{\Sigma_{\mu\in T}[\phi_\mu:\phi]} = \nu_{\phi'}(-1)^{\Sigma_{\mu\in T'}[\phi_\mu:\phi']} = 1.$$

But $\frac{p^\ell-1}{k'}$ is even and this follows from the simultaneous validity of (14.5$''$) and (14.6$''$).

We have yet to treat the case that $\frac{q-1}{k}$ is even and H_0 is contained in H^*. Then F'/F is unramified and $k'=k$. Suppose first of all that $\frac{p^\ell-1}{k}$ is also even. Then

$$\frac{q-1}{2k} = \left(\frac{p^\ell-1}{k}\right)\ \left(\frac{p^\ell+1}{2}\right)$$

is even. H_0 is contained in H^* and H is generated by σ_0 and H_0. Consequently σ_0 is not contained in H^* and

$$\sigma_0\rho_0\sigma_0^{-1} = \sigma\ \left(\frac{k}{2}\right)\ \rho_0.$$

Since $\rho_0 = \sigma(x_0)\tau_0$

$$(\mu_0-1)x_0 \equiv \frac{k}{2} \pmod{k}$$

if $\mu_0 = \lambda(\sigma_0)$. If

$$y_0 = x\left(\sigma_0^{[G:G_0]}\right)$$

and m is the greatest common divisor of y_0 and k then by the definition of x_0 the greatest common divisor of x_0 and k is $\frac{m}{2}$. Therefore $\frac{k}{m}$ is the greatest common divisor of $\mu_0 - 1$ and k. In particular $m < k$. The order of σ_0 in H is

$$\frac{k}{m}\,[G : G_0].$$

Therefore $[G : G_0]$ divides $\frac{k}{2m}\,[G : G_0]$ and H^* contains a cyclic subgroup of order

$$\frac{k}{2m}\,[G : G_0].$$

If σ is the element of order 2 in this subgroup, then σ belongs to H_0 and $\pi^*(\sigma)$ does not have 1 as an eigenvalue. Thus no non-zero element of V is fixed by any element of this cyclic subgroup and

$$p^\ell - 1 \equiv 0 \left(\mathrm{mod}\,\frac{k}{2m}\;[G : G_0]\right).$$

In particular $[G : G_0]$ divides $p^\ell - 1$ and

$$a'' = \left(\frac{p^\ell - 1}{k}\right)\left(\frac{p^\ell - 1}{[G : G_0]}\right)$$

is even. As before $\nu_\phi(\gamma_\mu) = 1$ if μ belongs to T and $F_\mu = L$. If $F_\mu \neq L$ then μ belongs to T' and G_μ lies in H^*C so that F_μ contains F'. In the present situation F'/F is unramified and we may take $\varpi_{F'} = \varpi_F$. If

$$N_{F_\mu/F'}\varpi_{F_\mu}^t = \gamma'_\mu \varpi_F^{\frac{t[F_\mu:F']}{k}}$$

then

$$N_{F_\mu/F}\varpi_{F_\mu}^t = (N_{F'/F}\,\gamma'_\mu)\,\varpi_F^{\frac{t[F_\mu:F]}{k}}.$$

The identity (14.5) reduces to

$$\nu_\phi\left(\prod\nolimits_{\mu\in T'} N_{F'/F}\,\gamma'_\mu\right) = (-1)^{a'}$$

or

$$\nu_{\phi'}\left(\prod\nolimits_{\mu\in T'} \gamma'_\mu\right) = (-1)^{a'}.$$

Since ϕ' is a quadratic extension of ϕ the number $\nu_{\phi'}(-1)$ is 1 and this relation is equivalent to (14.5″). To prove (14.6) we have to show that

$$\nu_\phi(-1)^{\Sigma_{\mu\in T}\,[\phi_\mu:\phi]} = 1.$$

This is clear because 2 divides each of the degrees $[\phi_\mu : \phi]$.

Finally we have to suppose that $\frac{p^\ell-1}{k}$ is odd. Since $[\phi' : \phi] = 2$ the relation (14.4″) amounts to

$$(-1)^{a'+1} = 1.$$

Again

$$\nu_\phi\left(\prod\nolimits_{\mu\in T} \gamma_\mu\right) = \nu_{\phi'}\left(\prod\nolimits_{\mu\in T'} \gamma'_\mu\right). \tag{14.13}$$

If μ belongs to T' and $\sigma \neq 1$ belongs to G_μ then some power of σ will equal ρ_0. Since

$$\frac{p^\ell - 1}{k} = \sum\nolimits_{\mu \in T'} \frac{[F_\mu : F']}{k}$$

is odd and

$$\frac{[F_\mu : F']}{k}$$

is a power of 2 there is at least one μ in T' for which $[F_\mu : F'] = k$. Then G_μ must contain an element of the form $\sigma(z_0)\sigma_0^2$. Then

$$\rho_0 = \sigma(x_0)\tau_0 = (\sigma(z_0)\sigma_0^2)^{\frac{1}{4}\,[G:G_0]} = \sigma\left(\left(\frac{\mu_0^{\frac{1}{2}\,[G:G_0]} - 1}{\mu_0^2 - 1}\right)^{z_0}\right)^{\tau_0}.$$

Thus

$$\left(\frac{\mu_0^{\frac{1}{2}\,[G:G_0]} - 1}{\mu_0^2 - 1}\right) z_0 \equiv x_0 \pmod{k}.$$

Let

$$\frac{1}{4}\,[G : G_0] = 2^b.$$

Since

$$\mu_0^2 \equiv 1 \pmod{4}$$

and, as before, the greatest common divisor of x_0 and k is $\frac{m}{2}$ if the greatest common divisor of y_0 and k is m, we infer that

$$\frac{\mu_0^{\frac{1}{2}\,[G:G_0]} - 1}{\mu_0^2 - 1} = \prod\nolimits_{j=1}^{b} \cdot \frac{\mu_0^{2^{j+1}} - 1}{\mu_0^{2^j} - 1} = \prod\nolimits_{j=1}^{b} \mu_0^{2^j} + 1$$

is multiplicatively congruent to

$$\frac{[G : G_0]}{4}$$

modulo 2 and that the greatest common divisor of z_0 and k is

$$\frac{2m}{[G : G_0]}.$$

In particular $\frac{[G:G_0]}{2}$ divides m. z_0 is odd if and only if

$$m = \frac{1}{2}\,[G : G_0].$$

If $\mu_0 \equiv 1 \pmod{4}$ the order of μ_0 in the group of units of $\mathbb{Z}/k\,\mathbb{Z}$ is m because as we observed when treating the case that $\frac{p^\ell - 1}{k}$ is even, the greatest common divisor of $\mu_0 - 1$ and k is $\frac{k}{m}$. However

$$\mu_0^{\frac{1}{2}\,[G:G_0]} \equiv \lambda(\tau_0) \equiv 1 \pmod{k}$$

and in this case m divides $\frac{1}{2}[G:G_0]$. Thus

$$m = \frac{1}{2}[G:G_0]$$

if $\mu_0 \equiv 1 \pmod 4$.

We shall define a sequence of fields $F^{(i)},\ L^{(i)},\ K^{(i)},\ 1 \le i \le n$. n is an integer to be specified. We will have $F^{(i)} \subseteq L^{(i)} \subseteq K^{(i)}$ and $K^{(i)}/F^{(i)}$ and $L^{(i)}/F^{(i)}$ will be Galois. Let $G^{(i)} = \mathfrak{G}(K^{(i)}/F^{(i)})$ and $C^{(i)} = \mathfrak{G}(L^{(i)}/F^{(i)})$. There will be a subgroup $H^{(i)}$ of $G^{(i)}$ such that $H^{(i)} \neq \{1\},\ H^{(i)} \cap C^{(i)} = \{1\}$, and $G^{(i)} = H^{(i)}C^{(i)}$. $C^{(i)}$ will be a non-trivial abelian normal subgroup of $G^{(i)}$ which is contained in every other non-trivial normal subgroup. $H^{(n)}$ will be abelian but $H^{(i)}$ will be non-abelian if $i < n$. Moreover $k^{(i)} = [H_0^{(i)} : 1]$ will be at least 4 for all i and $k^{(i)}$ will equal $2k^{(i+1)}$ if $i < n$. If x is an isomorphism of $H_0^{(i)}$ with $\mathbb{Z}/k^{(i)}\mathbb{Z}$ and σ belongs to $H^{(i)}$ let

$$x(\sigma\tau\sigma^{-1}) = \lambda^{(i)}(\sigma)x(\tau).$$

Then $\lambda^{(i)}(\sigma)$ will be congruent to 1 modulo 8 if $i < n$. If $q^{(i)}$ is the number of elements in $C^{(i)}$ then

$$\frac{q^{(i)} - 1}{k^{(i)}}$$

will be odd.

F' and K' have already been defined. L' is just the fixed field of C'.

$$\frac{q' - 1}{k'} = \frac{p^{\ell} - 1}{k}$$

is odd. If σ' in H' is the image of σ in H^*C then

$$\lambda'(\sigma') \equiv \lambda(\sigma) \pmod k.$$

Since σ is a square modulo H_0

$$\lambda'(\sigma') \equiv 1 \pmod k.$$

If $F^{(i)}$, $L^{(i)}$, and $K^{(i)}$ have been defined and $H^{(i)}$ is not abelian we can define $F^{(i+1)}$, $L^{(i+1)}$, $K^{(i+1)}$ by the process we used to pass from F, L, K to F', L', K'. We have seen that if

$$\frac{q^{(i)} - 1}{k^{(i)}}$$

is odd then

$$\frac{q^{(i+1)} - 1}{k^{(i+1)}}$$

is also odd and that

$$k^{(i)} = 2k^{(i+1)}.$$

We have also seen that $k^{(i)} \ge 8$ if $H^{(i)}$ is not abelian. If $H^{(i)}$ is abelian we take $n = i$.

When we pass from the ith stage to the $(i+1)$th we break up $T^{(i)}$, the analogue of T, into $T^{(i+1)}$ and a complementary set $U^{(i)}$. We may think of $T^{(i)}$ as lying in T. If $\sigma_0^{(i)}$ generates $H^{(i)}$ modulo $H_0^{(i)}$ then

$$\lambda'(\sigma_0^{(i)}) \equiv 1 \pmod 8.$$

We saw that this implies that $U^{(i)}$ has an even number of elements. If μ belongs to $U^{(i)}$ then F_μ is equal to $L^{(i)}$. Thus we may suppose that

$$\nu_{\phi'}\left(\prod\nolimits_{\mu\in U^{(i)}}\ \gamma'_\mu\right) = 1.$$

Moreover $L^{(i)}/F^{(i)}$ is non-abelian and therefore $L^{(i)}/F^{(i)}$ is not totally ramified. Thus μ is not in $U^{(i)}$ if $[F_\mu : F'] = k$.

Since $L^{(n)}/F^{(n)}$ is abelian the isotropy group in $H^{(n)}$ of any μ in $T^{(n)}$ is trivial so that $F_\mu = L^{(n)}$ for such μ. Since

$$\sum\nolimits_{\mu\in T'} \frac{[F_\mu : F']}{k} \equiv \sum\nolimits_{\mu\in T^{(n)}} \frac{[L^{(n)} : F']}{k} \pmod 2.$$

There are an odd number of elements in $T^{(n)}$ and

$$[L^{(n)} : F'] = k.$$

Choose z_0 so that $\sigma(z_0)\sigma_0^2$ lies in $\mathfrak{G}(L/L^{(n)})$. It then fixes each μ in $T^{(n)}$.

Since $L^{(n)}/F'$ must be totally ramified there is a δ in U_F such that

$$N_{L^{(n)}/F}\,\varpi_{L^{(n)}} = \delta\varpi_F^2.$$

The right side of (14.13) is equal to $\nu_\phi(\delta)$. $L^{(n)}$ is contained in L. Choose w_0 in $W_{L/F}$ so that $\tau_{L/F}(w_0) = \varpi_F$. We may suppose that σ_0 has been chosen to be $\sigma(w_0)$. Let L_0 be the fixed field of H_0. Choose u_0 in W_{L/L_0} so that $\sigma(u_0) = \sigma(z_0)$ and so that $\tau_{L/L_0}(u_0)$ is a unit. Clearly z_0 is even if and only if $\tau_{L/L_0}(u_0)$ or

$$N_{L_0/F}\left(\tau_{L/L_0}(u_0)\right) = \tau_{L/F}(u_0)$$

is a square. Since $\sigma(z_0)\sigma_0^2$ lies in $\mathfrak{G}(L/L^{(n)})$,

$$u_0w_0^2$$

lies in $W_{L/L^{(n)}}$. We may take

$$\varpi_{L^{(n)}} = \tau_{L/L^{(n)}}\,(u_0w_0^2).$$

Then

$$N_{L^{(n)}/F}\,(\varpi_{L^{(n)}}) = \tau_{L/F}\,(u_0w_0^2) = \tau_{L/F}\varpi_F^2$$

and $\delta = \tau_{L/F}(u_0)$ is a square if and only if z_0 is even.

Since $(-1)^{a'+1} = 1$ the relation (14.5) amounts to

$$(1)^{a''-1}\,\nu_\phi(-1)^{\frac{q-1}{2k}} = (-1)^{z_0}.$$

(14.6) is equivalent to (14.5) because each $[\phi_\mu : \phi] = 2[\phi_\mu : \phi']$ is even. Recall that

$$a'' = \left(\frac{p^\ell - 1}{k}\right)\left(\frac{p^\ell - 1}{[G : G_0]}\right) \equiv \frac{p^\ell - 1}{[G : G_0]} \pmod 2$$

and that

$$\frac{q-1}{2k} = \left(\frac{p^\ell - 1}{k}\right)\left(\frac{p^\ell + 1}{2}\right) \equiv \frac{p^\ell + 1}{2} \pmod 2.$$

If

$$\mu_0 \equiv 1 \pmod 4$$

then $\nu_\phi(-1) = 1$ and, as we observed earlier, z_0 is odd. We have to show that a'' is even. We showed before that H^* has to contain a cyclic subgroup of order $\frac{k}{2m}[G : G_0]$ and that $\frac{k}{2m}[G : G_0]$ has to divide $p^\ell - 1$. But $\frac{k}{m}$ is the greatest common divisor of $\mu_0 - 1$ and k. Since 4 divides $\mu_0 - 1$ and k it divides $\frac{k}{m}$ and $2[G : G_0]$ divides $p^\ell - 1$. Thus a'' is even.

If

$$\mu_0 \equiv 3 \pmod 4$$

then $\nu_\phi(-1) = -1$. Moreover $k > 2$ so that $p^\ell \equiv 1 \pmod 4$ and

$$\frac{q-1}{2k} \equiv \frac{p^\ell + 1}{2} \equiv 1 \pmod 2.$$

We have to show that a'' is odd if

$$m = \frac{1}{2}[G : G_0]$$

and even otherwise. But $\mu_0 \equiv 3 \pmod 4$ so that $\frac{k}{m} = 2$ and $m = \frac{k}{2}$. Thus $[G : G_0] = 2m$ if and only if $[G : G_0] = k$. If $[G : G_0] = k$ then

$$a'' \equiv \frac{p^\ell - 1}{k} \pmod 2$$

is odd. Otherwise $2[G : G_0]$ divides k and a'' is even.

Lemma 14.3 is now completely proved, so we turn to Lemma 14.4. In the proof of both Lemma 14.4 and 14.5, we will combine the induction assumption with Lemma 15.1 which is stated and proved in paragraph 15, the following paragraph. Suppose $F \subseteq F' \subseteq L$ and F'/F is cyclic of prime degree ℓ. Let $\mathfrak{G}(K/F')$ be $H'C$ where $H' \subseteq H$ and let E' be the fixed field of H'. Then E'/E is cyclic of prime order ℓ. If $S(F'/F)$ is the set of characters of $C_F/N_{F'/F}C_{F'}$ then

$$S(E'/E) = \{\nu_{E/F} \mid \nu_F \in S(F'/F)\}.$$

From Lemma 15.1 we see that for any quasi-character χ_F,

$$\mathrm{Ind}(W_{K/E}, W_{K/E'}, \chi_{E'/E}) \simeq \oplus_{\nu_F \in S(F'/F)}\ \nu_{E/F}\, \chi_{E/F}.$$

Therefore

$$\mathrm{Ind}(W_{K/F}, W_{K/E'}, \chi_{E'/E}) \simeq \oplus_{\nu_F}\, \mathrm{Ind}(W_{K/F}, W_{K/E}, \nu_{E/F}\, \chi_{E/F})$$

which is equivalent to

$$\oplus_{\nu_F}\{(\oplus_{\mu\in T}\,\mathrm{Ind}(W_{K/F}, W_{K/F_\mu}, \mu'\,\nu_{F_\mu/F}\,\chi_{F_\mu/F}))\oplus\nu_F\chi_F\}.$$

If T' is a set of representatives for the non-trivial orbits of H' in $S(K/L)$ then

$$\mathrm{Ind}(W_{K/F'}, W_{K/E'}, \chi_{E'/F}) = \sigma$$

is equivalent to

$$(\oplus_{\mu\in T'}\mathrm{Ind}(W_{K/F'}, W_{K/F'_\mu}, \mu'\,\chi_{F'_\mu/F}))\oplus\chi_{F'/F}.$$

Moreover

$$\mathrm{Ind}(W_{K/F}, W_{K/F'}, \sigma)\simeq\mathrm{Ind}(W_{K/F}, W_{K/E'}, \chi_{E'/E}).$$

Applying the induction assumption to L/F we see that

$$\left\{\prod\nolimits_{\nu_F}\Delta(\nu_F,\chi_F,\psi_F)\right\}\left\{\prod\nolimits_{\nu_F}\prod\nolimits_{\mu\in T}\Delta(\mu'\nu_{F_\mu/F}\,\chi_{F_\mu/F},\psi_{F_\mu/F})\lambda(F/F,\psi_F)\right\}$$

is equal to

$$\{\Delta(\chi_{F'/F},\psi_{F'/F})\lambda(F'/F,\psi_F)\}\left\{\prod\nolimits_{\mu\in T'}\Delta(\mu'\chi_{F'_\mu/F},\psi_{F'_\mu/F})\lambda(F'_\mu/F,\psi_F).\right. \tag{14.14}$$

The application is legitimate because the fields F', F_μ, and F'_μ all lie between F and L. By Lemma 4.5

$$\lambda(F'_\mu/F,\psi_F) = \lambda(F'_\mu/F',\psi_{F'/F})\,\lambda(F'/F,\psi_F)^{[F'_\mu:F']}.$$

Also

$$\lambda(F'/F,\psi_F)\left\{\prod\nolimits_{\mu\in T'}\lambda(F'/F,\psi_F)^{[F'_\mu:F']}\right\} = \lambda(F'/F,\psi_F)^{[E':F']}.$$

Since the fields F' and F'_μ lie between F' and K we can apply the induction assumption to K/F' to see that (14.14) is equal to the product of

$$\lambda(F'/F,\psi_F)^{[E':F']}$$

and

$$\Delta(\chi_{E'/F},\psi_{E'/F})\ \lambda(E'/F',\psi_{F'/F}).$$

Applying the induction assumption to K/E we see that

$$\Delta(\chi_{E'/F},\psi_{E'/F})$$

is equal to

$$\left\{\prod\nolimits_{\nu_F\in S(F'/F)}\Delta(\nu_{E/F}\,\chi_{E/F},\psi_{E/F})\right\}\lambda(E'/E,\psi_{E/F})^{-1}.$$

We conclude that the quotient

$$\prod\nolimits_{\nu_F}\left\{\frac{\Delta(\nu_F\,\chi_F,\psi_F)\,\prod_{\mu\in T}\Delta(\mu'\nu_{F_\mu/F}\,\chi_{F_\mu/F},\psi_{F_\mu/F}}{\Delta(\nu_{E/F}\,\chi_{E/F},\psi_{E/F})}\right\} \tag{14.15}$$

is independent of χ_F. Taking χ_F to be trivial we see that it equals

$$\prod_{\nu_F} \left\{ \frac{\Delta(\nu_F,\psi_F)\ \prod_{\mu\in T}\ \Delta(\mu'\,\nu_{F_\mu/F},\psi_{F_\mu/F})}{\Delta(\nu_{E/F},\psi_{E/F})} \right\}. \tag{14.16}$$

It is easily seen that the complex conjugate of $\Delta(\nu_F,\psi_F)$ is

$$\nu_F(-1)\,\Delta(\nu_F^{-1},\psi_F).$$

Thus

$$\Delta(\nu_F,\psi_F)\,\Delta(\nu_F^{-1},\psi_F) = \nu_F(-1).$$

If ℓ is odd the right side is 1. Since

$$\Delta(1,\psi_F) = 1$$

and $\nu_F \neq \nu_F^{-1}$ if ℓ is odd, the product

$$\prod_{\nu_F\in S(L/F)}\ \Delta(\nu_F,\psi_F) = 1.$$

For the same reasons

$$\prod_{\nu_F\in S(L/F)}\ \Delta(\nu_{E/F},\psi_{E/F}) = 1.$$

However, if ℓ is 2

$$\Delta(\nu_F,\psi_F) = \Delta(\nu_F^{-1},\psi_F)$$

has square ± 1 and is therefore a fourth root of unity. Thus

$$\prod_{\nu\in S(L/F)}\ \Delta(\nu_F,\psi_F) \sim \prod_{\nu\in S(L/F)}\ \Delta(\nu_{E/F},\psi_{E/F}) \sim_2 1.$$

On the other hand, $m(\mu') = t+1 \geq 2$ while $m(\nu_{F_\mu/F}) \leq 1$. Thus Lemma 9.5 shows that

$$\Delta(\mu'\nu_{F_\mu/F},\psi_{F_\mu/F}) \sim_\ell\ \Delta(\mu',\psi_{F_\mu/F}).$$

Thus the expression (14.16) and therefore the expression (14.15) is equal to

$$\eta\left\{\prod_{\mu\in T}\ \Delta(\mu',\psi_{F_\mu/F})\right\}^\ell$$

where $\eta \sim_\ell 1$.

If $m(\chi_F)$ is 0 or 1, Lemma 14.4 is a consequence of Lemma 14.2. We suppose therefore that $m(\chi_F) \geq 2$. In this case Lemma 9.5 implies that

$$\prod_{\nu_F}\ \Delta(\nu_F\,\chi_F,\psi_F) \sim_\ell\ \Delta(\chi_F,\psi_F)^\ell$$

and that

$$\prod_{\nu_F}\ \Delta(\nu_{E/F}\,\chi_{E/F},\psi_{E/F}) \sim_\ell\ \Delta(\chi_{E/F},\psi_{E/F})^\ell.$$

We also saw in the beginning of the paragraph that, in all cases, $m(\mu'\chi_{F_\mu/F}) \geq 2$. Thus

$$\Delta(\mu'\nu_{F_\mu/F}\chi_{F_\mu/F}, \psi_{F_\mu/F}) \sim_\ell \Delta(\mu'\chi_{F_\mu/F}, \psi_{F_\mu/F}).$$

Putting these facts together we see that if

$$\sigma\Big\{\Delta\left(\chi_F, \psi_F\right) \prod\nolimits_{\mu\in T} \Delta(\mu'\chi_{F_\mu/F}, \psi_{F_\mu/F})\Big\}^\ell$$

is equal to

$$\Big\{\Delta(\chi_{E/F}, \psi_{E/F}) \prod\nolimits_{\mu\in T} \Delta(\mu', \psi_{F_\mu/F})\Big\}^\ell$$

then $\sigma \sim_\ell 1$. Since $\sigma = \rho^\ell$ we conclude that

$$\rho \sim_\ell 1.$$

Finally we have to prove Lemma 14.5. Let F' be the fixed field of H_1C and let L' be the fixed field of H_2C. Let E' be the fixed field of H_1 and let K' be the fixed field of H_2. Let P be a set of representatives for the orbits under $\mathfrak{G}(L/F)$ of the characters in $S(L/L')$. If ν is one of these representatives, let $H_\nu H_2 C$ with H_ν and H_1 be its isotropy group and let F_ν be the fixed field of $H_\nu H_2 C$. Applying the induction assumption and Lemma 15.1 to the extension L/F we see that

$$\Delta(\chi_{F'/F}, \psi_{F'/F})\,\rho\,(F'/F, \psi_F)$$

is equal to

$$\prod\nolimits_{\nu\in P} \Delta(\nu'\chi_{F_\nu/F}, \psi_{F_\nu/F})\,\lambda(F_\nu/F, \psi_F). \tag{14.17}$$

Let

$$R = \{\nu \in P \mid F_\nu = F\}$$

and let S be the complement of R in P. R consists of the elements of $S(L/L')$ fixed by each element of $\mathfrak{G}(L/F)$. It is a subgroup of $S(L/L')$ and its order r must therefore be a power of ℓ. The expression (14.17) may be written as

$$\Big\{\prod\nolimits_{\nu\in R}\Delta(\nu'\chi_F, \psi_F)\Big\}\ \Big\{\prod\nolimits_{\nu\in S}\Delta(\nu'\chi_{F_\nu/F}, \psi_{F_\nu/F})\,\lambda(F_\nu/F, \psi_F)\Big\}.$$

If F is replaced by E and F' by E' then P is replaced by

$$\{\nu_{K'/L'} \mid \nu = \nu_{L'} \in P\}.$$

Also F_ν is replaced by E_ν, the fixed field of $H_\nu H_2$, and ν' is replaced by ν'_{E_ν/F_ν}. Applying the induction assumption to K/E we see that

$$\Delta(\chi_{E'/F}, \psi_{E'/F})\,\lambda(E'/E, \psi_{E/F})$$

is equal to the product of

$$\left\{\prod\nolimits_{\nu\in R}\,\Delta(\nu'_{E/F}\,\chi_{E/F},\psi_{E/F}\right\}$$

and

$$\left\{\prod\nolimits_{\nu\in S}\,\Delta(\nu'_{E_\nu/F_\nu}\chi_{E_\nu/F_\nu},\psi_{E_\nu/F})\,\lambda(E_\nu/E,\psi_{E/F}\right\}.$$

This equality will be referred to as relation (14.18).

To derive this equality we have used not only the induction assumption but also Lemma 15.1 which implies that

$$\mathrm{Ind}(W_{K/E},W_{K/E'},\chi_{E'/F})$$

is equivalent to

$$\{\oplus_R\,\mathrm{Ind}(W_{K/E},W_{K/E},\nu'_{E/F}\,\chi_{E/F})\}\ \oplus\ \{\oplus_S\,\mathrm{Ind}(W_{K/E},W_{K/E_\nu},\nu'_{E_\nu/F_\nu}\chi_{E_\nu/F})\}.$$

Thus

$$\mathrm{Ind}(W_{K/F},W_{K/E'},\chi_{E'/F})$$

will be equivalent to the direct sum of

$$\oplus_R\,\mathrm{Ind}(W_{K/F},W_{K/E},\nu'_{E/F}\,\chi_{E/F})$$

and

$$\oplus_S\,\mathrm{Ind}(W_{K/F},W_{K/E_\nu},\nu'_{E_\nu/F_\nu}\chi_{E_\nu/F}).$$

If ν is in R we can apply Lemma 15.1 to see that

$$\mathrm{Ind}\,(W_{K/F},W_{K/E},\nu'_{E/F}\,\chi_{E/F})$$

is equivalent to

$$\{\oplus_{\mu\in T}\,\mathrm{Ind}(W_{K/F},W_{K/F_\mu},\mu'\nu'_{F_\mu/F}\chi_{F_\mu/F})\}\oplus\nu'\chi_F.$$

We can obtain

$$\mathrm{Ind}\,(W_{K/F},W_{K/F_\nu},\nu'_{E_\nu/F_\nu}\chi_{E_\nu/F})$$

by first inducing from W_{K/E_ν} to W_{K/F_ν} and then from W_{K/F_ν} to $W_{K/F}$.

If T_ν is a set of representatives for the orbits of $S(K/L)$ under the action of $\mathfrak{G}(K/F_\nu)$ and $F_{\nu,\mu}$ is the fixed field of the isotropy group of μ in T_ν then, by Lemma 15.1 again,

$$\mathrm{Ind}\,(W_{K/F_\nu},W_{K/E_\nu},\nu'_{E_\nu/F_\nu}\chi_{E_\nu/F})$$

is equivalent to

$$\oplus_{T_\nu}\,\mathrm{Ind}\,(W_{K/F_\nu},W_{K/F_{\nu,\mu}},\mu'\nu'_{F_{\nu,\mu}/F_\nu}\chi_{F_{\nu,\mu}/F}).$$

Since $[K:F_\nu]<[K:F]$ if ν belongs to S, we can apply the induction assumption to see that

$$\Delta(\nu'_{E_\nu/F_\nu}\chi_{E_\nu/F},\psi_{E_\nu/F})\,\lambda(E_\nu/F_\nu,\psi_{F_\nu/F})$$

is equal to

$$\prod\nolimits_{\mu\in T_\nu} \Delta(\mu'\nu'_{F_{\nu,\mu}/F_\nu}\chi_{F_{\nu,\mu}/F},\psi_{F_\nu/F})\,\lambda(F_{\nu,\mu}/F_\nu,\psi_{F_\nu/F}).$$

This equality will be referred to as relation (14.19).

It also follows that

$$\operatorname{Ind}(W_{K/F},W_{K/E_\nu},\nu'_{E_\nu/F_\nu}\chi_{E_\nu/F})$$

is equivalent to

$$\oplus_{\mu\in T_\nu}\operatorname{Ind}(W_{K/F},W_{K/F_{\nu,\mu}},\mu'\nu'_{F_{\nu,\mu}/F_\nu}\chi_{F_{\nu,\mu}/F}).$$

The fields F_ν and $F_{\nu,\mu}$ all lie between F and L. Thus we have expressed

$$\operatorname{Ind}(W_{K/F},W_{K/E'},\chi_{E'/F}) \tag{14.20}$$

as a direct sum of terms of the form

$$\operatorname{Ind}(W_{K/F},W_{K/M},\chi_M) \tag{14.21}$$

where M lies between F and L. Moreover such a representation is in fact a representation of $W_{K/F}$ obtained by inflating a representation of $W_{L/F}$, namely, by inflating

$$\operatorname{Ind}(W_{L/F},W_{L/M},\chi_M).$$

Thus any other expression of (14.20) as a sum of representations of the form (14.21) will lead, by an application of the induction assumption to L/F, to an identity between the numbers $\Delta(\chi_M,\psi_{M/F})$.

To obtain another such expression, we observe that the representation (14.20) can be obtained by first inducing from $W_{K/E'}$ to $W_{K/F'}$ and then from $W_{K/F'}$ to $W_{K/F}$. If T' is a set of representatives for the orbits of non-trivial characters in $S(K/L)$ under the action of $\mathfrak{G}(K/F')$ and F'_μ is the fixed field of the isotropy group in $\mathfrak{G}(K/F')$ of μ in T' then

$$\operatorname{Ind}(W_{K/F'},W_{K/E'},\chi_{E'/F})$$

is equivalent to

$$\{\oplus_{\mu\in T'}\operatorname{Ind}(W_{K/F'},W_{K/F'_\mu},\mu'\chi_{F'_\mu/F}\}\oplus\chi_{F'/F}.$$

Thus (14.20) is equivalent to the direct sum of

$$\operatorname{Ind}(W_{K/F},W_{K/F'},\chi_{F'/F})$$

and

$$\oplus_{\mu\in T'}\operatorname{Ind}(W_{K/F},W_{K/F'_\mu},\mu'\,\chi_{F'_\mu/F}).$$

We shall describe the resultant identity in a moment. We first apply the induction assumption to the extension K/F' to see that

$$\Delta(\chi_{E'/F},\psi_{E'/F})\,\lambda(E'/F',\,\psi_{F'/F})$$

is equal to

$$\Delta(\chi_{F'/F},\psi_{F'/F})\prod\nolimits_{\mu\in T'}\Delta(\mu'\chi_{F'_\mu/F},\psi_{F'_\mu/F})\,\lambda(F'_\mu/F',\psi_{F'/F}).$$

This equality will be relation (14.22).

The two expressions for the representation (14.20) lead to the conclusion that the product of

$$\prod\nolimits_{\nu\in R}\Delta(\nu'\chi_F,\psi_F) \tag{14.23}$$

and

$$\prod\nolimits_{\nu\in R}\prod\nolimits_{\mu\in T}\Delta(\mu'\nu'_{F_\mu/F}\chi_{F_\mu/F},\psi_{F_\mu/F})\,\lambda(F_\mu/F,\psi_F) \tag{14.24}$$

and

$$\prod\nolimits_{\nu\in S}\prod\nolimits_{\mu\in T_\nu}\Delta(\mu'\nu'_{F_{\nu,\mu}/F_\nu}\chi_{F_{\nu,\mu}/F},\psi_{F_{\nu,\mu}/F})\,\lambda(F_{\nu,\mu}/F,\psi_F) \tag{14.25}$$

is equal to the product of

$$\Delta(\chi_{F'/F},\psi_{F'/F})\,\lambda(F'/F,\psi_F)$$

and

$$\prod\nolimits_{\mu\in T'}\Delta(\mu'\chi_{F'_\mu/F},\psi_{F'_\mu/F})\,\lambda(F'_\mu/F,\psi_F).$$

Applying relation (14.22) and Lemma 4.5 we see that the second of these two products is equal to

$$\Delta(\chi_{E'/F},\psi_{E'/F})\,\lambda(E'/F',\,\psi_{F'/F})\,\lambda(F'/F,\psi_F)^{[E':F']}.$$

According to the relation (14.18) this expression is the product of

$$\left\{\prod\nolimits_{\nu\in R}\Delta(\nu'_{E/F}\chi_{E/F},\psi_{E/F})\right\}\left\{\prod\nolimits_{\nu\in S}\Delta(\nu'_{E/F}\chi_{E/F},\psi_{E/F})\right\}$$

and

$$\prod\nolimits_{\nu\in S}\lambda(E_\nu/E,\psi_{E/F})$$

and

$$\lambda(E'/E,\psi_{E/F})^{-1}\,\lambda(E'/F',\psi_{F'/F})\,\lambda(F'/F,\psi_F)^{[E':F']}. \tag{14.26}$$

Equating this final product to the product of (14.23), (14.24), and (14.25) and then making certain cancellations by means of (14.19), we see that the product of (14.23) and (14.24) and

$$\prod\nolimits_{\nu\in S}\prod\nolimits_{\mu\in T_\nu}\lambda^{-1}(F_{\nu,\mu}/F_\nu,\psi_{F_\nu/F})\,\lambda(F_{\nu,\mu}/F,\psi_F)$$

is equal to the product of

$$\prod\nolimits_{\nu\in R}\Delta(\nu'_{E/F}\,\chi_{E/F},\psi_{E/F})$$

and

$$\prod\nolimits_{\nu\in S}\lambda^{-1}(E_\nu/F_\nu,\psi_{F_\nu/F})\,\lambda(E_\nu/E,\psi_{E/F})$$

and the expression (14.26).

In particular, the expression

$$\prod\nolimits_{\nu\in R}\left\{\frac{\Delta(\nu'\chi_F,\psi_F)\,\prod_{\mu\in T}\Delta(\mu'\nu'_{F_\mu/F}\,\chi_{F_\mu/F},\psi_{F_\mu/F})}{\Delta(\nu'_{E/F}\,\chi_{E/F},\psi_{E/F})}\right\}$$

is independent of χ_F. Taking χ_F to be trivial we see that

$$\prod_{\nu\in R}\left\{\frac{\Delta(\nu'\chi_F,\psi_F)\ \prod_{\mu\in T}\ \Delta(\mu'\nu'_{F_\mu/F}\,\chi_{F_\mu/F},\psi_{F_\mu/F})}{\Delta(\nu'_{E/F}\,\chi_{E/F},\psi_{E/F})\ \prod_{\mu\in T}\ \Delta(\mu'\nu'_{F_\mu/F},\psi_{F_\mu/F})}\right\}$$

is equal to

$$\prod_{\nu\in R}\ \frac{\Delta(\nu',\psi_F)}{\Delta(\nu'_{E/F},\psi_{E/F})}.$$

The set

$$R'=\{\nu'\mid \nu\in R\}$$

is a group of characters of C_F or of H. Regarded as characters of H the elements of R' are just those characters which are trivial on H_1. As a group R' is cyclic and its order is a power of ℓ. The argument used in the proof of Lemma 14.4 shows that

$$\prod_{\nu\in R}\ \Delta(\nu',\psi_F)\sim_\ell 1$$

and

$$\prod_{\nu\in R}\ \Delta(\nu'_{E/F},\psi_{E/F})\sim_\ell 1.$$

If $m(\chi_F)$ is 0 or 1, Lemma 14.5 is a consequence of Lemma 14.2. We may as well suppose therefore that $m(\chi_F)>1$. If ν belongs to R then ν' is 1 on $N_{L/F}C_L$. Therefore $m(\nu')$, as well as $m(\nu'_{F_\mu/F})$ and $m(\nu'_{E/F})$ is at most 1. We saw in the beginning of this paragraph that $m(\chi_{E/F})$ would also be at least 2. We also saw that $m(\mu'\chi_{F_\mu/F})$ would be either $t+1$ or $\psi_{F_\mu/F}(m-1)+1$. In any case it is at least 2. Also $m(\mu')=t+1$ is at least 2. Lemma 9.5 therefore implies the following relations:

$$\begin{aligned}
\Delta(\nu'\chi_F,\psi_F)&\sim_\ell\ \Delta(\chi_F,\psi_F)\\
\Delta(\nu'_{E/F}\,\chi_{E/F},\psi_{E/F}&\sim_\ell\ \Delta(\chi_{E/F},\psi_{E/F})\\
\Delta(\mu'\nu'_{F_\mu/F}\,\chi_{F_\mu/F},\psi_{F_\mu/F}&\sim_\ell\ \Delta(\mu'\chi_{F_\mu/F},\psi_{F_\mu/F})\\
\Delta(\mu'\nu'_{F_\mu/F},\psi_{F_\mu/F})&\sim_\ell\ \Delta(\mu',\psi_{F_\mu/F}).
\end{aligned}$$

We conclude finally that

$$\left\{\frac{\Delta(\chi_F,\psi_F)\ \prod_{\mu\in T}\Delta(\mu'\chi_{F_\mu/F},\psi_{F_\mu/F})}{\Delta(\chi_{E/F},\psi_{E/F})\ \prod_{\mu\in T}\Delta(\mu',\psi_{F_\mu/F})}\right\}^r\sim_\ell 1$$

if r is the number of elements in R. The lemma follows.

Chapter Fifteen.

Another Lemma

Suppose K/F is normal and $G = \mathfrak{G}(K/F)$. Suppose H is a subgroup of G and C is an abelian normal subgroup of G. Let E be the fixed field of H and L that of C. If μ is a character of C and h belongs to H, define μ^h by

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

The set of characters of C may be identified with $S(K/L)$. If α belongs to C_L

$$\mu^h(\alpha) = \mu(h(\alpha)).$$

The set of elements in $S(K/L)$ which are trivial on $H \cap C$ is invariant under H. Let T be a set of representatives for the orbits of H in this set. If $\mu \in T$ let H_μ be the isotropy group of μ, let $G_\mu = H_\mu C$ and let F_μ be the fixed field of G_μ. Define a character μ' of G_μ by

$$\mu'(hc) = \mu(c)$$

if $h \in H_\mu$ and $c \in C$. μ' may be regarded as a character of C_{F_μ}.

Lemma 15.1

If χ_F is a quasi-character of C_F then

$$\rho = \mathrm{Ind}(W_{K/F}, W_{K/E}, \chi_{E/F})$$

is equivalent to

$$\oplus_{\mu\in T} \mathrm{Ind}(W_{K/F}, W_{K/F_\mu}, \mu'\chi_{F_\mu/F}).$$

Let $G' = HC$ and let F' be the fixed field of G'. F' is contained in E and in the fields F_μ. Because of the transitivity of the induction process it is enough to show that

$$\mathrm{Ind}(W_{K/F'}, W_{K/E}, \chi_{E/F})$$

is equivalent to

$$\oplus_{\mu\in T}\mathrm{Ind}(W_{K/F'}, W_{K/F_\mu}, \mu'\chi_{F_\mu/F}).$$

If

$$\chi'_{F'} = \chi_{F'/F}$$

then

$$\chi_{E/F} = \chi'_{E/F'}$$

and

$$\chi_{F_\mu/F} = \chi'_{F_\mu/F'}.$$

Consequently we may suppose, with no loss of generality, that F' is F.

If K' is the fixed field of $H \cap C$ and $\nu \in S(K'/L)$ let φ_ν be the function on $W_{K/F}$ defined by

$$\varphi_\nu(hc) = \chi_F(\tau_{K/F}(hc))\ \nu(\tau_{K/L}(c))$$

for h in $W_{K/E},\ c$ in $W_{K/L}$. ρ acts on the space of all functions φ on $W_{K/F}$ satisfying

$$\varphi(hg) = \chi_F(\tau_{K/F}(h))\ \varphi(g)$$

for all h in $W_{K/E}$ and all g in $W_{K/F}$. The set

$$\{\varphi_\nu \,|\, \nu \in S(K'/L)\}$$

is a basis for this space. Clearly

$$\rho(c)\varphi_\nu = \chi_F(\tau_{K/F}(c))\ \nu(\tau_{K/L}(c))\varphi_\nu$$

if c belongs to $W_{K/L}$ and

$$\rho(h)\varphi_\nu = \chi_F(\tau_{K/F}(h))\varphi_{\nu'},$$

with $\nu' = \nu^{h^{-1}}$, if h belongs to $W_{K/E}$. Thus if R is an orbit of H in $S(K'/L)$

$$\oplus_{\nu\in R}\mathbb{C}_{\varphi_\nu} = V$$

is an invariant subspace.

Let μ be the element common to T and R and consider

$$\sigma = \mathrm{Ind}(W_{K/F}, W_{K/F_\mu}, \mu'\chi_{F_\mu/F}).$$

If $W_{K/F}$ is the disjoint union

$$\bigcup\nolimits_{i=1}^{r} W_{K/F_\mu} h_i$$

and if $\varphi_i(w) = 0$ unless

$$w \in W_{K/F_\mu} h_i$$

while

$$\varphi_i(wh_i) = \mu'\chi_{F_\mu/F}(\tau_{K/F_\mu}(w))$$

for w in W_{K/F_μ} then

$$\{\varphi_i \,|\, 1 \le i \le r\}$$

is a basis for the space U on which σ acts. If $\nu_i = \mu^{h_i}$ and if λ is the map from U to V which sends φ_i to $\chi_F^{-1}(\tau_{K/F}(h_i))\varphi_{\nu_i}$ then, as one verifies easily,

$$\lambda\sigma(w) = \rho(w)\lambda$$

for all w in $W_{K/F}$. The lemma follows.

The lemma has a corollary.

Lemma 15.2

If Theorem 2.1 is valid for K/F then

$$\Delta(\chi_{E/F}, \psi_{E/F})\ \prod\nolimits_{\mu\in T} \Delta(\mu', \psi_{F_\mu/F})$$

is equal to

$$\prod\nolimits_{\mu\in T} \Delta(\mu'\chi_{F_\mu/F}, \psi_{F_\mu/F}).$$

If Theorem 2.1 is valid

$$\Delta(\chi_{E/F}, \psi_{E/F})\,\lambda(E/F, \psi_F)$$

is equal to

$$\prod\nolimits_{\mu\in T} \Delta(\mu'\chi_{F_\mu/F}, \psi_{F_\mu/F})\ \lambda(F_\mu/F, \psi_F).$$

Taking $\chi_F = 1$, we see that

$$\lambda(E/F, \psi_F) = \prod\nolimits_{\mu\in T} \Delta(\mu', \psi_{F_\mu/F})\ \lambda(F_\mu/F, \psi_F).$$

Substituting this into the first equality and cancelling the non-zero factor

$$\prod\nolimits_{\mu\in T}\ \lambda(F_\mu/F, \psi_F)$$

we obtain the lemma.

To define the λ-function we shall need the following lemma.

Lemma 15.3

Suppose Theorem 2.1 is valid for all Galois extensions K_1/F_1 *with* $F \subseteq F_1 \subseteq K_1 \subseteq K$ *and* $[K_1 : F_1] < [K : F]$. *Then*

$$\Delta(\chi_{E/F}, \psi_{E/F})\ \prod\nolimits_{\mu\in T} \Delta(\mu', \psi_{F_\mu/F})$$

is equal to

$$\prod\nolimits_{\mu\in T} \Delta(\mu'\chi_{F_\mu/F}, \psi_{F_\mu/F}).$$

The conclusion of this lemma is the same as that of the previous one. There is however a critical difference in the assumptions.

Let F' be the fixed field of HC. If

$$\psi'_{F'} = \psi_{F'/F}$$

then for all separable extensions E' of F'

$$\psi'_{E'/F'} = \psi_{E'/F}.$$

If $[K : F'] < [K : F]$ the relation of the lemma is a consequence of the induction assumption and the previous lemma. We thus suppose that $F = F'$ and $G = HC$.

Suppose in addition that there is a subgroup C_1 of C, which is neither C nor $\{1\}$, whose normalizer contains H. C_1 is then a normal subgroup of G. Let F_1 be the fixed field of HC_1 and L_1 the fixed field of C_1. Lemma 15.1 applies to the extension K/F_1. Thus there are fields $A_1, \dots, A_r$ lying between F_1 and L_1 and quasi-characters $\chi_{A_1}, \dots, \chi_{A_r}$ such that

$$\mathrm{Ind}(W_{K/F_1}, W_{K/E}, \chi_{E/F})$$

is equivalent to
$$\oplus_{i=1}^{r}\ \mathrm{Ind}(W_{K/F_1}, W_{K/A_i}, \chi_{A_i}).$$
The induction assumption then implies that
$$\Delta(\chi_{E/F}, \psi_{E/F})\,\lambda(E/F_1, \psi_{F_1/F}) \tag{15.1}$$
is equal to
$$\prod_{i=1}^{r}\ \Delta(\chi_{A_i}, \psi_{A_i/F})\,\lambda(A_i/F_1, \psi_{F_1/F}). \tag{15.2}$$

Inducing the first of these two representations from W_{K/F_1} to $W_{K/F}$, we obtain
$$\mathrm{Ind}(W_{K/F}, W_{K/E}, \psi_{E/F}).$$
Thus
$$\oplus_{\mu\in T}\ \mathrm{Ind}(W_{K/F}, W_{K/F_\mu}, \mu'\chi_{F_\mu/F}) \tag{15.3}$$
is equivalent to
$$\oplus_{i=1}^{r}\ \mathrm{Ind}(W_{K/F}, W_{K/A_i}, \chi_{A_i}). \tag{15.4}$$

We recall that there exist surjective homomorphisms
$$\tau_{K/F,L_1/F} : W_{K/F} \longrightarrow W_{L_1/F}$$
$$\tau_{K/A_i,L_1/A_i} : W_{K/A_i} \longrightarrow W_{L_1/A_i}$$
$$\tau_{K/F_\mu,L_1/F_\mu} : W_{K/F_\mu} \longrightarrow W_{L_1/F_\mu}$$
whose kernels are all equal to the commutator subgroup W^c_{K/L_1} of W_{K/L_1}. Moreover the diagrams
$$\begin{array}{ccc} W_{K/A_i} & \longrightarrow & W_{L_1/A_i} \\ \downarrow & & \downarrow \\ W_{K/F} & \longrightarrow & W_{L_1/F} \end{array}$$
and
$$\begin{array}{ccc} W_{K/F_\mu} & \longrightarrow & W_{L_1/F_\mu} \\ \downarrow & & \downarrow \\ W_{K/F} & \longrightarrow & W_{L_1/F} \end{array}$$
may be supposed commutative. Since W^c_{K/L_1} lies in the kernel of χ_{A_i} and $\mu'\chi_{F_\mu/F}$ the equivalence of (15.3) and (15.4) amounts to the equivalence of
$$\oplus_{\mu\in T}\mathrm{Ind}(W_{L_1/F}, W_{L_1/F_\mu}, \mu'\chi_{F_\mu/F})$$
and
$$\oplus_{i=1}^{r}\mathrm{Ind}(W_{L_1/F}, W_{L_1/A_i}, \chi_{A_i}).$$

The induction assumption applied to the extension L_1/F implies that

$$\prod_{i=1}^{r} \Delta(\chi_{A_i}, \psi_{A_i/F})\, \lambda(A_i/F, \psi_F)$$

is equal to

$$\prod_{\mu\in T} \Delta(\mu'\chi_{F_\mu/F}, \psi_{F_\mu/F})\, \lambda(F_\mu/F, \psi_F).$$

It also implies that

$$\lambda(A_i/F, \psi_F) = \lambda(A_i/F_1, \psi_{F_1/F})\, \lambda(F_1/F, \psi_F)^{[A_i:F_1]}.$$

Since

$$\sum_i [A_i : F_1] = [E : F_1]$$

we infer from the equality of (15.1) and (15.2) that

$$\Delta(\chi_{E/F}, \psi_{E/F})\, \lambda(E/F_1, \psi_{F_1/F})\, \lambda(F_1/F, \psi_F)^{[E:F_1]}$$

is equal to

$$\prod_{\mu\in T} \Delta(\mu'\chi_{F_\mu/F}, \psi_{F_\mu/F})\, \lambda(F_\mu/F, \psi_F).$$

Taking $\chi_F = 1$ to find the value of

$$\lambda(E/F_1, \psi_{F_1/F})\, \lambda(F_1/F, \psi_F)^{[E:F_1]}$$

and then substituting the result into the equation and cancelling the common factors we obtain the assertion of the lemma.

Now suppose that H contains a normal subgroup $H_1 \neq \{1\}$ which lies in the centralizer of C. H_1 is a normal subgroup of G if, as we are assuming, $G = HC$. K_1, the fixed field of H_1, contains E and all the fields F_μ. Lemma 15.1 together with the argument just applied to L_1 shows that

$$\mathrm{Ind}(W_{K_1/F}, W_{K_1/E}, \chi_E)$$

is equivalent to

$$\oplus_{\mu\in T}\mathrm{Ind}(W_{K_1/F}, W_{K_1/F_\mu}, \mu'\chi_{F_\mu/F}).$$

In this case the assertion of the lemma follows from the induction assumption applied to K_1/F.

We have finally to suppose that $G = HC$, C contains no proper subgroup invariant under H, and H contains no normal subgroup lying in the centralizer of C. In particular $H \cap C = \{1\}$. If Z is the centralizer of C then $Z = (Z \cap H)C$ and $Z \cap H$ is a normal subgroup of H. Consequently $Z = C$. If D is a normal subgroup of G and D does not contain C then

$$D \cap C = \{1\}.$$

This implies that D is contained in Z. Thus D is contained in C and $D = \{1\}$. If $H \neq \{1\}$ the assertion of the lemma is that of the third and fourth main lemmas. If $H = \{1\}$ then $G = C$ and C is cyclic of prime order so that the assertion is that of the first main lemma.

Chapter Sixteen.

Definition of the λ Functions

In this and the next three paragraphs, we take a fixed Galois extension K/F, assume that Theorem 2.1 is valid for all Galois extensions K'/F' with $F \subseteq F' \subseteq K' \subseteq K$ and $[K' : F'] < [K : F]$, and prove that it is valid for K/F itself. The first step is to define and establish some simple properties of the function which will serve as the λ-function.

Lemma 16.1

Suppose

$$E/F' \longrightarrow \lambda(E/F',\, \psi_{F'})$$

is a weak λ-function on $\mathcal{P}_0(K'/F')$. If $\sigma \in \mathfrak{G}(K'/F')$ let

$$E^\sigma = \{\sigma^{-1}(\alpha) \mid \alpha \in E\}.$$

Then

$$\lambda(E^\sigma/F', \psi_{F'}) = \lambda(E/F', \psi_{F'}).$$

If μ is a character of $\mathfrak{G}(K/E)$ let μ^σ be the character of $\mathfrak{G}(K/E^\sigma)$ defined by

$$\mu^\sigma(\rho) = \mu(\sigma\rho\sigma^{-1}).$$

According to Lemma 13.2

$$\Delta(\mu^\sigma, \psi_{E^\sigma/F'}) = \Delta(\mu, \psi_{E/F'}).$$

The representation

$$\mathrm{Ind}(\mathfrak{G}(K'/F'),\ \mathfrak{G}(K'/E), \mu)$$

acts on the space U of functions φ on $\mathfrak{G}(K'/F')$ satisfying

$$\varphi(\rho\tau) = \mu(\rho)\ \varphi(\tau)$$

for all τ in $\mathfrak{G}(K'/F')$ and all ρ in $\mathfrak{G}(K'/E)$. The map $\varphi \longrightarrow \psi$ with

$$\psi(\tau) = \varphi(\sigma\tau)$$

is a $\mathfrak{G}(K'/F')$ isomorphism of U with the space on which

$$\mathrm{Ind}(\mathfrak{G}(K'/F'),\ \mathfrak{G}(K'/E^\sigma),\, \mu^\sigma)$$

acts. Thus the two representations are equivalent.

If

$$\oplus_{i=1}^r \mathrm{Ind}(\mathfrak{G}(K'/F'),\ \mathfrak{G}(K'/E_i),\, \mu_i)$$

is equivalent to

$$\oplus_{j=1}^s \mathrm{Ind}(\mathfrak{G}(K'/F'),\ \mathfrak{G}(K'/F_j),\, \nu_j)$$

then

$$\oplus_{i=1}^{r}\mathrm{Ind}(\mathfrak{G}(K'/F'),\,\mathfrak{G}(K'/E_i^\sigma),\,\mu_i^\sigma)$$

is equivalent to

$$\oplus_{j=1}^{s}\mathrm{Ind}(\mathfrak{G}(K'/F'),\,\mathfrak{G}(K'/F_j^\sigma),\,\nu_j^\sigma)$$

and, with the conventions of the fourth paragraph,

$$\prod_{i=1}^{r}(\chi_{E_i^\sigma},\psi_{E_i^\sigma/F'})\,\lambda(E_i^\sigma/F',\psi_{F'})$$

is equal to

$$\prod_{j=1}^{s}\Delta(\chi_{F_j^\sigma},\psi_{F_j^\sigma/F'})\,\lambda(F_j^\sigma/F',\psi_{F'}).$$

Since

$$\Delta(\chi_{F_j^\sigma},\psi_{F_j^\sigma/F'})=\Delta(\chi_{F_j},\psi_{F_j/F'})$$

and

$$\Delta(\chi_{E_i^\sigma},\psi_{E_i^\sigma/F'})=\Delta(\chi_{E_i},\psi_{E_i/F'}).$$

We conclude that

$$\prod_{i=1}^{r}\Delta(\chi_{E_i},\psi_{E_i/F'})\,\lambda(E_i^\sigma/F',\psi_{F'})$$

is equal to

$$\prod_{j=1}^{s}\Delta(\chi_{F_j},\psi_{F_j/F'})\,\lambda(F_j^\sigma/F',\psi_{F'}).$$

In other words

$$E/F'\longrightarrow\lambda(E^\sigma/F',\psi_{F'})$$

is a weak λ-function on $\mathcal{P}_0(K'/F')$. Lemma 16.1 follows from the uniqueness of such functions.

We return to the problem of defining a λ-function on $\mathcal{P}_0(K/F)$. Choose a non-trivial abelian normal subgroup C of $G=\mathfrak{G}(K/F)$ and let L be the fixed field of C. If E is any field lying between F and K let H be the corresponding subgroup of G. Choose the set T of characters and the fields F_μ as in the previous paragraph. Since $F_\mu\subseteq L$ the numbers $\lambda(F_\mu/F,\psi_F)$ are defined.

Lemma 16.2

Suppose $F\subseteq E\subseteq K_1\subsetneq K$ with K_1/F normal so that $\lambda(E/F,\psi_F)$ is defined. Then

$$\lambda(E/F,\psi_F)=\prod_{\mu\in T}\Delta(\mu',\psi_{F_\mu/F})\,\lambda(F_\mu/F,\psi_F).$$

Let K_1 be the fixed field of H_1. If $H_1\cap C\neq\{1\}$ we may enlarge K_1 and replace H_1 by $H_1\cap C$. Thus we may suppose that either H_1 is contained in C or $H_1\cap C=\{1\}$. In either case H_1 is contained in the centralizer of C. We saw in the previous paragraph that under these circumstance

$$\mathrm{Ind}(W_{K_1/F},W_{K_1/E},1)\simeq\oplus_{\mu\in T}\mathrm{Ind}(W_{K_1/F},W_{K_1/F_\mu},\mu').$$

Consequently

$$\lambda(E/F,\psi_F)=\prod_{\mu\in T}\Delta(\mu',\psi_{F_\mu/F})\,\lambda(F_\mu/F,\psi_F).$$

In general, we define

$$\lambda(E/F, \psi_F) = \prod\nolimits_{\mu \in T} \Delta(\mu', \psi_{F_\mu/F})\, \lambda(F_\mu/F, \psi_F)$$

if E/F is in $\mathcal{P}_0(K/F)$ T is, of course, not always uniquely determined. We may replace any μ in T by μ^σ with σ in H. Then H_μ and G_μ are replaced by $\sigma^{-1}H_\mu\sigma$ and $\sigma^{-1}G_\mu\sigma$ while F_μ is replaced by F_μ^σ and μ' is replaced by $(\mu')^\sigma$. Since

$$\Delta(\mu', \psi_{F_\mu/F})\, \lambda(F_\mu/F, \psi_F) = \Delta((\mu')^\sigma, \psi_{F_\mu^\sigma/F})\, \lambda(F_\mu^\sigma/F, \psi_F)$$

the number $\lambda(E/F, \psi_F)$ does not depend on T. *A priori*, it may depend on C but that is unimportant since C is fixed and, the uniqueness having been proved, we are interested only in the existence of a λ-function.

We shall need only one property of the function just defined.

Lemma 16.3

If $F \subseteq E \subseteq E' \subseteq K$ *then*

$$\lambda(E'/F, \psi_F) = \lambda(E'/E, \psi_{E/F})\, \lambda(E/F, \psi_F)^{[E':E]}.$$

If $E = F$ then

$$\lambda(E'/E, \psi_{E/F}) = \lambda(E'/F, \psi_F)$$

and if $E \neq F$

$$\lambda(E'/E, \psi_{E/F})$$

is the value of the λ-function of $\mathcal{P}(K/E)$, which is defined by assumption, at E'/E. Since

$$\lambda(F/F, \psi_F) = 1$$

the assertion is clear if $E = F$. It is also clear if $E = E'$.

Let E be the fixed field of H as before and let F' be the fixed field of HC. We suppose that $H \neq G$. Lemma 4.5 and the induction assumption imply that

$$\lambda(F_\mu/F, \psi_F) = \lambda(F_\mu/F', \psi_{F'/F})\, \lambda(F'/F, \psi_F)^{[F_\mu:F']}.$$

The relation

$$[E : F'] = \sum [F_\mu : F']$$

implies that

$$\lambda(E/F, \psi_F) = \lambda(E/F', \psi_{F'/F})\, \lambda(F'/F, \psi_F)^{[E:F']}.$$

There is a similar formula for $\lambda(E'/F, \psi_F)$. If $F' \neq F$ the induction assumption implies that

$$\lambda(E'/E, \psi_{E/F})\, \lambda(E/F', \psi_{F'/F})^{[E':E]} = \lambda(E'/F', \psi_{F'/F}).$$

Since

$$[E' : F'] = [E' : E]\,[E : F']$$

the assertion of the lemma is proved simply by multiplying both sides of this equation by

$$\lambda(F'/F,\psi_F)^{[E':F']}.$$

Now suppose that $G = HC$ and $H \cap C = \{1\}$. Let E' be the fixed field of H' and let F' be the fixed field of $H'C = G'$. Each character of H' may be identified with a character of $C_{E'}/N_{K/E'}C_K$ and each character of G' may be identified with a character of $C_{F'}/N_{K/F'}C_K$. Any character $\chi_{E'}$ of H' may be extended to a character $\chi_{F'}$ of G' by setting

$$\chi_{F'}(\rho\sigma) = \chi_{E'(\rho)}$$

if $\rho \in H'$ and $\sigma \in C$. Then

$$\chi_{E'} = \chi_{E'/F'}.$$

It follows from Lemma 15.1 that there are fields of $F_i(E')$, $1 \leq i \leq m(E')$, lying between F' and L and characters $\mu_{F_i(E')}$ such that

$$\mathrm{Ind}(W_{K/F'}, W_{K/E'}, \chi_{E'})$$

is equivalent to

$$\oplus_{i=1}^{m(E')}\mathrm{Ind}(W_{K/F'}, W_{K/F_i(E')}, \mu_{F_i(E')}\chi_{F_i(E')/F'}).$$

If $E \neq E'$ so that $F \neq F'$ the induction assumption implies that

$$\Delta(\chi_{E'},\psi_{E'/F})\,\lambda(E'/F',\psi_{F'/F})$$

is equal to

$$\prod_{i=1}^{m(E')} \Delta(\mu_{F_i(E')}\chi_{F_i(E')/F'},\psi_{F_i(E')/F})\,\lambda(F_i(E)/F',\psi_{F'/F}).$$

We have seen that the lemma is valid for any pair E', E for which $HC \neq G$. In particular, it is valid for the pair E', F' and the pairs $F_i(E'), F'$. Multiplying the equality just obtained by

$$\lambda(F'/F,\psi_F)^{[E':F']}$$

we see that

$$\Delta(\chi_{E'},\psi_{E'/F})\,\lambda(E'/F,\psi_F) \tag{16.1}$$

is equal to

$$\prod_{i=1}^{m(E')} \Delta(\mu_{F_i(E')}\chi_{F_i(E')/F'},\psi_{F_i(E')/F})\,\lambda(F_i(E')/F,\psi_F). \tag{16.2}$$

If $F' = F$ the equality of (16.1) and (16.2), for a suitable choice of the fields $F_i(E')$, results from Lemma 15.1, Lemma 15.3, and the definition of

$$\lambda(E'/F,\psi_F).$$

In any case the equality is valid for all fields lying between E and K.

Suppose $E_1,\ldots,E_r,\ E'_1,\ldots,E'_s$ are such fields, χ_{E_i} is a character of $C_{E_i}/N_{K/E_i}C_K, \chi_{E'_j}$ is a character of $C_{E'_j}/N_{K/E'_j}C_K$, and

$$\oplus_{i=1}^{r}\mathrm{Ind}(W_{K/E}, W_{K/E_i}, \chi_{E_i})$$

is equivalent to

$$\oplus_{j=1}^{s}\mathrm{Ind}(W_{K/E}, W_{K/E'_j}, \chi_{E'_j}).$$

Then

$$\sum\nolimits_{i=1}^{r}[E_i : E] = \sum\nolimits_{j=1}^{s}[E'_j : E] \tag{16.3}$$

and, by the transitivity of the induction process,

$$\oplus_{i=1}^{r} \oplus_{k=1}^{m(E_i)} \mathrm{Ind}(W_{K/F}, W_{K/F_k(E_i)}, \mu_{F_k(E_i)}\, \chi_{F_k(E_i)/F_i})$$

is equivalent to

$$\oplus_{j=1}^{s} \oplus_{\ell=1}^{m(E'_j)} \mathrm{Ind}(W_{K/F}, W_{K/F_\ell(E'_j)}, \mu_{F_\ell(E'_j)}\, \chi_{F_\ell(E'_j)/F'_j}).$$

If E_i is the fixed field of H_i and E'_j the fixed field of H'_j then F_i and F'_j are the fixed fields of H_iC and H'_jC. This equivalence and the induction assumption for L/F imply that

$$\prod\nolimits_{i=1}^{r}\prod\nolimits_{k=1}^{m(E_i)} \Delta(\mu_{F_k(E_i)}\, \chi_{F_k(E_i)/F_i}, \psi_{F_k(E_i)/F})\, \lambda(F_k(E_i)/F, \psi_F)$$

is equal to

$$\prod\nolimits_{j=1}^{s}\prod\nolimits_{\ell=1}^{m(E'_j)} \Delta(\mu_{F_\ell(E'_j)}\, \chi_{F_\ell(E'_j)/F'_j}, \psi_{F_\ell(E'_j)/F})\, \lambda(F_\ell(E'_j)/F, \psi_F).$$

This equality, the equality of (16.1) and (16.2), and the relation (16.3) imply that

$$\prod\nolimits_{i=1}^{r} \Delta(\chi_{E_i}, \psi_{E_i/F})\, \lambda(E_i/F, \psi_F)\, \lambda(E/F, \psi_F)^{-[E_i:E]}$$

is equal to

$$\prod\nolimits_{j=1}^{s} \Delta(\chi_{E'_j}, \psi_{E'_j/F})\, \lambda(E'_j/F, \psi_F)\, \lambda(E/F, \psi_F)^{-[E'_j:E]}.$$

Consequently

$$E' \longrightarrow \lambda(E'/F, \psi_F)\, \lambda(E/F, \psi_F)^{-[E':E]}$$

is a weak λ-function on $\mathcal{P}_0(K/E)$. The lemma of uniqueness implies that

$$\lambda(E'/F, \psi_F)\, \lambda(E/F, \psi_F)^{-[E':E]} = \lambda(E'/E, \psi_{E/F}).$$

This is, of course, the assertion of the lemma.

At this point, we have proved the lemma when various supplementary conditions are satisfied. Before proving it, in general, we make an observation. Suppose

$$F \subseteq E \subseteq E' \subseteq E'' \subseteq K$$

and the assertion of the lemma is valid for E''/E' and E'/E. Then

$$\lambda(E''/F, \psi_F) = \lambda(E''/E', \psi_{E'/F})\, \lambda(E'/F, \psi_F)^{[E'':E']}$$

and

$$\lambda(E'/F, \psi_F) = \lambda(E'/E, \psi_{E/F})\, \lambda(E/F, \psi_F)^{[E':E]}.$$

Moreover, by induction,

$$\lambda(E''/E, \psi_{E/F}) = \lambda(E''/E', \psi_{E'/F})\, \lambda(E'/E, \psi_{E/F})^{[E'':E']}.$$

The assertion for E''/E is obtained by substituting the second relation in the first and simplifying according to the third.

If the lemma is false in general, chose amongst all the extensions in $\mathcal{P}(K/F)$ for which it is false one E'/E for which $[E' : E]$ is a minimum. Let E be the fixed field of H and E' that of H'. According to the previous discussion $G = HC,\ H \cap C \neq \{1\}$, and there are no fields lying between E and E'. If $H' \cap C = H \cap C$, which is a normal subgroup of G, the fields $F,\ E$, and E' are contained in the fixed field of $H \cap C$ and the assertion is a consequence of the induction assumption. Thus H' is a proper subgroup of $H'(H \cap C)$. Because there are no intermediate fields $H = H'(H \cap C)$.

As we have seen there are fields $E_1, \ldots, E_r$ lying between E and the fixed field K_1 of $H \cap C$ and characters $\mu_{E_1}, \ldots, \mu_{E_r}$ such that

$$\mathrm{Ind}(W_{K/E}, W_{K/E'}, 1)$$

is equivalent to

$$\oplus_{i=1}^{r} \mathrm{Ind}(W_{K/E}, W_{K/E_i}, \mu_{E_i}).$$

Then

$$\lambda(E'/E, \psi_{E/F}) = \prod\nolimits_{i=1}^{r} \Delta(\mu_{E_i}, \psi_{E_i/E})\, \lambda(E_i/E, \psi_{E/F}).$$

By the induction assumption, applied to K_1/F,

$$\lambda(E_i/E, \psi_{E/F})\, \lambda(E/F, \psi_F)^{[E_i:E]} = \lambda(E_i/F, \psi_F).$$

Thus

$$\lambda(E'/E, \psi_{E/F})\, \lambda(E/F, \psi_F)^{[E':E]}$$

is equal to

$$\prod\nolimits_{i=1}^{r} \Delta(\mu_{E_i}, \psi_{E_i/E})\, \lambda(E_i/F, \psi_F). \tag{16.4}$$

Moreover, by the transitivity of the induction process,

$$\mathrm{Ind}(W_{K/F}, W_{K/E'}, 1) \tag{16.5}$$

is equivalent to

$$\oplus_{i=1}^{r} \mathrm{Ind}(W_{K/F}, W_{K/E_i}, \mu_{E_i}). \tag{16.6}$$

On the other hand, there are fields $F_1, \ldots, F_s$ contained in L and characters $\nu_{F_1}, \ldots, \nu_{F_s}$ such that (16.5) is equivalent to

$$\oplus_{j=1}^{s} \mathrm{Ind}(W_{K/F}, W_{K/F_j}, \nu_{F_j}) \tag{16.7}$$

and such that, by definition,

$$\lambda(E'/F, \psi_F) = \prod\nolimits_{j=1}^{s} \Delta(\nu_{F_j}, \psi_{F_j/F})\, \lambda(F_j/F, \psi_F). \tag{16.8}$$

Since the representations (16.6) and (16.7) are equivalent the induction assumption, applied to K_1/F, shows that (16.4) is equal to the right side of (16.8). This is a contradiction.

Chapter Seventeen.

A Simplification.

We shall use the symbol Ω to denote an orbit in the set of quasi-characters of C_K under the action of $\mathfrak{G}(K/F)$ or, what is the same, under the action of $W_{K/F}$ on C_K by means of inner automorphisms. If χ_K is a quasi-character of C_K its orbit will be denoted $\Omega(\chi_K)$. If ρ is a representation of $W_{K/F}$ the restriction of ρ to C_K is the direct sum of one-dimensional representations. Let $S(\rho)$ be the collection of quasi-characters to which these one-dimensional representations correspond.

Suppose
$$\rho = \mathrm{Ind}(W_{K/F}, W_{K/E}, \chi_E).$$
Let $W_{K/F}$ be the disjoint union
$$\bigcup_{i=1}^{m} W_{K/E} w_i.$$
Define the function φ_i by

$$\begin{aligned} &\varphi_i(ww_j) = 0 && w \in W_{K/E},\ \ j \neq i \\ &\varphi_i(ww_i) = \chi_E(\tau_{K/E} w) && w \in W_{K/E}. \end{aligned}$$

$\{\varphi_1, \dots, \varphi_m\}$ is a basis for the space of functions of which ρ acts. If $a \in C_K$ then

$$ww_j a = w(w_j a w_j^{-1}) w_j$$

and $w_j a w_j^{-1}$ belongs to C_K which, of course, lies in $W_{K/E}$. Thus

$$\rho(a)\varphi_i = \chi_E(\tau_{K/E}(w_i a w_i^{-1}))\varphi_i = \chi_{K/E}^{\sigma_i}(a)\varphi_i$$

if σ_i is the image of w_i in $\mathfrak{G}(K/F)$. Thus

$$S(\rho) = \Omega(\chi_{K/E}).$$

Suppose $E_1, \dots, E_r,\ E_1', \dots, E_s'$ lie between F and K, χ_{E_i} is a quasi-character of E_i, and $\chi_{E_j'}$ is a quasi-character of E_j'. Let
$$\rho_i = \mathrm{Ind}(W_{K/F}, W_{K/E_i}, \chi_{E_i})$$
and let
$$\rho_j' = \mathrm{Ind}(W_{K/F}, W_{K/E_j'}, \chi_{E_j'}).$$
Suppose ρ_i acts on V_i and ρ_j' acts on V_j'. The direct sum of the representations ρ_i acts on

$$V = \oplus_{i=1}^{r} V_i$$

and the direct sum of the representations ρ_j' acts on

$$V' = \oplus_{j=1}^{s} V_j'.$$

Let

$$V_\Omega = \oplus_{\{i\,|\,\chi_{K/E_i}\in\Omega\}} V_i$$
$$V'_\Omega = \oplus_{\{i\,|\,\chi_{K/E'_j}\in\Omega\}} V'_j.$$

Any isomorphism of V with V' which commutes with the action of $W_{K/F}$ takes V_Ω to V'_Ω.

If $\chi_{K/E_i} \in \Omega(\chi_K)$ there is a σ in $\mathfrak{G}(K/F)$ such that $\chi_K = \chi^\sigma_{K/E_i}$. Then

$$\rho_i \simeq \mathrm{Ind}(W_{K/F}, W_{K/E_i^\sigma}, \chi^\sigma_{E_i})$$

and

$$\Delta(\chi_{E_i}, \psi_{E_i/F})\,\lambda(E_i/F, \psi_F) = \Delta(\chi^\sigma_{E_i}, \psi_{E_i^\sigma/F})\,\lambda(E_i^\sigma/F, \psi_F).$$

We conclude that Theorem 2.1 is a consequence of the following lemma.

Lemma 17.1

Suppose χ_K is a quasi-character of C_K. Suppose $E_1, \ldots, E_r,\ E'_1, \ldots, E'_s$ lie between F and K, χ_{E_i} is a quasi-character of C_{E_i}, $\chi_{E'_j}$ is a quasi-character of $C_{E'_j}$, and

$$\rho = \oplus_{i=1}^r \mathrm{Ind}(W_{K/F}, W_{K/E_i}, \chi_{E_i})$$

is equivalent to

$$\rho' = \oplus_{j=1}^s\ \mathrm{Ind}(W_{K/F}, W_{K/E'_j}, \chi_{E'_j}).$$

If $\chi_{K/E_i} = \chi_{K/E'_j} = \chi_K$ for all i and j then

$$\prod\nolimits_{i=1}^r \Delta(\chi_{E_i}, \psi_{E_i/F})\,\lambda(E_i/F, \psi_F)$$

is equal to

$$\prod\nolimits_{j=1}^s \Delta(\chi_{E'_j}, \psi_{E'_j/F}),\ \lambda(E'_j/F, \psi_F).$$

Let $F(\chi_K)$ be the fixed field of the isotropy group of χ_K. Let ρ act on V and let ρ' act on V'. Let

$$V(\chi_K) = \{v \in V \mid \rho(a)v = \chi_K(a)v \ \text{ for all } \ a \ \text{ in } \ C_K\}.$$

Define $V'(\chi_K)$ in a similar fashion. It is clear that any isomorphism of V with V' which commutes with the action of $W_{K/F}$ takes $V(\chi_K)$ to $V'(\chi_K)$. The group $W_{K/F(\chi_K)}$ leaves both $V(\chi_K)$ and $V'(\chi_K)$ invariant and its representations on these two spaces are equivalent.

Let

$$\mathrm{Ind}(W_{K/F}, W_{K/E_i}, \chi_{E_i})$$

acts on V_i and define $V_i(\chi_K)$ in the obvious manner. Then

$$V(\chi_K) = \oplus_{i=1}^r V_i(\chi_K).$$

Defining V_j' and $V_j'(\chi_K)$ in a similar manner, we have

$$V'(\chi_K) = \oplus_{j=1}^{s} V_j'(\chi_K).$$

It is clear that the representation of $W_{K/F(\chi_K)}$ on $V_i(\chi_K)$ is equivalent to

$$\mathrm{Ind}(W_{K/F(\chi_K)}, W_{K/E_i}, \chi_{E_i}).$$

Thus

$$\oplus_{i=1}^{r} \mathrm{Ind}(W_{K/F(\chi_K)}, W_{K/E_i}, \chi_{E_i})$$

is equivalent to

$$\oplus_{j=1}^{s} \mathrm{Ind}(W_{K/F(\chi_K)}, W_{K/E_j'}, \chi_{E_j'}).$$

If $F(\chi_K) \neq F$ the assertion of the lemma follows from the induction assumption and Lemma 16.3.

Chapter Eighteen.

Nilpotent Groups.

In this paragraph we prove Lemma 17.1 assuming that $F = F(\chi_K)$ and that $G = \mathfrak{G}(K/F)$ is nilpotent.

Lemma 18.1

Suppose D is a normal subgroup of G of prime order ℓ which is contained in the center of G. Let M be the fixed field of D. Suppose $F \subseteq E \subseteq K$ and χ_E is a quasi-character of C_E. Suppose also that $F(\chi_{K/E}) = F$.

(a) *There are fields $F_1, \ldots, F_r$ contained in M and quasi-characters $\chi_{F_1}, \ldots, \chi_{F_r}$ such that $\chi_{K/F_i} = \chi_{K/E}$ and such that*

$$\mathrm{Ind}(W_{K/F}, W_{K/E}, \chi_E)$$

is equivalent to

$$\oplus_{i=1}^r \mathrm{Ind}(W_{K/F}, W_{K/F_i}, \chi_{F_i}).$$

(b) *If Theorem 2.1 is valid for all Galois extensions K'/F' in $\mathcal{P}(K/F)$ with $[K' : F'] < [K : F]$ then*

$$\Delta(\chi_E, \psi_{E/F})\, \lambda(E/F, \psi_F)$$

is equal to

$$\prod_{i=1}^r \Delta(\chi_{F_i}, \psi_{F_i/F})\, \lambda(F_i/F, \psi_F).$$

We prove the lemma by induction on $[K : F]$. Let H be the subgroup of G corresponding to E; let $G' = HD$ and let F' be the fixed field of G'. If $F' \neq F$ the induction assumption implies that there are fields $F_1, \ldots, F_r$ contained in M and quasi-characters $\chi_{F_1}, \ldots, \chi_{F_r}$ such that $\chi_{K/F_i} = \chi_{K/E}$ for each i and such that

$$\mathrm{Ind}(W_{K/F}, W_{K/E}, \chi_E)$$

is equivalent to

$$\oplus_{i=1}^r \mathrm{Ind}(W_{K/F'}, W_{K/F_i}, \chi_{F_i}).$$

The first part of the lemma follows from the transitivity of the induction process. The second part follows from Lemma 16.3 and the assumed validity of Theorem 2.1 for the extension K/F'.

We suppose now that $G = HD$. Suppose that H contains a normal subgroup H_1 of G which is different from $\{1\}$ and suppose that, if K_1 is the fixed field of H_1, $F(\chi_{K_1/E}) = F$. If M_1 is the fixed field of $H_1 D$ then, according to the induction assumption, there are fields $F_1, \ldots, F_r$ contained in M_1 and quasi-characters $\chi_{F_1}, \ldots, \chi_{F_r}$ such that

$$\chi_{K_1/F_i} = \chi_{K_1/E}$$

and such that

$$\mathrm{Ind}(W_{K_1/F}, W_{K_1/E}, \chi_E)$$

is equivalent to

$$\oplus_{i=1}^{r}\mathrm{Ind}(W_{K_1/F}, W_{K_1/F_i}, \chi_{F_i}).$$

It follows immediately that

$$\chi_{K/F_i} = \chi_{K/E}$$

and that

$$\mathrm{Ind}(W_{K/F}, W_{K/E}, \chi_E)$$

is equivalent to

$$\oplus_{i=1}^{r}\mathrm{Ind}(W_{K/F}, W_{K/F_i}, \chi_{F_i}).$$

The equality of (b) is a consequence of the assumed validity of Theorem 2.1 for K_1/F.

We assume now that $G = HD$ and that if H_1 is a normal subgroup of H different from $\{1\}$ with fixed field K_1 the field $F(\chi_{K_1/E})$ is not F. If w_1 belongs to $W_{K/E}$ and w_2 belongs to $W_{K/M}$ then

$$w_1 w_2 w_1^{-1} w_2^{-1} \in C_K.$$

Let $\chi_K = \chi_{K/E}$. Since $F(\chi_K) = F$

$$\chi_K(w_1 w_2 w_1^{-1} w_2^{-1}) = \chi_K(w_2 w_1^{-1} w_2^{-1} w_1) = \chi_K(w_1^{-1} w_2^{-1} w_1 w_2) = \chi_K(w_2^{-1} w_1 w_2 w_1^{-1}).$$

Denote the common value of the expressions by $\omega(w_1, w_2)$. Then $\omega(v_1 w_1, w_2)$ is equal to

$$\chi_K(v_1 w_1 w_2 w_1^{-1} v_1^{-1} w_2^{-1}) = \chi_K(w_2^{-1} w_1 w_2 w_1^{-1} v_1^{-1} w_2^{-1} v_1 w_2).$$

The right side is

$$\omega(v_1, w_2)\ \omega(w_1, w_2).$$

In the same way $\omega(w_1, v_2 w_2)$ is

$$\chi_K(w_1 v_2 w_2 w_1^{-1} w_2^{-1} v_2^{-1}) = \chi_K(w_1^{-1} v_2^{-1} w_1 v_2 w_2 w_1^{-1} w_2^{-1} w_1)$$

which equals

$$\omega(w_1, v_2)\ \omega(w_1, w_2).$$

If either w_1 or w_2 belong to C_K, we have

$$\omega(w_1, w_2) = 1.$$

Thus, for each w_2,

$$w_1 \longrightarrow \omega(w_1, w_2)$$

is a homomorphism of $H = W_{K/E}/C_K$ into $\mathbb{C}^*$ and, for each w_1,

$$w_2 \longrightarrow \omega(w_1, w_2)$$

is a homomorphism of $D = W_{K/M}/C_K$ into $\mathbb{C}^*$. If w belongs to $W_{K/F}$ then

$$\omega(w w_1 w^{-1},\ w w_2 w^{-1}) = \omega(w_1, w_2).$$

Thus there is a normal extension K_1 containing E such that

$$W_{K/K_1} = \{w_1 \mid \omega(w_1, w_2) = 1 \text{ for all } w_1 \in W_{K/M}\}.$$

But $F(\chi_{K_1/E})$ will be F so that K_1 must be K.

It follows immediately that H is isomorphic to a subgroup of the dual group of D. Thus $H = \{1\}$ or H is cyclic of order ℓ. In either case H must lie in the centralizer of D so that E/F is normal and $\mathfrak{G}(E/F)$ is isomorphic to D. If $H = \{1\}$ then χ_E may be extended from $C_E = C_K$ to a quasi-character of $W_{E/F}$. In other words, there is a quasi-character χ_F of C_F such that $\chi_E = \chi_{E/F}$. Then

$$\operatorname{Ind}(W_{K/F}, W_{K/E}, \chi_E)$$

is equivalent to

$$\oplus_{\mu_F \in S(E/F)} \operatorname{Ind}(W_{K/F}, W_{K/F}, \mu_F \chi_F).$$

Suppose $H \neq \{1\}$. Since $W_{K/M}/C_K$ is cyclic there is a quasi-character χ_M of C_M such that $\chi_K = \chi_{K/M}$. If w_1 belongs to $W_{K/E}$ let χ_{w_1} be the character of $W_{K/M}$ or, what is the same, of C_M defined by

$$\chi_{w_1}(w_2) = \omega(w_1, w_2)$$

and if w_2 belongs to $W_{K/M}$ let

$$\chi_{w_2}(w_1) = \omega(w_1, w_2).$$

Clearly

$$\{\chi_{w_1} \mid w_1 \in W_{K/E}\} = S(K/M)$$

and

$$\{\chi_{w_2} \mid w_2 \in W_{K/M}\} = S(K/E).$$

If σ_1 is the image of w_1 in H and σ_2 the image of w_2 in D then

$$\chi_E^{\sigma_2}(w_1) = \chi_E(w_2 w_1 w_2^{-1} w_1^{-1} w_1) = \chi_{w_2}^{-1}(w_1)\, \chi_E(w_1)$$

and

$$\chi_M^{\sigma_1}(w_2) = \chi_M(w_1 w_2 w_1^{-1} w_2^{-1} w_2) = \chi_{w_1}(w_2)\, \chi_M(w_2).$$

Let $W_{K/F}$ be the disjoint union

$$\bigcup_{i=1}^{\ell} W_{K/E} v_i$$

with v_i in $W_{K/M}$. Define the function φ_i on $W_{K/F}$ by

$$\varphi_i(w v_j) = 0$$

if $w \in W_{K/E}$ and $j \neq i$ and by

$$\varphi_i(w v_i) = \chi_E(w)$$

if $w \in W_{K/E}$. Then

$$\{\varphi_i \mid 1 \leq i \leq \ell\}$$

is a basis for the space U on which

$$\operatorname{Ind}(W_{K/F}, W_{K/E}, \chi_E)$$

acts. Let $\psi_i,\ 1 \le i \le \ell$ be the function $W_{K/F}$ defined by

$$\psi_i(w_2 w_1) = \chi_M(w_2)\chi_E^{\sigma(v_i)}(w_1)$$

if w_1 belongs to $W_{K/E}$ and w_2 belongs to $W_{K/M}$. Here $\sigma(v_i)$ is the image of v_i in $\mathfrak{G}(K/F)$. It is necessary, but easy, to verify that ψ_i is well-defined. The collection

$$\{\psi_i \mid 1 \le i \le \ell\}$$

is a basis for the space V on which

$$\mathrm{Ind}(W_{K/F}, W_{K/M}, \chi_M)$$

acts. It is easily verified that the isomorphism of U with V which sends $\chi_M(v_i)\varphi_i$ to ψ_i is an isomorphism. Thus

$$\mathrm{Ind}(W_{K/F}, W_{K/E}, \chi_E) \simeq \mathrm{Ind}(W_{K/F}, W_{K/M}, \chi_M).$$

This takes care of the first part of the lemma.

Whether $H = \{1\}$ or not,

$$\mathrm{Ind}(W_{K/F}, W_{K/E}, 1)$$

is equivalent to

$$\oplus_{\mu_F \in S(E/F)} \mathrm{Ind}(W_{K/F}, W_{K/F}, \mu_F).$$

If $H \ne 1$ we may apply Theorem 2.1 to E/F to see that

$$\lambda(E/F, \psi_F) = \prod\nolimits_{\mu_F \in S(E/F)} \Delta(\mu_F, \psi_F).$$

If $H = \{1\}$ this equality is just the definition of the left side. In this case the second part of the lemma asserts that

$$\Delta(\chi_E, \psi_{E/F}) \ \prod\nolimits_{\mu_F \in S(E/F)} \Delta(\mu_F, \psi_F) \tag{18.1}$$

is equal to

$$\prod\nolimits_{\mu_F \in S(E/F)} \Delta(\mu_F \chi_F,\ \psi_F)$$

where $\chi_E = \chi_{E/F}$. This is a consequence of the first main lemma. If $H \ne \{1\}$, Theorem 2.1 applied to M/F, shows that

$$\lambda(M/F, \psi_F) = \prod\nolimits_{\mu_F \in S(M/F)} \Delta(\mu_F, \psi_F)$$

and the second part of the lemma asserts that (18.1) is equal to

$$\Delta(\chi_M, \psi_{M/F}) \prod\nolimits_{\mu_F \in S(M/F)} \Delta(\mu_F, \psi_F).$$

This is a consequence of the second main lemma.

A non-trivial nilpotent group always contains a subgroup D satisfying the conditions of the previous lemma. Lemma 17.1 is clear if $K = F$. If $K \ne F$ and $\mathfrak{G}(K/F)$ is nilpotent it is a consequence of the following lemma.

Lemma 18.2

Suppose K/F is normal and Theorem 2.1 is valid for all normal extensions K'/F' in $\mathcal{P}(K/F)$ with $[K' : F'] < [K : F]$. Suppose $F \subseteq M \underset{\neq}{\subset} K$ and M/F is normal. Suppose $E_1, \ldots, E_r$, $E'_1, \ldots, E'_s$ lie between F and M, χ_{E_i} is a quasi-character of C_{E_i}, $\chi_{E'_j}$ is a quasi-character of $C_{E'_j}$, and

$$\oplus_{i=1}^r \mathrm{Ind}(W_{K/F}, W_{K/E_i}, \chi_{E_i})$$

is equivalent to

$$\oplus_{j=1}^s \mathrm{Ind}(W_{K/F}, W_{K/E'_j}, \chi_{E'_j}).$$

Then

$$\prod_{i=1}^r \Delta(\chi_{E_i}, \psi_{E_i/F})\, \lambda(E_i/F, \psi_F)$$

is equal to

$$\prod_{j=1}^s \Delta(\chi_{E'_j}, \psi_{E'_j/F})\, \lambda(E'_j/F, \psi_F).$$

The representation

$$\mathrm{Ind}(W_{K/F}, W_{K/E_i}, \chi_{E_i})$$

can be obtained by inflating the representation

$$\mathrm{Ind}(W_{M/F}, W_{M/E_i}, \chi_{E_i})$$

from $W_{M/F}$ to $W_{K/F}$. A similar remark applies to the representations induced from the $\chi_{E'_j}$. Thus

$$\oplus_{i=1}^r \mathrm{Ind}(W_{M/F}, W_{M/E_i}, \chi_{E_i})$$

is equivalent to

$$\oplus_{j=1}^s \mathrm{Ind}(W_{M/F}, W_{M/E'_j}, \chi_{E'_j}).$$

Applying Theorem 2.1 to the extension M/F we obtain the lemma.

Chapter Nineteen.

Proof of the Main Theorem.

We shall first prove Lemma 17.1 when there is a quasi-character χ_F of C_F such that $\chi_K = \chi_{K/F}$. Implicit in the statement of the following lemma as in that of Lemma 17.1, is the assumption that Theorem 2.1 is valid for all pairs K'/F' in $\mathcal{P}(K/F)$ for which $[K':F'] < [K:F]$. Recall that we have fixed a non-trivial abelian normal subgroup C of $G = \mathfrak{G}(K/F)$ and that L is its fixed field.

Lemma 19.1

Suppose $F \subseteq E \subseteq K$, χ_F is a quasi-character of C_F, χ_E is a quasi-character if C_E, and $\chi_{K/E} = \chi_{K/F}$. There are fields $F_1, \ldots, F_r$ contained in L and quasi-characters χ_{F_i}, $1 \le i \le r$, such that $\chi_{K/F_i} = \chi_{K/F}$,

$$\mathrm{Ind}(W_{K/F}, W_{K/E}, \chi_E)$$

is equivalent to

$$\oplus_{i=1}^r \mathrm{Ind}(W_{K/F}, W_{K/F_i}, \chi_{F_i})$$

and

$$\Delta(\chi_E, \psi_{E/F})\,\lambda(E/F, \psi_F)$$

is equal to

$$\prod_{i=1}^r \Delta(\chi_{F_i}, \psi_{F_i/F})\,\lambda(F_i/F, \psi_F).$$

We prove the lemma by induction on $[K:F]$. Let E be the fixed field of H and let F' be the fixed field of HC. If $F' \neq F$ then, by induction, there are fields $F_1, \ldots, F_r$ lying between F' and L and quasi-characters $\chi_{F_1}, \ldots, \chi_{F_r}$ such that $\chi_{K/F_i} = \chi_{K/F}$ and

$$\mathrm{Ind}(W_{K/F'}, W_{K/E}, \chi_E)$$

is equivalent to

$$\oplus_{i=1}^r \mathrm{Ind}(W_{K/F'}, W_{K/F_i}, \chi_{F_i}).$$

In this case the lemma follows from the transitivity of the induction process, the assumed validity of Theorem 2.1 for K/F' and Lemma 16.3.

We suppose henceforth that $G = HC$. There is a character θ_E in $S(K/E)$ such that $\chi_E = \theta_E \chi_{E/F}$. θ_E may be regarded as a character of H. If $H \cap C = \{1\}$ we may define a character θ_F of G by setting

$$\theta_F(hc) = \theta_E(h)$$

if h is in H and c is in C. θ_F may be regarded as a character of C_F and $\theta_E = \theta_{E/F}$. Replacing χ_F by $\theta_F\,\chi_F$ we suppose that $\chi_E = \chi_{E/F}$. Then in the notation of Lemma 15.1, we may take

$$\{F_1, \ldots, F_r\} = \{F_\mu \mid \mu \in T\}$$

and if $F_i = F_\mu$,

$$\chi_{F_i} = \mu' \chi_{F_\mu/F}.$$

The assertions of the lemma are consequences of Lemmas 15.1 and 15.3.

We suppose now not only that $G = HC$ but also that $H \cap C \neq \{1\}$. Let S be the set of characters in $S(K/L)$ whose restriction to $H \cap C$ agrees with the restriction of θ_E. S is invariant under the action of H on $S(K/L)$. If ν belongs to S let φ_ν be the function on $W_{K/F}$ defined by

$$\varphi_\nu(wv) = \chi_E(w)\,\chi_{L/F}(v)\;\nu(v)$$

if w is in $W_{K/E}$ and v is in $W_{K/L}$. ν is a character of C and may therefore be regarded as a character of $W_{K/L}$ or of C_L. It is easy to verify that φ_ν is well-defined. If

$$\rho = \mathrm{Ind}(W_{K/F}, W_{K/E}, \chi_E)$$

then

$$\{\varphi_\nu \mid \nu \in S\}$$

is a basis for the space of functions on which ρ acts. If w belongs to $W_{K/E}$

$$\rho(w)\varphi_\nu = \chi_E(w)\varphi_{\nu'}$$

with $\nu' = \nu^{\sigma^{-1}}$ is σ is the image of w in $\mathfrak{G}(K/F)$. If v belongs to $W_{K/L}$

$$\rho(v)\varphi_\nu = \chi_{L/F}(v)\;\nu(v)\varphi_\nu.$$

Thus if R is an orbit in S under the action of H, the space

$$V_R = \sum\nolimits_{\nu\in R} \mathbb{C}_{\varphi_\nu}$$

is invariant under $W_{K/F}$ and ρ is the direct sum of its restrictions to the spaces V_R.

If μ belongs to R let H_μ be the isotropy group of μ, let $G_\mu = H_\mu C$, and let F_μ be the fixed field of G_μ. Extend μ to a character μ' of G_μ by setting

$$\mu'(hc) = \theta_E(h)\;\mu(c)$$

if h is in H_μ and c is in C. μ', which is easily seen to be well-defined, may be regarded as a character of W_{K/F_μ} of C_{F_μ}. Let $W_{K/F}$ be the disjoint union

$$\bigcup\nolimits_{i=1}^{s} W_{K/F_\mu} w_i$$

with w_i in $W_{K/E}$ and let σ_i be the image of w_i in $\mathfrak{G}(K/F)$. Let φ_i be the function of $W_{K/F}$ defined by

$$\begin{aligned} &\varphi_i(ww_j) = 0 && w \in W_{K/F_\mu},\;\; j \neq i \\ &\varphi_i(ww_i) = \mu'(w)\chi_{F_\mu/F}(w) && w \in W_{K/F_\mu}. \end{aligned}$$

The collection

$$\{\varphi_i \mid 1 \le i \le s\}$$

is a basis for the space V_μ on which the representation

$$\sigma_\mu = \mathrm{Ind}(W_{K/F}, W_{K/F_\mu}, \mu'\chi_{F_\mu/F})$$

acts. Let

$$\psi_i = \chi_E(w_i)\varphi_i.$$

If w belongs to $W_{K/L}$

$$\sigma_\mu(w)\psi_i = \mu^{\sigma_i}(w)\,\chi_{L/F}(w)\psi_i.$$

If w belongs to $W_{K/E}$ and $w_j w = v w_i$ with v in W_{K/F_μ} then

$$\sigma_\mu(w)\psi_i = \chi_E(w)\psi_j.$$

Thus the isomorphism of V_μ with V_R which takes ψ_i to $\varphi_{\mu^{\sigma_i}}$ commutes with the action of $W_{K/F}$. If T is a set of representatives for the orbits in S

$$\rho \simeq \oplus_{\mu\in T}\sigma_\mu.$$

If K_1 is the fixed field of $H\cap C$ then K_1/F is normal and ρ is the inflation to $W_{K/F}$ of

$$\mathrm{Ind}(W_{K_1/F}, W_{K_1/E}, \chi_E) \tag{19.1}$$

and σ_μ is the inflation of

$$\mathrm{Ind}(W_{K_1/F}, W_{K_1/F_\mu}, \mu'\chi_{F_\mu/F}).$$

Thus the representation (19.1) is equivalent to

$$\oplus_{\mu\in T}\mathrm{Ind}(W_{K_1/F}, W_{K_1/F_\mu}, \mu'\chi_{F_\mu/F}).$$

Applying Theorem 2.1 to K_1/F we see that

$$\Delta(\chi_E, \psi_{E/F})\,\lambda(E/F, \psi_F)$$

is equal to

$$\prod\nolimits_{\mu\in T}(\mu'\chi_{F_\mu/F}, \psi_{F_\mu/F})\,\lambda(F_\mu/F, \psi_F).$$

If there is a quasi-character χ_F such that $\chi_K = \chi_{K/F}$, Lemma 17.1 follows from Lemma 18.2 and the lemma just proved. To complete the proof of Theorem 2.1 we have to prove Lemma 17.1 when $F = F(\chi_K)$, G is not nilpotent, and there is no quasi-character χ_F of C_F such that $\chi_K = \chi_{K/F}$. In this case none of the fields $E_1, \dots, E_r,\ E'_1, \dots, E'_s$ is equal to F and Theorem 2.1 may be applied to K/E_i and K/E'_j.

Lemma 19.2

Suppose A and B lie between F and K. Suppose χ_A and χ_B are quasi-characters of C_A and C_B respectively. There are fields $A_1, \dots, A_m$ lying between A and K, fields $B_1, \dots, B_m$ lying between B and K, elements $\sigma_1, \dots, \sigma_m$ in G, and quasi-characters $\chi_{A_1}, \dots, \chi_{A_m},\ \chi_{B_1}, \dots, \chi_{B_m}$ such that $B_i = A_i^{\sigma_i}, \chi_{B_i} = \chi_{A_i}^{\sigma_i}$, and such that the tensor product

$$\mathrm{Ind}(W_{K/F}, W_{K/A}, \chi_A)\ \otimes\ \mathrm{Ind}(W_{K/F}, W_{K/B}, \chi_B)$$

is equivalent to

$$\oplus_{i=1}^m \mathrm{Ind}(W_{K/F}, W_{K/A_i}, \chi_{A_i})$$

and to

$$\oplus_{i=1}^m \mathrm{Ind}(W_{K/F}, W_{K/B_i}, \chi_{B_i}).$$

Let

$$\rho = \mathrm{Ind}(W_{K/F}, W_{K/A}, \chi_A)$$
$$\sigma = \mathrm{Ind}(W_{K/F}, W_{K/B}, \chi_B).$$

Let α be the restriction of σ to $W_{K/A}$ and β the restriction of ρ to $W_{K/B}$. By Lemma 2.3

$$\rho \otimes \sigma \simeq \mathrm{Ind}(W_{K/F}, W_{K/A}, \chi_A \otimes \alpha)$$

and

$$\rho \otimes \sigma \simeq \mathrm{Ind}(W_{K/F}, W_{K/B}, \chi_B \otimes \beta).$$

Let $W_{K/F}$ be the disjoint union

$$\bigcup_{i=1}^m W_{K/A} w_i W_{K/B}.$$

If U_i is the space of functions in U, the space on which ρ acts, which are zero outside of the double coset $W_{K/A} w_i W_{K/B}$ then U_i is invariant under β. Define the field B_i by demanding that

$$W_{K/B_i} = W_{K/B} \cap w_i^{-1} W_{K/A} w_i.$$

If σ_i is the image of w_i in $\mathfrak{G}(K/F)$ let χ'_{B_i} be the restriction of $\chi_A^{\sigma_i}$ to W_{K/B_i}. If U'_i is the space of functions on which

$$\mathrm{Ind}(W_{K/B}, W_{K/B_i}, \chi'_{B_i})$$

acts, the map of U_i to U'_i which sends φ to the function φ' defined by

$$\varphi'(w) = \varphi(w_i w)$$

if w is in $W_{K/B}$ is an isomorphism which commutes with the action of $W_{K/B}$. Thus

$$\beta \simeq \oplus_{i=1}^m \mathrm{Ind}(W_{K/B}, W_{K/B_i}, \chi'_{B_i})$$

and, if $\chi_{B_i} = \chi_{B_i/B}\, \chi'_{B_i}$,

$$\chi_B \otimes \beta \simeq \oplus_{i=1}^m \mathrm{Ind}(W_{K/B}, W_{K/B_i}, \chi_{B_i}).$$

Similar considerations apply if the roles of A and B are interchanged. The double coset decomposition becomes

$$\bigcup_{i=1}^m W_{K/B} w_i^{-1} W_{K/A}$$

and

$$W_{K/A_i} = W_{K/A} \cap w_i W_{K/B} w_i^{-1} = w_i W_{K/B_i} w_i^{-1}.$$

Thus $B_i = A_i^{\sigma_i}$. It is also clear that $\chi_{B_i} = \chi_{A_i}^{\sigma_i}$.

To complete the proof of Lemma 17.1 we use Brauer's theorem in the following form. There are fields $F_1, \ldots, F_n$ lying between F and K such that $\mathfrak{G}(K/F_k)$ is nilpotent for each k, characters χ_{F_k} of $C_{F_k}/N_{K/F_k}C_K$, and integers $m_1, \ldots, m_n$ such that

$$1 \simeq \oplus_{k=1}^{n} m_k \operatorname{Ind}(W_{K/F}, W_{K/F_k}, \chi_{F_k}).$$

Since we are assuming that G is not nilpotent none of the F_k are equal to F and we may apply Theorem 2.1 to each of the extensions K/F_k.

We shall apply the previous lemma with $A = E_i$, $B = F_k$ and with $A = E'_j$, $B = F_k$. m will be denoted by $m(ik)$ or $m'(j\ell)$. A_ℓ will be denoted by $E_{ik\ell}$ or $E'_{jk\ell}$ and B_ℓ will be denoted by $F_{ik\ell}$ or $F'_{jk\ell}$. Observe that

$$\Delta(\chi_{E_{ik\ell}}, \psi_{E_{ik\ell}/F}\, \lambda(E_{ik\ell}/F, \psi_F) \tag{19.2}$$

is equal to

$$\Delta(\chi_{F_{ik\ell}}, \psi_{F_{ik\ell}/F})\, \lambda(F_{ik\ell}/F, \psi_F) \tag{19.3}$$

and that

$$\Delta(\chi_{E'_{jk\ell}}, \psi_{E'_{jk\ell}/F})\, \lambda(E'_{jk\ell}/F, \psi_F) \tag{19.4}$$

is equal to

$$\Delta(\chi_{F'_{jk\ell}}, \psi_{F'_{jk\ell}/F})\, \lambda(F'_{jk\ell}/F, \psi_F). \tag{19.5}$$

χ_{E_i} may be regarded as a one-dimensional representation of W_{K/E_i} and as such is equivalent to

$$\oplus_{k=1}^{n} \oplus_{\ell=1}^{m(ik)} m_k \operatorname{Ind}(W_{K/E_i}, W_{K/E_{ik\ell}}, \chi_{E_{ik\ell}}).$$

Therefore

$$1 = \sum_{k=1}^{n} \sum_{\ell=1}^{m(ik)} m_k\, [E_{ik\ell} : E_i]$$

and

$$\Delta(\chi_{E_i}, \psi_{E_i/F})$$

is equal to

$$\prod_{k=1}^{n} \prod_{\ell=1}^{m(ik)} \{\Delta(\chi_{E_{ik\ell}}, \psi_{E_{ik\ell}/F})\, \lambda(E_{ik\ell}/E_i, \psi_{E_i/F})\}^{m_k}.$$

Multiplying both of these expressions by $\lambda(E_i/F, \psi_F)$, we see that

$$\Delta(\chi_{E_i}, \psi_{E_i/F})\, \lambda(E_i/F, \psi_F) \tag{19.6}$$

is equal to

$$\prod_{k=1}^{n} \prod_{\ell=1}^{m(ik)} \{\Delta(\chi_{E_{ik\ell}}, \psi_{E_{ik\ell}/F})\, \lambda(E_{ik\ell}/F, \psi_F)\}^{m_k}. \tag{19.7}$$

The same argument establishes that

$$\Delta(\chi_{E'_j}, \psi_{E'_j/F})\, \lambda(E'_j/F, \psi_F) \tag{19.8}$$

is equal to

$$\prod_{k=1}^{n} \prod_{\ell=1}^{m'(jk)} \{\Delta(\chi_{E'_{jk\ell}}, \psi_{E'_{jk\ell}/F})\, \lambda(E'_{jk\ell}/F, \psi_F)\}^{m_k}. \tag{19.9}$$

We are trying to show that the product over i of the expressions (19.6) is equal to the product over j of the expressions (19.8). It will be enough to show that the product of the expressions (19.7) is equal to the product of the expressions (19.9).

The representations

$$\oplus_{i=1}^{r} \oplus_{\ell=1}^{m(ik)} \mathrm{Ind}(W_{K/F_k}, W_{K/F_{ik\ell}}, \chi_{F_{ik\ell}})$$

and

$$\oplus_{j=1}^{s} \oplus_{\ell=1}^{m'(jk)} \mathrm{Ind}(W_{K/F_k}, W_{K/F'_{jk\ell}}, \chi_{F'_{jk\ell}})$$

are equivalent. Therefore

$$\sum_{i=1}^{r} \sum_{\ell=1}^{m(ik)} [F_{ik\ell} : F_k] = \sum_{j=1}^{s} \sum_{\ell=1}^{m'(jk)} [F'_{jk\ell} : F_k].$$

Denote the common value of these expressions by $N(k)$. Moreover

$$\prod_{i=1}^{r} \prod_{\ell=1}^{m(ik)} \Delta(\chi_{F_{ik\ell}}, \psi_{F_{ik\ell}/F})\, \lambda(F_{ik\ell}/F_k, \psi_{F_k/F})$$

is equal to

$$\prod_{j=1}^{s} \prod_{\ell=1}^{m'(jk)} \Delta(\chi_{F'_{jk\ell}}, \psi_{F'_{jk\ell}/F})\, \lambda(F'_{jk\ell}/F, \psi_{F_k/F}).$$

Multiplying both of these expressions by

$$\lambda(F_k/F, \psi_F)^{N(k)}$$

we see that

$$\prod_{i=1}^{r} \prod_{\ell=1}^{m(ik)} \Delta(\chi_{F_{ik\ell}}, \psi_{F_{ik\ell}/F})\, \lambda(F_{ik\ell}/F, \psi_F) \tag{19.10}$$

is equal to

$$\prod_{j=1}^{s} \prod_{\ell=1}^{m'(jk)} \Delta(\chi_{F'_{jk\ell}}, \psi_{F'_{jk\ell}/F})\, \lambda(F'_{jk\ell}/F, \psi_F). \tag{19.11}$$

Because of the equality of (19.2) and (19.3) the product over i of the expressions (19.7) is equal to the product over k of of the m_kth powers of the expressions (19.10). The product over j of the expressions (19.9) is equal to the product over k of the m_kth powers of the expressions (19.11). Lemma 17.1, and with it Theorem 2.1, is now completely proved.

Chapter Twenty.

Artin L-functions.

Suppose ω is an equivalence class of representations of the Weil group of the non-archimedean local field F. Let K be a Galois extension of F and let σ be a representation of $W_{K/F}$ in the class ω. Suppose σ acts on V. Let V^0 be the subspace of V fixed by every element of $W^0_{K/F}$. Since $W^0_{K/F}$ is a normal subgroup of $W_{K/F}$ the space V^0 is invariant under $W_{K/F}$ and on V^0 we get a representation σ^0. Since $W^0_{K/F} = \tau^{-1}_{K/F}(u^0_F)$ the class of σ^0 depends only on w. σ^0 breaks up into the direct sum of 1-dimensional representations corresponding to unramified generalized characters $\mu_1, \ldots, \mu_r$ of C_F. We set

$$L(s,w) = \prod\nolimits_{i=1}^{r} \frac{1}{1-\mu_i(\pi_F)\,|\pi_F\,|^s}.$$

This we take as the local function. It is clear that when w is one-dimensional the present definition agrees with that of the introduction and that of $\omega = \omega_1 \oplus \omega_2$. Then

$$L(s,\omega) = L(s,\omega_1) \oplus L(s,\omega_2).$$

Suppose $F \subseteq E \subseteq K$, ρ is a representation of $W_{K/E}$, and

$$\sigma = \operatorname{Ind}(W_{K/F}, W_{K/E}, \rho).$$

We have to show that if θ is the class of ρ then

$$L(s,\omega) = L(s,\theta).$$

Let ρ act on W. Then V is the space of functions f on $W_{K/F}$ with values in W which satisfy

$$f(uv) = \rho(u)f(v)$$

for u in $W_{K/E}$ and v in $W_{K/F}$. If f lies in V_0 and u lies in $W^0_{K/E}$ then

$$\rho(u)f(v) = f(uv) = f(vv^{-1}uv) = f(v)$$

because v^{-1} lies in $W^0_{K/F}$. Thus f takes values in W^0. In other words, we may as well assume that $W = W^0$. Indeed we may as well go further and assume that $W = W^0$ has dimension one.

Let $N_{E/F}\,\pi_E = \varepsilon\pi_F^f$ where ε is a unit and choose w_0 in $W_{K/F}$ so that $\tau_{K/F}w_0 = \pi_F$. Then $w^f = u_0v_0$ with u_0 in $W^0_{K/F}$ and v_0 in $W_{K/E}$ such that $\tau_{K/E}v_0 = \pi_E$. Clearly, V^0 consists of the functions f with values in W which satisfy $f(uw) = f(w)$ for u in $W^0_{K/F}$ and $f(uw) = \mu(\tau_{K/E}u)f(w)$ if ρ is associated to the generalized character μ of C_E. Take as basis of V^0 the functions $\varphi_0, \ldots, \varphi_{f-1}$ defined by

$$\varphi_i(uvw_0^j) = \mu(\tau_{K/E}v)\delta_i^j x$$

where x is a non-zero vector in W, u belongs to $W^0_{K/F}$, v belongs to $W_{K/E}$, $0 \le j < f$, and δ^j_i is Kronecker's delta. The matrix of $\sigma(w_0)$ with respect to this basis is

$$A = \begin{pmatrix} 0 & \cdot & \cdot & \cdot & \mu(\tau_{K/E}v_0) \\ 1 & 0 & & & \cdot \\ & 1 & \ddots & & \cdot \\ & & \ddots & \ddots & \cdot \\ & 0 & & 1 & 0 \end{pmatrix}$$

and

$$L(s,\omega) = \frac{1}{\det(I - A\,|\pi_F|^s)} = \frac{1}{1-\mu(\pi_E)\,|\pi_F|^{fs}} = L(s,\theta)$$

since $|\pi_F|^f = |\pi_E|$.

For archimedean fields we proceed in a different manner. If we write ω, as we may, as a sum of irreducible representations the components are unique up to order. If $\omega = \sum_{i=1}^r \oplus\omega_i$, we will have to have

$$L(s,\omega) = \prod\nolimits_{i=1}^r L(s,\omega_i).$$

Thus it is a matter of defining $L(s,\omega)$ for irreducible ω. If ω is one-dimensional this was done in the introduction. If ω is not one-dimensional then F must be $\mathbb{R}$. Let σ be a representation of $W_{\mathbb{C}/\mathbb{R}}$ in the class ω. $W_{\mathbb{C}/\mathbb{R}}$ is an extension of the group of order 2 by $\mathbb{C}^*$. Let $W_{\mathbb{C}/\mathbb{R}} = \mathbb{C}^\times \cup w_0\mathbb{C}^\times$. If σ acts on V there is a non-zero vector x in V and a generalized character μ of $\mathbb{C}^\times$ such that $\sigma(a)x = \mu(a)x$ for all a in $\mathbb{C}^\times$. Then the space spanned by $\{x, \sigma(w_0)x\}$ is invariant and therefore all of V. Since V is not one-dimensional $\sigma(w_0)x$ is not a multiple of x. Notice that $\sigma(a)\sigma(w_0)x = \sigma(w_0)\sigma(w_0^{-1}aw_0)x = \mu(\overline{a})\sigma(w_0)x$. If

$$\mu(z) = |z|^r\ \frac{z^m\overline{z}^n}{|z|^{\frac{m+n}{2}}}$$

with $m+n \ge 0,\ mn = 0$ we set

$$L(s,\omega) = 2(2\pi)^{-\left(s+r+\frac{m+n}{2}\right)}\ \Gamma\left(s+r+\frac{m+n}{2}\right).$$

The initial choice of μ is of course not uniquely determined. However if μ_0 is one choice the only other choice is the character $a \to \mu_0(\overline{a})$. Thus the resulting local L-function is independent of the choice.

The only point to be checked is that the local L-function behaves properly under induction. We have to verify that if ρ is a representation of $\mathbb{C}^* = W_{\mathbb{C}/\mathbb{C}}$ in the class θ and

$$\sigma = \mathrm{Ind}(W_{\mathbb{C}/\mathbb{R}}, W_{\mathbb{C}/\mathbb{C}}, \rho)$$

is in the class w then $L(s,w) = L(s,\theta)$. We may as well assume that ρ is irreducible and therefore one-dimensional. Let it correspond to the generalized character ν. If σ is irreducible we could choose the generalized character μ above to be ν and the equality of the two L-functions becomes a matter of definition. If σ is irreducible it breaks up into the sum of two one-dimensional representatives. It follows easily that $\nu(a) = \nu(\overline{a})$ for all a. Thus ν is of the form $\nu(a) = |a|^r$ and

$$L(s,\theta) = 2(2\pi)^{-(s+r)}\ \Gamma(s+r).$$

If $\mu_{\mathbb{R}} = \mu$ is the generalized character $x \to |x|^r$ of $\mathbb{R}^\times$ then $\nu = \mu_{\mathbb{C}/\mathbb{R}}$ and, as we saw in chapter 10, the representation σ is equivalent to the direct sum of the one-dimensional representations corresponding to μ and to μ' where $\mu'(x) = \mathrm{sgn} x \mu(x)$. Thus

$$L(s,\omega) = \left\{\pi^{-\frac{1}{2}(s+r)}\ \Gamma\ \left(\frac{s+r}{2}\right)\right\}\left\{\pi^{-\frac{1}{2}(s+r+1)}\ \Gamma\ \left(\frac{s+r+1}{2}\right)\right\}.$$

The required result is thus a consequence of the familiar duplication formula

$$2^{2z-1}\,\Gamma(z)\,\Gamma(z+1/2) = \pi^{1/2}\,\Gamma(2z).$$

If F is a global field and ω is an equivalence class of representations of the Weil group of F, we define as in the introduction, the global L-function to be

$$L(s,\omega) = \prod\nolimits_{\mathfrak{p}} L(s,\omega_{\mathfrak{p}}).$$

I repreat that the product is taken over all primes, including those at infinity. It is not difficult to see that the product converges in a half-plane Re $s > c$. One need only verify it for ω irreducible. Choose a Galois extension K of F so that there is a representation σ of $W_{K/F}$ in the class ω. The restriction of σ to C_K is equivalent to the direct sum of 1-dimensional representations corresponding to generalized characters $\mu^{(1)},\dots,\mu^{(r)}$ of C_K. For each i and j there is a σ in $\mathfrak{G}(K/F)$ such that $\mu^j(a) \equiv \mu^i(\sigma(a))$. Then $|\mu_i^{-1}\mu_j(a)| = |\mu^i(a^{-1}\sigma(a))| = 1$ because $a^{-1}\sigma(a)$ belongs to the compact group of i idèle classes of norm 1. Let $|\mu'(a)| = |a|^r$. Let ν_F be the generalized character $a \to |a|^r$ of C_F. Replacing σ by $\nu_F^{-1}\otimes\sigma$ we replace $L(s,w_{\mathfrak{p}})$ by $L(s-r,w_{\mathfrak{p}})$ and $\mu^{(i)}$ by $|\mu^{(i)}|^{-1}\mu^{(i)}$. Thus we may as well suppose that all $\mu^{(i)}$ are ordinary characters. Since C_K is of finite index in $W_{K/F}$ the eigenvalues of $\sigma(w)$ will all have absolute 1 for any w in $W_{K/F}$ and at any non-archimedean prime the local L-function will be of the form

$$\prod\nolimits_{i=1}^{s}\ \frac{1}{1-\alpha_i\,|\pi_{F_{\mathfrak{p}}}|^s}$$

with $s \le \dim w$ and $|\alpha_i| = 1,\ 1 \le i \le s$. The required result follows from the well-known fact that

$$\prod\nolimits^{1}\ \frac{1}{1-|\pi_{F_{\mathfrak{p}}}|^s}$$

converges from Re $s > 1$. This product is taken only over the non-archimedean primes.

Chapter Twenty-one.

Proof of the Functional Equation.

Choose a non-trivial character ψ_F of $\mathbb{A}_F/F$. Before we can write down the factor appearing in the functional equation of the global L-function we have to verify that $\varepsilon(s,\omega_\gamma,\psi_{F_\gamma})=1$ for all but a finite number of γ.

Let ω be realized as a representation σ of $W_{K/F}$ and let the restriction of σ to C_K be equivalent to the direct sum of 1-dimensional representations corresponding to the generalized characters $\mu^{(1)},\ldots,\mu^{(r)}$. All but finitely many primes $\mathfrak{p}$ will satisfy the following conditions.

(i) $\mathfrak{p}$ is non-archimedean.

(ii) $n(\psi_{F_\mathfrak{p}})=1$.

(iii) $\mathfrak{p}$ does not ramify in K.

(iv) $m(\mu^{(i)}_\mathfrak{P})=0$ for all $\mathfrak{P}$ dividing $\mathfrak{p}$ and all i.

Choose one such $\mathfrak{p}$ and let $\mathfrak{P}$ divide $\mathfrak{p}$. Corresponding to the map $K/F\longrightarrow K_\mathfrak{P}/F_\mathfrak{p}$ is a map $\varphi_\mathfrak{p}: W_{K_\mathfrak{P}/F_\mathfrak{p}}\longrightarrow W_{K/F}$. $\omega_\mathfrak{p}$ is the class of $\sigma_\mathfrak{p}=\sigma\circ\varphi_\mathfrak{p}$. The kernel of $\sigma_\mathfrak{p}$ contains $U_{K_\mathfrak{P}}$. Since $K_\mathfrak{P}/F_\mathfrak{p}$ is unramified the quotient of $W_{K_\mathfrak{P}/F_\mathfrak{p}}$ by $U_{K_\mathfrak{P}}$ is abelian and $\sigma_\mathfrak{p}$ is the direct sum of one-dimensional representations. Let them correspond to the generalized characters $\nu^{(1)}_\mathfrak{p},\ldots,\nu^{(r)}_\mathfrak{p}$ of $C_{F_\mathfrak{p}}$. Since $\tau_{K_\mathfrak{P}/F_\mathfrak{p}}$ takes $U_{K_\mathfrak{P}}$ onto $U_{F_\mathfrak{p}}$ each of these characters is unramified. Thus

$$\varepsilon(s,\omega_\mathfrak{p},\psi_{F_\mathfrak{p}})=\prod\nolimits_{i=1}^{r}\Delta\left(\alpha_{F_\mathfrak{p}}^{s-\frac12}\nu^{(i)}_\mathfrak{p},\psi_{F_\mathfrak{p}}\right)=1.$$

If ψ'_F is another non-trivial character of $\mathbb{A}_F/F$ there is a β in F^* such that $\psi'_F(x)\equiv\psi_F(\beta x)$. According to Lemma 5.1

$$\varepsilon(s,\omega,\psi_{F_\mathfrak{p}})=\alpha_{F_\mathfrak{p}}^{s-\frac12}(\beta)\det\omega_\mathfrak{p}(\beta)\ \varepsilon(s,\omega,\psi_{F_\mathfrak{p}}).$$

Since

$$\prod\nolimits_\mathfrak{p}\alpha_{F_\mathfrak{p}}(\beta)^{s-\frac12}\det\omega_\mathfrak{p}(\beta)=|\beta|^{s-\frac12}\det\omega(\beta)=1$$

the function

$$\varepsilon(s,\omega)=\prod\nolimits_\mathfrak{p}\varepsilon(s,\omega_\mathfrak{p},\psi_{F_\mathfrak{p}})$$

is indeed independent of ψ_F.

We can infer from Tate's thesis not only that $L(s,\omega)$ is meromorphic in the whole complex plane if ω is one-dimensional but also that it satisfies the functional equation

$$L(s,\omega)=\varepsilon(s,\omega)\,L(1-s,\widetilde{\omega})$$

if $\widetilde{\omega}$ is contragredient to ω. As is well-known, Lemma 2.2 then implies that $L(s,\omega)$ is meromorphic in the whole complex plane for any ω. In any case, Theorem B is true for one-dimensional ω and, granting this, we have to establish it in general.

First we need a lemma.

Lemma 21.1

Suppose F is a global field, K is a Galois extension of F, E is a field lying between F and K, χ is a generalized character of C_E and

$$\sigma = \mathrm{Ind}(W_{K/F}, W_{K/E}, \chi).$$

If ω is the class of σ and, for each prime $\mathfrak{q}$ of E, $\chi_{\mathfrak{q}}$ is the restriction of χ to $C_{E_{\mathfrak{q}}}$ then for each prime $\mathfrak{p}$ of F

$$\varepsilon(s, \omega_{\mathfrak{p}}, \psi_{F_{\mathfrak{p}}}) = \prod_{\mathfrak{q}|\mathfrak{p}} \{\varepsilon(s, \chi_{\mathfrak{q}}, \psi_{E_{\mathfrak{q}}/F_{\mathfrak{p}}})\ \rho\,(E_{\mathfrak{q}}/F_{\mathfrak{p}}, \psi_{F_{\mathfrak{p}}})\}.$$

Let $\mathfrak{P}$ be a prime of K dividing $\mathfrak{p}$. The first step is to find a set of representatives for the double cosets $W_{K/E}\,w\,W_{K_{\mathfrak{P}}/F_{\mathfrak{p}}}$. Since $C_K \subseteq W_{K/E}$ is a normal subgroup of $W_{K/F}$ we can factor out C_K and merely find a set of representatives for the double cosets

$$\mathfrak{G}(K/E)\sigma\,\mathfrak{G}(K_{\mathfrak{P}}/F_{\mathfrak{p}}).$$

Let $\mathfrak{P}_1, \ldots, \mathfrak{P}_r$ be the primes of K dividing $\mathfrak{p}$ and let $\mathfrak{P}_1$ divide $\mathfrak{q}_i$ in E. $\mathfrak{G}(K/F)$ is the disjoint union

$$\bigcup_{i=1}^{r} \sigma_i \mathfrak{G}(K_{\mathfrak{P}}/F_{\mathfrak{p}})$$

where $\sigma_i(\mathfrak{P}) = \mathfrak{P}_i$. If σ_i and σ_j belong to the same double coset $\mathfrak{q}_i = \mathfrak{q}_j$. Conversely, if $\mathfrak{q}_i = \mathfrak{q}_j$ there is a ρ in $\mathfrak{G}(K/E)$ such that $\rho(\mathfrak{P}_i) = \mathfrak{P}_j$. Then $\rho\sigma_i(\mathfrak{P}) = \sigma_j(\mathfrak{P})$ and

$$\rho\sigma_i \in \sigma_j\,\mathfrak{G}(K_{\mathfrak{P}}/F_{\mathfrak{p}}).$$

Thus we may write $\mathfrak{G}(K/F)$ as the disjoint union

$$\bigcup_{\tau \in S} \mathfrak{G}(K/E)\tau\,\mathfrak{G}(K_{\mathfrak{P}}/F_{\mathfrak{p}})$$

so that if $\mathfrak{P}$ divides $\mathfrak{q}$ in E the collection $\{\tau(\mathfrak{q}) \mid \tau \in S\}$ is the collection of distinct primes in E dividing $\mathfrak{p}$.

For each τ in S choose a representative $w(\tau)$ in $W_{K/F}$. For each τ in S the restriction of σ to $W_{K_{\mathfrak{P}}/F_{\mathfrak{p}}}$ leaves invariant the space of functions f on the double coset $W_{K/E}w(\tau)W_{K_{\mathfrak{P}}|F_{\mathfrak{p}}}$ which satisfy $f(vw) = \chi(\tau_{K/E}(v))f(w)$ for all v in $W_{K/E}$. The representation of $W_{K_{\mathfrak{P}}/F_{\mathfrak{p}}}$ on this space is equivalent to

$$\mathrm{Ind}(W_{K_{\mathfrak{P}}/F_{\mathfrak{p}}}, W_{K_{\mathfrak{P}}/E^{\tau}_{\mathfrak{q}^{\tau}}}, \chi'_{\mathfrak{q}^{\tau}}$$

if $E^{\tau} = \tau^{-1}(E)$ and

$$\chi'_{\mathfrak{q}^{\tau}}(a) = \chi(\tau(a)).$$

Thus

$$\varepsilon(s, \omega_{\mathfrak{q}}, \psi_{F_{\mathfrak{p}}}) = \prod\nolimits_{\tau \in S} \varepsilon(s, \chi'_{\mathfrak{q}^{\tau}}, \psi_{E^{\tau}_{\mathfrak{q}^{\tau}}/F_{\mathfrak{p}}})\,\rho(E^{\tau}_{\mathfrak{q}^{\tau}}/F_{\mathfrak{p}}, \psi_{F_{\mathfrak{p}}})$$

which is of course equal to

$$\prod\nolimits_{\tau \in S} \varepsilon(s, \chi_{\mathfrak{q}}, \psi_{E_{\mathfrak{q}}/F_{\mathfrak{p}}})\,\rho(E_{\mathfrak{q}}/F_{\mathfrak{p}}, \psi_{F_{\mathfrak{p}}}).$$

We set

$$\rho(E/F) = \prod_{\mathfrak{q}} \prod_{\mathfrak{q}|\mathfrak{p}} \rho(E_{\mathfrak{q}}/F_{\mathfrak{p}}, \psi_{F_{\mathfrak{p}}}).$$

The preceding discussion together with Lemma 5.1 shows that it does not depend on ψ_F. However that does not really matter since we are about to show that for any choice of ψ_F it is 1. Observe first of all that the previous lemma implies immediately that if ω is the class of

$$\sigma = \mathrm{Ind}(W_{K/F}, W_{K/E}, \chi)$$

then

$$\varepsilon(s,\omega) = \varepsilon(s,\chi)\,\rho(E/F).$$

Given an arbitrary class ω realizable as a representation of $W_{K/F}$ we can find fields $E_1, \dots, E_r$ lying between F and K, generalized characters $\chi_{E_1}, \dots, \chi_{E_r}$, and integers $m_1, \dots, m_r$ such that

$$\sum_{i=1}^{r} \oplus m_i \ \mathrm{Ind}(W_{K/F}, W_{K/E_i}, \chi_{E_i})$$

is in the class ω. Then

$$\varepsilon(s,\omega) = \prod_{i=1}^{r} \{\varepsilon(s,\chi_{E_i})^{m_i}\,\rho(E_i/F)^{m_i}\}.$$

On the other hand

$$L(s,\omega) = \prod_{i=1}^{r} L(s,\chi_{E_i})^{m_i}$$

and

$$L(s,\widetilde{\omega}) = \prod_{i=1}^{r} L(s,\chi_{E_i}^{-1})^{m_i}.$$

Since

$$L(s,\chi_{E_i}) = \varepsilon(s,\chi_{E_i})\,L(1-s,\chi_{E_i}^{-1})$$

we have

$$L(s,\omega) = \prod_{i=1}^{r} \varepsilon(s,\chi_{E_i})^{m_i}\,L(1-s,\widetilde{\omega})$$

because $\widetilde{\omega}$ contains

$$\sum_{i=1}^{r} \oplus m_i \ \mathrm{Ind}(W_{K/F}, W_{K/E_i}, \chi_{E_i}^{-1}).$$

Consequently

$$\prod_{i=1}^{r} \varepsilon(s,\chi_{E_i})^{m_i}$$

depends only on ω and not on the particular way it is written as a sum of induced representations. Thus

$$\prod_{i=1}^{r} \rho(E_i/F)^{m_i}$$

also depends only on ω. We call it $H(\omega)$. It is clear that to prove Theorem B we have to show that $H(\omega) = 1$ for all ω or, what is the same, that $\rho(E/F) = 1$ for all E and F.

Suppose $F \subseteq E \subseteq E'$. Denote the primes of F by $\mathfrak{p}$, those of E by $\mathfrak{q}$, and those of E' by $\mathfrak{q}'$. Then

$$\rho(E'/F) = \prod_{\mathfrak{p}} \prod_{\mathfrak{q}'|\mathfrak{p}} \rho(E'_{\mathfrak{q}'}/F_{\mathfrak{p}}, \psi_{F_{\mathfrak{p}}}).$$

Apply Lemma 4.5 to see that the right side equals

$$\prod_{\mathfrak{p}}\prod_{\mathfrak{q}|\mathfrak{p}}\prod_{\mathfrak{q}'|\mathfrak{q}}\left\{\rho(E'_{\mathfrak{q}'}/E_{\mathfrak{q}},\psi_{F_{\mathfrak{q}}/F_{\mathfrak{p}}})\,\rho(E_{\mathfrak{q}}/F_{\mathfrak{p}},\psi_{F_{\mathfrak{p}}})^{[E'_{\mathfrak{q}}:E_{\mathfrak{q}}]}\right\}.$$

Since

$$\sum_{\mathfrak{q}'|\mathfrak{q}}[E'_{\mathfrak{q}'}:E_{\mathfrak{q}}]=[E':E]$$

this may be written as

$$\left\{\prod_{\mathfrak{q}}\prod_{\mathfrak{q}'|\mathfrak{q}}\rho(E'_{\mathfrak{q}'}/E_{\mathfrak{q}},\psi_{F_{\mathfrak{q}}/F_{\mathfrak{p}}})\right\}\ \left\{\prod_{\mathfrak{p}}\prod_{\mathfrak{q}|\mathfrak{p}}\ \rho(E_{\mathfrak{q}}/F_{\mathfrak{p}},\psi_{F_{\mathfrak{p}}})\right\}^{[E':E]}$$

which is of course

$$\rho(E'/E)\ \rho(E/F)^{[E':E]}. \tag{20.1}$$

Suppose E/F is an abelian extension and ω is the class of the representation of $W_{E/F}$ induced from the trivial representation of $C_E=W_{E/E}$. Then $H(\omega)=\rho(E/F)$. On the other hand, ω is the direct sum of $[E:F]$ one-dimensional representations; so $H(\omega)=\rho(F/F)^{[E:F]}=1$. It follows immediately not only that $\rho(E/F)=1$ if E/F is abelian but also that $\rho(E/F)=1$ if E can be obtained from F by a succession of abelian extensions. In particular if $F\subseteq E\subseteq L$ and L/F is nilpotent $\rho(E/F)=1$.

Observe that (20.1) together with Lemma 2.2 and the transitivity of induction imply that if ω is the class of

$$\sigma=\mathrm{Ind}(W_{K/F},W_{K/E},\rho)$$

and θ is the class of ρ then

$$H(\omega)=H(\theta)\,\rho(E/F)^{\dim\,\theta}.$$

To complete the proof we will show that $H(\omega_1\otimes\omega_2)=H(\omega_2)^{\dim\,\omega_1}$ for all ω_1 and ω_2. Taking $\omega_2=1$ we find $H(\omega_1)=1$. It is enough to prove the equality when ω_1 and ω_2 are both realizable as representations of $W_{K/F}$ and there is a field E lying between E and K with $\mathfrak{G}(K/E)$ nilpotent and a generalized character χ_E such that ω_2 is the class of

$$\mathrm{Ind}(W_{K/F},W_{K/E},\chi_E).$$

Then $H(\omega_2)=\rho(E/F)$. If ρ is a representation in the restriction of ω_1 to $W_{K/E}$ then, by Lemma 2.3, $\omega_1\otimes\omega_2$ is the class of

$$\mathrm{Ind}(W_{K/F},W_{K/E},\rho\otimes\chi_E).$$

Let θ be the class of $\rho\otimes\chi_E$. $H(\theta)$ is of the form

$$\prod_{i=1}^{r}\ \rho(E_i/E)^{m_i}$$

where $E\subseteq E_i\subseteq K$ and is therefore 1. Thus

$$H(\omega_1\otimes\omega_2)=H(\theta)\rho(E/F)^{\dim\,\theta}=\rho(E/F)^{\dim\omega_1}.$$

as required.

Chapter Twenty-two.

Appendix.

There is clearly not much to be said about the functions $\varepsilon(s,\omega,\psi_F)$ when F is archimedean. However for non-archimedean F their properties are more obscure. In this appendix we shall describe and prove some properties which were not needed in the proofs of the main theorems and so found no place in the main body of the paper but which will be used elsewhere.

The first step is to define the Artin conductor of ω. We follow a well-trodden path. If K is a finite Galois extension of the local field F then $W^0_{K/F}$ contains U_K as a subgroup of finite index and is therefore compact. It is, in fact, a maximal compact subgroup of $W_{K/F}$. Choose that Haar measure dw on $W_{K/F}$ which assigns the measure 1 to $W^0_{K/F}$. If f is a locally constant function on $W_{K/F}$ and u is a non-negative real number set

$$\hat{f}(u) = \left\{\int_{W^u_{K/F}} dw\right\}^{-1} \int_{W^u_{K/F}} \{f(1) - f(w)\} dw.$$

Since $W^u_{K/F}$ is an open subgroup of $W_{K/F}$ it is meaningful to restrict dw to it. $\hat{f}(u)$ is bounded, continuous from the left, and 0 for u sufficiently large. Since $W^u_{K/F} = W^0_{K/F}$ for $1 < u \leq 0$ we have $\hat{f}(u) = \hat{f}(0)$ for such u. The integral

$$\int_{-1}^{\infty} \hat{f}(u) du$$

is well-defined.

There are some simple lemmas to be verified.

Lemma 22.1

Suppose $F \subseteq K \subseteq L$ and L/F is also a Galois extension. Define g on $W_{L/F}$ by $g(w) = f_{(\tau_{L/F},K/F}(w))$. Then $\hat{g}(u) = \hat{f}(u)$ for all u.

This is immediate because by Lemma 6.16, $\tau_{L/F,K/F}$ maps $W^u_{L/F}$ onto $W^u_{K/F}$ for every u.

When we want to make the roles of K and F explicit we write $\hat{f}(u) = \hat{f}_{K/F}(u)$.

Lemma 22.2

Suppose $F \subseteq E \subseteq K$ and g is a function on $W_{K/E}$ satisfying $g(wzw^{-1}) = g(z)$ for all z and w in $W_{K/E}$. Regard $W_{K/E}$ as a subgroup of $W_{K/F}$ and set

$$f(w) = \sum\nolimits_{z \in W_{K/E}\backslash W_{K/F}} g(z^{-1}wz).$$

If $N_{E/F}\,\pi_E$ is a unit times $\pi_F^{f_{E/F}}$ and $\mathfrak{P}_E^{\delta_{E/F}}$ is the different of E/F

$$\int_{-1}^{\infty} \hat{f}_{K/F}(u) du = f_{E/F} \int_{-1}^{\infty} \hat{g}_{K/E}(u) du + f_{E/F}\delta_{E/F} g(1).$$

Let $dw_{K/F}$ be the normalized Haar measure on $W_{K/F}$ and let $dw_{K/E}$ be the normalized Haar measure on $W_{K/E}$. On $W_{K/E}$

$$dw_{K/E} = [W^0_{K/F} : W^0_{K/E}]dw_{K/F}.$$

Suppose at first that $g(1) = 0$. Denote also by g the function on $W_{K/F}$ which equals the given g on $W_{K/E}$ but is 0 outside of $W_{K/E}$. Then

$$\hat{f}_{K/F}(u) = [W_{K/F} : W_{K/E}]\,\hat{g}_{K/F}(u).$$

Since $W^u_{K/F} \cap W_{K/E} = W^v_{K/E}$ if $v = \psi_{E/F}(u)$

$$\begin{aligned}\hat{g}_{K/F}(u) &= -[W^0_{K/F} : W^u_{K/F}] \int_{W^u_{K/F}} g(w)dw_{K/F} \\ &= -\frac{[W^0_{K/F} : W^u_{K/F}]}{[W^0_{K/F} : W^0_{K/E}]} \int_{W^v_{K/E}} g(w)dw_{K/E} \\ &= \frac{1}{[W^0_{K/F} : W^0_{K/E}]}\;\frac{[W^0_{K/F} : W^u_{K/F}]}{[W^0_{K/E} : W^v_{K/E}]}\;\hat{g}_{K/E}(v).\end{aligned}$$

Recall that

$$f_{E/F} = \frac{[W_{K/F} : W_{K/E}]}{[W^0_{K/F} : W^0_{K/E}]}.$$

Moreover

$$\frac{[W^0_{K/F} : W^u_{K/F}]}{[W^0_{K/E} : W^v_{K/E}]} = \frac{[W^0_{K/F} : W^u_{K/F}\,U^0_K]}{[W^0_{K/E} : W^v_{K/E}\,U^0_K]} \cdot \frac{[U^0_K : U^0_K \cap W^u_{K/F}]}{[U^0_K : U^0_K \cap W^v_{K/E}]}$$

and $U^0_K \cap W^u_{K/F} = U^0_K \cap W^v_{K/E}$. By Lemma 6.11 the first term in this product is equal to

$$\frac{[G^0 : G^u]}{[H^0 : H^v]}$$

if $G = \mathfrak{G}(K/F)$ and $H = \mathfrak{G}(K/E)$. But

$$[G^0 : G^u] = \psi'_{K/F}(u)$$

and

$$[H^0 : H^v] = \psi'_{K/E}(v)$$

while

$$\psi'_{K/F}(u) = \psi'_{K/E}(v)\psi'_{E/F}(u).$$

Thus

$$\begin{aligned}\int_{-1}^{\infty} \hat{f}_{K/F}(u)du &= f_{E/F} \int_{-1}^{\infty} \hat{g}_{K/E}(\psi_{E/F}(u))\,\psi'_{E/F}(u)du \\ &= f_{E/F} \int_{-1}^{\infty} \hat{g}_{K/E}(v)dv.\end{aligned}$$

To complete the proof of the lemma, we have to show that if $g(w) = 1$ so that $\hat{g}_{K/E}(u) \equiv 0$ then

$$\int_{-1}^{\infty} \hat{f}_{K/F}(u)du = f_{E/F}\,\delta_{E/F}.$$

In this case

$$\hat{f}_{K/F}(u) = [G:H] - \frac{[G:H]}{[G^0:H^0]}\ \frac{[G^0:G^u]}{[H^0:H^v]}$$

if $v = \psi_{E/F}(u)$. After some simple rearranging this becomes

$$\frac{[G:H]}{[G^u:1]}\ \{[G^u:1] - [H^v:1]\} = \frac{[G:H]}{[G^u:1]}\ \{([G^u:1]-1) - ([H^v:1]-1)\}.$$

The factor

$$\frac{[G:H]}{[G^u:1]} = \frac{[G:G^0]}{[H:1]}\ \psi'_{K/F}(u)$$

and, from paragraph IV.2 of [ ],

$$\int_{1}^{\infty} ([G^u:1]-1)\psi'_{K/F}(u)du = \int_{-1}^{\infty} ([G_x:1]-1)dx = \delta_{K/F}$$

while

$$\int_{-1}^{\infty} ([H^v:1]-1)\,\psi'_{K/F}(u)du = \int_{-1}^{\infty} ([H^v:1]-1)\,\psi'_{K/E}(v)dv = \delta_{K/E}.$$

Thus

$$\int_{-1}^{\infty} \hat{f}_{K/F}(u)du = \frac{[G:G^0]}{[H:1]}\,(\delta_{K/F} - \delta_{K/E}) = f_{E/F}\,\delta_{E/F}$$

because

$$\delta_{K/F} = \delta_{K/E} + [H_0:1]\,\delta_{E/F}.$$

Suppose ω is an equivalence class of representations of the Weil group of F and σ is a representation of $W_{K/F}$ in the class of ω. Let f_σ be the character of σ. It follows from Lemma 22.1 that the value of

$$\int_{-1}^{\infty} \hat{f}_\sigma(u)du$$

depends only on ω and not on σ. We call it the order of ω and denote it by $m(\omega)$. Since $\hat{f}_\sigma(u)$ is clearly non-negative for all u and vanishes identically if and only if $W^0_{K/F}$ is contained in the kernel of σ, the order $m(\omega)$ is always non-negative and equals zero if and only if the kernel of each realization σ of ω contains $W^0_{K/F}$.

Lemma 22.3

(a) *If* $\omega = \omega_1 \oplus \omega_2$ *then* $m(\omega) = m(\omega_1) + m(\omega_2)$.

(b) *If*

$$\omega = \mathrm{Ind}(W_{K/F}, W_{K/E}, \nu)$$

then

$$m(\omega) = f_{E/F} m(\nu) = f_{E/F}\,\delta_{E/F}\dim\nu.$$

(c) $m(\omega)$ *is a non-negative integer.*

The first property is immediate. The second is a consequence of Lemma 22.2. To verify the third we merely have to show that $m(\omega)$ is integral. If $\omega = \mu\oplus\nu$ and the assertion is true for any two of μ,ν and ω it is true for the third. This observation, together with part (b) and Lemma 2.2, shows that it is enough to verify (c) when ω is the one-dimensional class corresponding to a generalized character χ_F of C_F. To do this we show that $m(\omega) = m(\chi_F)$.

If $f(a) = \chi_F(a)$ for a in $C_F = W_{F/F}$ then $\hat{f}(u) = \hat{f}(m)$ for $m-1 < u \le m$ and

$$\hat{f}(m) = [U_F^0 : U_F^m]\ \int_{U_F^m}\{1-\chi_F(a)\}da.$$

The right side is 1 if $m < m(\chi_F)$ and 0 if $m \ge m(\chi_F)$. Thus

$$m(\omega) = \int_{-1}^{m(\chi_F)-1} du = m(\chi_F).$$

The function $\omega \longrightarrow m(\omega)$ is characterized by (a) and (b) together with the fact that $m(\omega) = m(\chi_F)$ if ω is the class of χ_F.

Lemma 22.4

If ω is an equivalence class of representations of the Weil group of the non-archimedean local field F and ψ_F is a non-trivial additive character of F set $m'(\omega) = m(\omega) + n(\psi_F)\dim\omega$. There is a non-zero complex constant $a(\omega)$ such that, as a function of s,

$$\varepsilon(s,\omega,\psi_F) = a(\omega)\ |\pi_F|^{m'(\omega)s}.$$

If $\omega = \mu\oplus\nu$ and the lemma is true for any two of μ,ν, and ω, it is true for the third. Applying Lemma 2.2 we see that it is enough to verify it when ω contains a representation

$$\mathrm{Ind}(W_{K/F}, W_{K/E}, \chi_E).$$

Then

$$\varepsilon(s,\omega,\psi_F) = \Delta(\alpha_E^{s-\frac{1}{2}}\chi_E,\psi_{E/F})\ \rho(E/F,\psi_F).$$

Clearly

$$\Delta(\alpha_E^{s-\frac{1}{2}}\chi_E,\psi_{E/F}) = \alpha_E^{s-\frac{1}{2}}\left(\pi_E^{m(\chi_E)+\delta_{E/F}}\pi_F^{n(\psi_F)}\right)\ \Delta(\chi_E,\psi_{E/F}).$$

But

$$\alpha_E\left(\pi_E^{m(\chi_E)+\delta_{E/F}}\pi_F^{n(\psi_F)}\right) = \alpha_F\left(N_{E/F}\left(\pi_E^{m(\chi_E)+\delta_{E/F}}\pi_F^{n(\psi_F)}\right)\right)$$

and the argument on the right is the product of a unit and

$$\pi_F^{f_{E/F}\left(m(\chi_E)+\delta_{E/F}\right)+n(\psi_F)\dim\omega} = \pi_F^{m'(\omega)}.$$

The lemma follows.

The next lemma is rather technical and to prove it we will have to use the notations and results of paragraphs 8 and 9.

Lemma 22.5

Let ω be an equivalence class of representations of the Weil group of the non-archimedean local field F and m_1 a positive integer. There is a positive integer m_2 such that if χ_F and $\mu_1, \ldots, \mu_r$ with $r = \dim\omega$, are generalized characters of C_F and $m(\chi_F) \geq m_2,\ m(\mu_i) \leq m_1,\ 1 \leq i \leq r$, while

$$\prod_{i=1}^{r} \mu_i = \det\omega$$

then for any non-trivial additive character ψ_F

$$\varepsilon(s, \chi_F \otimes \sigma, \psi_F) = \prod_{i=1}^{r} \varepsilon(s, \mu_i\chi_F, \psi_F).$$

Choose, as a start, $m_2 \geq 2m_1 + 1$. If μ_F is a generalized character of C_F and $m(\mu_F) \leq m_1$ while $m(\chi_F) \geq m_2$ then $m(\mu_F\chi_F) = m(\chi_F) = m$. Let $n = n(\psi_F)$ and choose γ so that $O_F\gamma = \mathfrak{P}_F^{m+n}$. If $\beta = \beta(\chi_F)$ we may choose $\beta(\mu_F\chi_F) = \beta$. Appealing to Lemmas 8.1 and 9.4 we see that

$$\begin{aligned}\varepsilon(s, \mu_F\chi_F, \psi_F) &= \Delta(\alpha_F^{s-\frac{1}{2}}\mu_F\chi_F, \psi_F)\\ &= (\alpha_F^{s-\frac{1}{2}}\mu_F)\ \left(\frac{\gamma}{\beta}\right)\ \Delta(\chi_F, \psi_F).\end{aligned}$$

In particular

$$\prod_{i=1}^{r} \varepsilon(s, \mu_i\chi_F, \psi_F) = \alpha_F^{r(s-\frac{1}{2})}\ \left(\frac{\gamma}{\beta}\right)\ \det\omega\ \left(\frac{\gamma}{\beta}\right)\ \{\Delta(\chi_F, \psi_F)\}^r.$$

If $\omega = \mu \oplus \nu$ then

$$\varepsilon(s, \chi_F \otimes \omega, \psi_F) = \varepsilon(s, \chi_F \otimes \mu, \psi_F)\ \varepsilon(s, \chi_F \otimes \nu, \psi_F)$$

and all three terms are different from zero. Thus if the lemma is true for two of μ, ν and ω it is true for the third. Using Lemma 2.2 once again, we see that it is enough to prove the lemma when there is an intermediate field E and a generalized character μ_E of C_E such that ω is the class of

$$\mathrm{Ind}(W_{K/F}, W_{K/E}, \mu_E).$$

Then $\chi_F \otimes \omega$ is the class of

$$\mathrm{Ind}(W_{K/F}, W_{K/E}, \mu_E\, \chi_{E/F})$$

and

$$\varepsilon(s, \chi_F \otimes \omega, \psi_F) = \Delta(\alpha_E^{s-\frac{1}{2}}\mu_E\chi_{E/F}, \psi_{E/F})\, \rho(E/F, \psi_F).$$

There are two simple lemmas which we need before we can proceed further and we digress to prove them.

Lemma 22.6

Let E be a separable extension of F. If m is sufficiently large

$$\psi_{E/F}(m-1)+1 = m\,e_{E/F}-\delta_{E/F}$$

if $e_{E/F}$ is the index of ramification of F in E.

Suppose $F\subseteq E\subseteq K$ where K/F is Galois and the assertion is true for K/F and K/E. Subtracting 1 from both sides of the equation, applying $\psi_{K/E}$, and then adding 1, we obtain the equivalent equation

$$\psi_{K/F}(m-1)+1=\psi_{K/E}(m\,e_{E/F}-\delta_{E/F}-1)+1.$$

By assumption, the left side equals

$$m\,e_{K/F}-\delta_{K/F}$$

and the right side equals

$$(m\,e_{E/F}-\delta_{E/F})\,e_{K/E}-\delta_{K/E}.$$

Since $e_{K/F}=e_{K/E}e_{E/F}$ and $\delta_{K/F}=\delta_{K/E}+e_{K/E}\delta_{E/F}$ these two expressions are equal and we have only to prove the lemma for Galois extensions.

Suppose $F\subseteq K\subseteq L$ and L/F and K/F are Galois. Suppose also that the lemma is true for L/K and K/F. Then

$$\begin{aligned}\psi_{L/F}(m-1)+1&=\psi_{L/F}(\psi_{K/F}(m-1))+1\\&=\psi_{L/F}(m\,e_{K/F}-\delta_{K/F}-1)+1\\&=(m\,e_{K/F}-\delta_{K/F})\,e_{L/K}-\delta_{L/K}\\&=m\,e_{L/F}-\delta_{L/F}\end{aligned}$$

as before. Thus, if we use induction, we need only verify the lemma directly for a Galois extension K/F of prime degree.

We apply Lemma 6.3. If K/F is unramified, $e_{K/F}=1$ and $\delta_{K/F}=0$ while $\psi_{K/F}(m-1)=m-1$; so the relation follows. If K/F is ramified there is an integer t such that $\delta_{K/F}=([K:F]-1)(t+1)$ while $\psi_{K/F}(m-1)+1=[K:F]m-([K:F]-1)(t+1)$ for $m-1\geq t$. Since $e_{K/F}=[K:F]$ the relation follows again.

If $n=n(\psi_F)$ then

$$n'=n(\psi_{E/F})=n\,e_{E/F}+\delta_{E/F}.$$

Thus if m is sufficiently large and $m'=\psi_{E/F}(m-1)+1$

$$m'+n'=(m+n)\,e_{E/F}$$

and if $O_F\gamma=\mathfrak{P}_F^{m+n}$ then $O_E\gamma=\mathfrak{P}_E^{m'+n'}$. We define

$$P^*_{E/F}(x)=P^*_{E/F}(x;\gamma,\gamma)$$

as in paragraph 8.

Lemma 22.7

If m_1 is a given positive integer then for m sufficiently large

$$P^*_{E/F}(x) \equiv x \pmod{\mathfrak{P}_E^{m_1}}.$$

As in paragraph 8, let d be the integral part of $\frac{m}{2}$, d' the integral part of $\frac{m'}{2}$, and let $m = 2d+\varepsilon,\ m' = 2d'+\varepsilon'$. $P^*_{E/F}(x)$ depends only on the residue of x modulo $\mathfrak{P}_F^d$ and is only determined modulo $\mathfrak{P}_E^{d'}$. Recall that if

$$P_{E/F}(y) = N_{E/F}(1+y) - 1$$

for y in $\mathcal{P}_E^{d'+\varepsilon'}$ then

$$\psi_{E/F}\left(\frac{P^*_{E/F}(x)y}{\gamma}\right) = \psi_F\left(\frac{x\,P_{E/F}(y)}{\gamma}\right).$$

To show that $P^*_{E/F}(x) \equiv x \pmod{\mathfrak{P}_E^{m_1}}$ when m is sufficiently large, we have to show that

$$\psi_F\left(\frac{x\,P_{E/F}(y)}{\gamma}\right) = \psi_{E/F}\left(\frac{xy}{\gamma}\right)$$

for y in $\mathfrak{P}_E^{m'-m_1}$. To do this we show that

$$P_{E/F}(y) \equiv S_{E/F}(y) \pmod{\mathfrak{P}_F^m}$$

when m is sufficiently large and y is in $\mathfrak{P}_E^{m'-m_1}$.

To put it another way, we have to show that if K/F is any Galois extension the assertion is true for all intermediate fields E. For this we use induction on $[K:F]$ together with Lemma 3.3. There are three facts to verify:

(i) If E/F is a Galois extension of prime degree then

$$P_{E/F}(y) \equiv S_{E/F}(y) \pmod{\mathfrak{P}_F^m}$$

when m is sufficiently large and y is in $\mathfrak{P}_E^{m'-m_1}$.

(ii) Suppose $F \subseteq E \subseteq K$ and K/F is Galois. Let $G = \mathfrak{G}(K/F)$ and let E be the fixed field of H. Suppose $H \neq \{1\}$ and $G = HC$ where $H \cap C = \{1\}$ and C is a non-trivial abelian normal subgroup of G which is contained in every other non-trivial normal subgroup. If the induction assumption is valid

$$P_{E/F}(y) \equiv S_{E/F}(y) \pmod{\mathfrak{P}_F^m}$$

when m is sufficiently large and y is in $\mathfrak{P}_E^{m'-m_1}$.

(iii) Suppose $F \subseteq E \subseteq E' \subseteq K$ and $m'' = \psi_{E'/F}(m-1)+1$. If, for any choice of m_1,

$$P_{E/F}(y) \equiv S_{E/F}(y) \pmod{\mathfrak{P}_F^m}$$

when m is sufficiently large and y is in $\mathfrak{P}_E^{m'-m_1}$ and, for any choice of m_1',

$$P_{E'/E}(y) \equiv S_{E'/E}(y) \pmod{\mathfrak{P}_E^{m'}}$$

when m, or m', is sufficiently large and y is in $\mathfrak{P}_{E'}^{m''-m_1'}$ then, for any choice of m_1',

$$P_{E'/F}(y) \equiv S_{E'/F}(y) \pmod{\mathfrak{P}_F^m}$$

if m is sufficiently large and y is in $\mathfrak{P}_{E'}^{m''-m_1'}$.

We first verify (i) for E/F unramified. By paragraph V.2 of [12]

$$P_{E/F}(y) = N_{E/F}(1+y) - 1 \equiv S_{E/F}(y) \pmod{\mathfrak{P}_F^m}$$

if y belongs to $\mathfrak{P}_E^{d'+\varepsilon'}$. In this case $m = m'$ and we take $m > 2m_1$ so that $m' - m_1 > d' + \varepsilon'$. If E/F is ramified and of degree ℓ we again choose m sufficiently large that $m' > 2m_1$. If $m > t$

$$\frac{2(m'-m_1)+(\ell-1)(t+1)}{\ell} \geq \frac{m'+(\ell-1)(t+1)}{\ell} = m$$

so that by Chapter V of [12],

$$\mathcal{P}_{E/F}(y) \equiv S_{E/F}(y) + N_{E/F}(y) \pmod{\mathfrak{P}_F^m}$$

if y belongs to $\mathfrak{P}_E^{m'-m_1}$. t of course has its usual meaning. Since $N_{E/F}(y)$ belongs to $\mathfrak{P}_F^{m'-m_1}$ all we have to do is arrange that $m' - m_1 \geq m$. Since

$$m' - m_1 = \ell m - (\ell-1)\,(t+1) - m_1$$

and $\ell \geq 2$, this can certainly be done by choosing m sufficiently large.

To verify the second fact let L be the fixed field of C. We can assume that the required assertion is true for the extension K/L. Let $\ell = \psi_{L/F}(m-1)+1$ and $\ell' = \psi_{K/F}(m-1)+1$. If m is sufficiently large and H_0 is the inertial group of H

$$\ell = [H_0:1]m - ([H_0:1]-1)$$

and

$$\ell' = [H_0:1]m' - ([H_0:1]-1).$$

Thus

$$\mathfrak{P}_L^{\ell} \cap F = \mathfrak{P}_F^m$$

and if $\ell_1 = [H_0:1]m_1$ then

$$\mathfrak{P}_K^{\ell'-\ell_1} \cap E = \mathfrak{P}_E^{m'-m_1}.$$

If m and therefore ℓ is sufficiently large

$$P_{K/L}(y) = N_{K/L}(1+y) - 1 \equiv S_{K/L}(y) \pmod{\mathfrak{P}_L^{\ell}}$$

if y belongs to $\mathfrak{P}_K^{\ell'-\ell_1}$. Thus if y belongs to $\mathfrak{P}_E^{m'-m_1}$

$$P_{E/F}(y) = P_{K/L}(y) \equiv S_{K/L}(y) = S_{E/F}(y) \pmod{\mathfrak{P}_F^m}.$$

To verify the third fact we choose, once m_1' is given, m_1 so that

$$S_{E'/E}\left(\mathfrak{P}_{E'}^{-\delta_{E'/E}-m_1'}\right)=\mathfrak{P}_E^{-m_1}.$$

If m is sufficiently large

$$m''=m'\,e_{E'/E}-\delta_{E'/E}$$

and if y belongs to $\mathfrak{P}_{E'}^{m''-m_1'}$

$$S_{E'/E}(y)\in\mathfrak{P}_E^{m'-m_1}.$$

Taking in even larger if necessary, we have

$$\begin{aligned}P_{E'/F}(y)&\equiv P_{E/F}(P_{E'/E}(y))\\&\equiv P_{E/F}(S_{E'/E}(y))\\&\equiv S_{E/F}(S_{E'/E}(y))\\&\equiv S_{E'/F}(y)\pmod{\mathfrak{P}_F^m}.\end{aligned}$$

Returning to the proof of Lemma 22.5, we choose

$$\beta'=\beta(\chi_{E/F})=P_{E/F}^*(\beta).$$

If $m(\chi_F)$ and therefore $m(\chi_{E/F})$ is sufficiently large,

$$\Delta(\alpha_E^{s-\frac12}\mu_E\,\chi_{E/F},\psi_{E/F})=\alpha_E^{s-\frac12}\,\left(\frac{\gamma}{\beta'}\right)\,\mu_E\,\left(\frac{\gamma}{\beta'}\right)\,\Delta(\chi_{E/F},\psi_{E/F}).$$

Both β and β' are units and therefore

$$\alpha_E^{s-\frac12}\,\left(\frac{\gamma}{\beta'}\right)=\alpha_E^{r-\frac12}\,\left(\frac{\gamma}{\beta}\right)=\alpha_F^{s-\frac12}\,\left(N_{E/F}\,\left(\frac{\gamma}{\beta}\right)\right)=\alpha_F^{r(s-\frac12)}\,\left(\frac{\gamma}{\beta}\right).$$

If $m(\chi_F)$ is sufficiently large

$$\beta'\equiv\beta\quad\left(\operatorname{mod}\mathfrak{P}_E^{m(\mu_E)}\right)$$

and $\mu_E(\beta')=\mu_E(\beta)$. In paragraph 5 we saw that

$$\det\omega\,\left(\frac{\gamma}{\beta}\right)=\mu_E\,\left(\frac{\gamma}{\beta}\right)\,\det\iota_{E/F}\,\left(\frac{\gamma}{\beta}\right),$$

if $\iota_{E/F}$ is the representation of $W_{K/F}$ induced from the trivial representation of $W_{K/E}$. We are reduced to showing that

$$\det\iota_{E/F}\,\left(\frac{\gamma}{\beta}\right)\,\{\Delta(\chi_F,\psi_F)\}^r=\Delta(\chi_{E/F},\psi_{E/F})\,\rho(E/F,\psi_F)\tag{22.1}$$

if $m(\chi_F)$ is sufficiently large. Of course $r=[E:F]$.

What we do is show that for each Galois extension K/F the relation (22.1) is true for all fields E lying between K and F. For this we use induction on $[K:F]$. Let $G = \mathfrak{G}(K/F)$ and let C be a non-trivial abelian normal subgroup of G. Let L be the fixed field of C. We saw in Chapter 13 that there are fields $F_1, \dots, F_s$ lying between F and L and generalized characters $\mu_1, \dots, \mu_s$ of $C_{F_1}, \dots, C_{F_s}$ respectively such that

$$\iota_{E/F} \simeq \oplus_{i=1}^{s} \mathrm{Ind}(W_{K/F}, W_{K/F_i}, \mu_i).$$

Then

$$\chi_F \otimes \iota_{E/F} \simeq \oplus_{i=1}^{s} \mathrm{Ind}(W_{K/F}, W_{K/E_i}, \mu_i\, \chi_{F_i/F})$$

and by Theorem 2.1, the Main Theorem, the right side of (22.1) is equal to

$$\prod_{i=1}^{s} \Delta(\mu_i\, \chi_{F_i/F}, \psi_{F_i/F})\, \rho(F_i/F, \psi_F).$$

We just saw that if $m(\chi_F)$ is sufficiently large this is equal to

$$\left\{\prod_{i=1}^{s} \mu_i \left(\frac{\gamma}{\beta}\right)\right\} \left\{\prod_{i=1}^{s} \Delta(\chi_{F_i/F}, \psi_{F_i/F})\, \rho(F_i/F, \psi_F)\right\}.$$

Since

$$\sum_{i=1}^{s} [F_i : F] = [E : F]$$

we see upon applying the induction assumption to L/F that this equals

$$\left\{\prod_{i=1}^{s} \mu_i \left(\frac{\gamma}{\beta}\right) \det \iota_{F_i/F} \left(\frac{\gamma}{\beta}\right)\right\} \{\Delta(\chi_F, \psi_F)\}^r.$$

We complete the proof of (22.1) by appealing to Chapter 5 to see that

$$\det \iota_{E/F} = \prod_{i=1}^{s} \mu_i \det \iota_{F_i/F}.$$

References

1. Artin, E., *Zur Theorie der L - Reihen mit allgemeinen Gruppencharakteren,* Collected Papers, Addison–Wesley
2. Artin, E., *Die gruppentheoretische Struktur der Diskriminanten algebraischer Zahlkörper,* Collected Papers, Addison–Wesley
3. Artin, E. and Tate, J., *Class Field Theory,* W.A Benjamin, NY
4. Brauer, R. and Tate, J, *On the characters of finite groups,* Ann. of Math. **62** (1955)
5. Davenport, H. and Hasse, H., *Die Nullstellen der Kongruenzzetafunktion in gewissen zyklischen Fällen,* Jour. für Math. **172** (1935)
6. Dwork, B., *On the Artin root number,* Amer. Jour. Math. **78** (1956)
7. Hall, M., *The Theory of Groups,* Macmillan, N.Y. (1959)
8. Hasse, H., *Artinsche Führer, Artinsche L - Funktionen und Gauss'sche Summen über endlich-algebraischen Zahlkörpern,* Acta Salmanticensia (1954)
9. Lakkis, K., *Die galoisschen Gauss'schen Summen von Hasse,* Dissertation, Hamburg (1964)
10. Lamprecht, E., *Allgemeine Theorie der Gauss'schen Summen in endlichen kommutativen Ringen,* Math. Nach. **9** (1953)
11. Mackenzie, E. and Whaples, G., *Artin–Schreier equations in characteristic zero,* Amer. Jour. Math **78** (1956)
12. Serre, J.-P., *Corps locaux,* Hermann. (1962)
13. Tate, J., *Fourier Analysis in Number Fields and Hecke's Zeta-functions,* Thesis, Princeton (1950)
14. Weil, A., *Numbers of solutions of equations in finite fields,* Bull. Amer. Math. Soc. **55** (1949)
15. Weil, A., *Sur la théorie du corps de classes,* Jour. Math. Soc. Japan, **3** (1951)
16. Weil, A., *Basic Number Theory,* Springer-Verlag, (1967)