On the Root Number in the Functional Equation of the Artin-Weil L-series.

by Bernard M. Dwork.

April 1954

Submitted in partial fulfillment of the requirements for the degree of Doctor of Philosophy in the Faculty of Pure Science, of Columbia University.

ABSTRACT

On the Root Number in the Functional Equation of the Artin-Weil L-series.

Bernard M. Dwork

The Artin concept of conductors of characters of galois groups of number fields may be extended to characters of Weil groups. These conductors, themselves of interest, lead by the methods of Artin to the functional equation of the Weil L-series. The problem of determining the root number appearing in this functional equation is studied with emphasis upon the possibility of decomposing the root number into factors which depend only upon the local behavior of the character. A decomposition exists if the Tate factors (i.e. the factors appearing in the functional equation of the local zeta functions of Tate) may be extended in a natural manner to characters of local Weil groups (decomposition subgroups of Weil groups). The investigation of Tate factors indicated by this line of reasoning gives the main result of the thesis: If K is an abelian extension of a local number field, k, X is a character of K^* trivial on the kernel in K^* of the relative norm, and $\sigma_1, \ldots, \sigma_n$ is the set of all characters of k whose composition with the relative norm is X, then the ratio between the Tate factor for X and the product of the factors for $\sigma_1, \ldots, \sigma_n$ is a fourth root of unity depending only upon the conductor of X and the square of the ratio depends only upon the norm group and the relative degree. It follows that at best the fourth power

of the Tate factors may be extended to characters of the local Weil groups. The conjecture that the fourth power may indeed be so extended is verified under a restrictive hypothesis, from which it follows that the root number associated with the Weil L-series, L(s,X,K/k), may be decomposed modulo the fourth roots of unity if K/k is locally cyclic. The same conclusion holds for the Artin L-series if K is an abelian extension of an intermediate field which is normal over k and locally cyclic.

Introduction

Let k be a number field, C_k the group of idele classes, D_k the connected component of the unit element in C_k. The abelian L-series may be described as an Euler product over the primes of k involving a character of the factor group C_k/D_k. By class field theory such a character may be identified with a character of the galois group of a cyclic extension of k. The step from L-series with characters of C_k/D_k to L-series with characters of C_k ("Grossencharakter" in the ideal-theoretic formulation) was taken by Hecke (1) who proved that these L-series have an analytic continuation over the entire complex plane, that they satisfy a functional equation of the classical type and that the L-series is analytic over the entire complex plane if the character is non-trivial on the largest compact subgroup of C_k. Applying Fourier analysis of locally compact abelian groups to the idele group, Tate(2) developed a much simpler proof of these results and in addition gave in terms of the local behavior of the character a canonical formulation of the factors which appear in the functional equation. This is of great importance for our work.

(1) Hecke, E. "Uber eine neue Art von Zetafunctionen und ihre Beziehungen zur Verteilung der Primzahlen", Math. Zeitschr., Vol 1, 1918 and Vol 4, 1920.
(2) Tate, J. "Fourier Analysis in Number Fields and Hecke's Zeta Functions", Thesis, Princeton Univ., 1950 (unpublished).

In a somewhat different direction, by using the average value on a Frobenius class of a character of the galois group of a normal extension of k, Artin (3),(4), constructed non-abelian L-series. Artin showed that these L-series satisfy a functional equation of classical type but with an undetermined unimodular factor, a global root number independent of the complex variable appearing in the functional equation. Brauer (5) showed that each character of a finite group is a linear combination with integral coefficients of characters induced by linear characters of subgroups. This completed the proof that the non-abelian L-series may be expressed as a product of abelian L-series and therefore have an analytic continuation throughout the complex plane.

These extensions of the abelian L-series are unified inthe L-series of Weil(6), constructed with characters of the Weil group, the group extension of C_K by the galois group, G(K/k), corresponding to the canonical cohomology class. By extending Brauer's result to characters of the Weil group, Weil proved that these L-series may be expressed as a product of Hecke L-series and therefore are meromorphic over the entire complex plane.

Chevalley suggested that I extend to these last L-series, Tate's treatment of the Hecke L-series. Artin pointed out that a good

---

(3) Artin, E. "Uber eine neue Art von L-Reihen", Abh. Math. Sem. Hamburgischen Univ. vol.3 (1923) pp. 89-108.
(4) Artin, E. "Zur Theorie der L-Reihen mit allgemeinen Gruppencharakteren", Ibid, vol.8 (1931) pp. 292-306.
(5) Brauer, R. "On Artin's L-Series with General Group Characters" Annals of Math., vol.48, no.2,(1947) pp. 502-514.
(6) Weil, A.,"Sur la theorie du Corps de Classes" J.Math.Soc.of Japan,vol3,(1951)

extension of Tate's local zeta function would give a determination of the root number appearing in the functional equation of his L-series. Indeed, such an extension would give an extension of the Tate factors (the factors appearing in the functional equation of Tate's local zeta function). This would in particular give the theory of the Artin non-abelian conductor(7) and considerable information concerning the local root numbers described in chapter II (generalizations of Gauss sums). This information would be read off in much the same way that the conductor discriminant formula, a relation between abelian conductors, is obtained from Artin's non-abelian conductor.

While extensions of the Tate local zeta functions were constructed, none had the properties (listed in Chapter IV) necessary for a simple theory. This led to the question of whether the Tate factors could be extended in the desired manner. Without the construction of an extension, this question could be answered only by a closer examination of the Tate coefficients. Once it is known how to extend the abelian conductor, the only difficult part of the Tate factor is the local root number. Explicit formulae for these numbers exist but are difficult to apply as various cases must be treated separately. For this reason the results appearing here depend upon a detailed consideration of special cases. These results involve the approximation of multiplicative characters of non-archimedean local fields by expressions of the

Artin, E. "Die gruppen theoretische Structure der Discriminanten algebraischer Zahlkorper", Journal fur Math. vol. 164 (1931) v.

type, $\theta(ax+bx^2)$, where θ is an additive character. Further development appears to depend upon refinement of this approximation, a refinement which seems to be feasible.

For completeness, Artin's functional equation is extended to the Weil L-series. The corresponding theory of conductors of characters of Weil groups is developed at the beginning so that some of the consequences may be used in the susequent theory.

I wish to express to Artin, Chevalley and Tate my gratitude for suggesting the topic and for continued advice and encouragement.

Chapter I

Local Conductor

In the following k is a $\mathfrak{p}$-adic number field and K is a normal extension of finite degree. $W_{K/k}$, the local Weil group, is the group extension of K^* by the galois group, G(K/k), corresponding to the canonical cohomology class. By character we mean the trace of a continuous representation by unitary matrices. The problem is to extend the Artin conductor of a character of a finite galois group to a conductor of characters of $W_{K/k}$. The Artin definition is in terms of the ramification subgroups of the galois group. As $W_{K/k}$ is essentially the galois group of A_K/k (where A_K is the maximal abelian extension of K), it would appear that the definition could be extended by means of the Hilbert theory of this infinite extension. However, the Artin definition does not go over directly even in the most simple case (K=k) and for this reason a different proceedure was used.

As A_K is an algebraic extension of k, there exists a valuation, P, of A_K with the property that for each subfield, M, of finite degree over k, the restriction of P to M is precisely that valuation of M which coincides on k with $\mathfrak{p}$. Let A_t be the inertial subfield of A_K/k. The restriction P_t of P to A_t is discrete and therefore the Hilbert theory of finite extensions of A_t has a simple structure. The relative different $\mathfrak{D}_{E/F}$, for $A_K \supset E \supset F \supset A_t$, E/A_t finite, may be difined in the usual way and in this connection the relative discriminant, $D_{E/F}$, is simply defined to be $N_{E/F}\mathfrak{D}_{E/F}$. The associated theory need not be discussed here.

In the following, unless otherwise stated, all fields lie in A_K and contain k. If E/F normal and otherwise as above and χ a character of G(E/F), then following Artin we define the conductor of χ to be $f_0(\chi, E/F) = \mathfrak{P}^r$, $\mathfrak{P}$ being the prime of F and

$$r = [\mathcal{W}_0]^{-1} \Sigma_{i=0} \Sigma_{x \in \mathcal{W}_i} (\chi(1) - \chi(x))$$

where $\mathcal{W}_0$ is the inertial subgroup of $G(E/F)$ (i.e. the whole group) and $\mathcal{W}_i$ is the i-th ramification subgroup for i not zero.

Conductors of this type may be expressed in terms of conventional Artin conductors. For E, F as above, there exists an element, α, of E such that $E=F(\alpha)$. Let M be any galois extension of k of finite degree containing α. Let $F'=M\cap F$; $E'=M\cap E$. We assert that E'/F' is normal and that $E=E'F$. Every automorphism of M/F' is the restriction to M of an element of $G(A_K/F')$, which is the group theoretic union of $G(A_K/M)$ and $G(A_K/F)$. Hence the automorphisms of M/F' are the restrictions to M of the elements of $G(A_K/F)$. As the elements of $G(A_K/F)$ map E onto itself, the elements of $G(M/F')$ map E' onto itself, whence E'/F' is normal. It follows that $E\supset E'F$, $\deg(E'/F')=\deg(E'F/F)$, $\deg(M/F')=\deg(MF/F)$, $\deg(M/E')=\deg(MF/E)$, whence $E=E'F$. As F A_t, E'/F' is purely ramified. Let π be a prime element of E', then $E'=F'(\pi)$, $E=F(\pi)$ and the natural isomorphism between $G(E/F)$ and $G(E'/F')$ can be expressed in terms of the effects of automorphisms on π. As the ramification subgroups may be described in terms of congruences involving the effects of automorphisms on π, and as the valuation of E' is the restriction of the valuation of E it is trivial that the natural isomorphism between the two galois groups maps the ramification subgroup of given order of one galois group onto the ramification subgroup of the same order of the other group.

With this construction, if χ is a character of $G(E/F)$ then by the natural isomorphism we may construct a character χ' of $G(E'/F')$ which has a conventional Artin conductor, $f(\chi',E'/F')$. It follows from the above that $\text{ord}_{\mathfrak{p}}\, f(\chi',E'/F') = \text{ord}_{\mathfrak{p}}\, f_0(\chi,E/F)$, where $\mathfrak{p}$ is the prime of F'.

From the above construction and the properties of the Artin conductor, it follows that :

1. If χ and χ' are characters of $G(E/F)$ then $f_0(\chi+\chi',E/F)=$

$f_o(\chi, E/F)\ f_o(\chi', E/F)$.

2. If L is a finite extension of E, L normal over F, χ' a character of G(L/F) which is trivial on G(L/E) and which, by passage to quotients, gives a character χ of G(E/F), then $f_o(\chi', L/F) = f_o(\chi, E/F)$.

3. If $E \supset L \supset F$, ψ a character of G(E/L), χ_ψ, the induced character of G(E/F), then

$$f_o(\chi_\psi, E/F) = D_{L/F}^{\psi(1)}\ N_{L/F} f_o(\psi, E/L).$$

4. $f_o(\chi, E/F)$ is an integral power of $\mathfrak{y}$.

These are the only properties of the conductors f_o that will be needed.

Let χ be a character of $W_{K/k}$. Its kernel in H, the inertial subgroup of the Weil group, is a closed invariant subgroup of H. The finiteness of the index follows from the fact that U_K, the group of units in K, is of finite index in H and χ splits into a finite set of linear characters on U_K, all of which are trivial on some subgroup of U_K of finite index. Hence the kernel of χ in H determines a galois extension L of A_t of finite degree and by passage to quotients a character χ_L of $G(L/A_t)$ is obtained. The conductor, $F(\chi, K/k)$, of χ is defined to be $\mathfrak{y}^r$, where $r = \text{ord}_{P_t} f_o(\chi_L, L/A_t)$.

We first observe that if L' is any normal extension of finite degree of A_t which contains L then again by passage to quotients a character $\chi_{L'}$ of $G(L'/A_t)$ is obtained from χ. It follows from property 2. that $\text{ord}_{\mathfrak{y}} F(\chi, K/k) = \text{ord}_{P_t} f_o(\chi_{L'}, L'/A_t)$.

If χ, χ' are characters of $W_{K/k}$ then there exists a finite normal extension E of A_t such that the image of $G(A_K/E)$ in H lies in the kernels of both χ and χ' and therefore in the kernel of $\chi + \chi'$. It now follows from the previous paragraph and from the corresponding property for the conductors f_o that

$F(\chi+\chi', K\ k) = F(\chi, K\ k)F(\chi', K\ K)$.

This definition of conductor extends that of Artin in the following manner. If χ is a character of $W_{K/k}$ whose kernel is of finite index in $W_{K/k}$ then this kernel determines a finite normal extension, M, of k. Then $L=MA_t$ is the extension of A_t determined by the kernel of χ in H and by the arguments appearing in the construction, if χ_M is the character of G(M/k) obtained by passage to quotients, then $f(\chi_M, M\ k) = F(\chi, K/k)$. In particular, if K = k, then the Weil group is k and a linear character may be replaced by a linear character, χ, whose kernel is of finite index in k without changing either the class field conductor or the conductor in the new sense. It follows from the corresponding property of the Artin conductor that in this case the class field conductor is the same as the new conductor.

We now prove the

<u>Induced Character Theorem</u>

If $K \supset \Omega \supset k$, ψ a character of $W_{K/\Omega}$, χ, the induced character of $W_{K/k}$ then $F(\chi, K\ k) = D_{\Omega/k}^{\psi(1)}\ N_{\Omega/k} F(\psi, K/\Omega)$.

<u>Proof</u>

Let: be the prime of K, η that of Ω, y that of k

$f, \bar{f}, f'$ be the residue class degrees of K/k, K/Ω, Ω/k resp.

$e, \bar{e}, e'$ be the corresponding relative ramifications

be the inertial subgroups of G(K/k), G(K/Ω) resp.

τ be any element in the Frobenius class of G(K/k)

$\{\alpha_i\}$ be a set of representatives of right cosets of $\bar{\mathcal{I}}$ in $\mathcal{I}$

H be the inertial subgroup of $W_{K/k}$.

Then $\mathcal{I} = \bigcup_{i=1}^{e'} \bar{\mathcal{I}}\alpha_i$ whence $G(K/k) = \bigcup_{j=0}^{f-1} \mathcal{I}\tau^j = \bigcup_{r=0,\, s=0}^{\bar{f}-1\;\; f'-1} \mathcal{I}\tau^{f'r}\tau^s$

As the Frobenius class of $G(K/\Omega)$ is $\mathcal{I}\tau^{f'} \cap G(K/\Omega)$, if we pick $\bar{\tau}$ in this class then there exists $\alpha \in \mathcal{I}$ such that $\tau^{f'} = \alpha\bar{\tau}$,

whence $G(K/k) = \bigcup_{r=0,\, s=0}^{\bar{f}-1\;\; f'-1} \mathcal{I}(\alpha\bar{\tau})^r\tau^s$

$$= \bigcup_{r,s} \mathcal{I}\tau^s$$
$$= \bigcup_{r=0,\, s=0,\, i=1}^{\bar{f}-1\;\; f'-1\;\; e'} \bar{\tau}^r\bar{\mathcal{I}}\alpha_i\tau^s$$
$$= \bigcup_{s=0,\, i=1}^{f'-1\;\; e'} G(K/\Omega)\alpha_i\tau^s$$

Letting s_i be a representative in H of α_i ($1 \le i \le e'$)

t be a representative of τ.

we have $W_{K/k} = \bigcup_{j=0,\, i=1}^{f'-1\;\; e'} W_{K/\Omega}\, s_i t^j$. Hence for $x \in W_{K/k}$,

$\chi(x) = \Sigma_{j=0,\, i=1}^{f'-1\;\; e'} \psi(s_i t^j x\, t^{-j} s_i^{-1})$, where as usual $\psi(x) = 0$ for x not in $W_{K/\Omega}$.

Let $\Omega_j = \tau^{-j}\Omega$ ($0 \le j \le f'-1$, $\Omega_0 = \Omega$)

$\mathcal{I}_j$ be the inertial subgroup of $G(K/\Omega_j)$

H_j be the inertial subgroup of W_{K/Ω_j}

Then $\beta \to \tau^{-j}\beta\tau^j$ is an isomorphism of $G(K/\Omega)$ onto $G(K/\Omega_j)$ and $\bar{\mathcal{I}}_j = \tau^{-j}\bar{\mathcal{I}}\tau^j$, $H_j = t^{-j} H_0 t^j$

$$\mathcal{I} = \bigcup_{i=1}^{e'} \mathcal{I}\alpha_i = \bigcup_{i=1}^{e'} (\tau^{-j}\bar{\mathcal{I}}\tau^j)(\tau^{-j}\alpha_i\tau^j) = \bigcup_{i=1}^{e'} \bar{\mathcal{I}}_j(\tau^{-j}\alpha_i\tau^j)$$

Whence $H = \bigcup_{i=1}^{e'} H_j\,(t^{-j} s_i t^j)$.

Let ψ_0 be the restriction of ψ to H_0, then $x \to \psi_0(t^j x\, t^{-j})$

is a character, ψ_j, of $\overline{H}_j$. Let χ_j be the character of H induced by ψ_j on $\overline{H}_j$, then for $x \in H$

$$\chi_j(x) = \Sigma_{i=1}^{e'} \psi_j(t^{-j}s_i t^j x t^{-j} s_i^{-1} t^j)$$

$$= \Sigma_{i=1}^{e'} \psi_0(s_i t^j x t^{-j} s_i^{-1}),$$ where ψ_0 is taken to be zero outside of $\overline{H}_0$.

Let χ' be the restriction of χ to H. For $x \in H$, we have: $s_i t^j x t^{-j} s_i^{-1} \in W_{K/\Omega} \Leftrightarrow s_i t^j x t^{-j} s_i^{-1} \in W_{K/\Omega} \cap H = \overline{H}_0$. It follows that $\chi' = \Sigma_{j=0}^{f'-1} \chi_j$.

We now pick a finite extension L of KA_t such that L/A_t is normal and such that $G(A_K/L)$ lies in the kernels of each of the characters χ_j, ψ_j $(0 \leq j \leq f'-1)$.

Let U' be $G(A_K/L)$ (and its replica in H),

$x \to \check{x}$ be the natural map of H onto $G(L/A_t)$,

$\check{\chi}_j$ be the character of $G(L/A_t)$ obtained from χ_j by passage to quotients,

$\check{\psi}_j$ be the character of $G(L/\Omega_j A_t)$ obtained from ψ_j by passage to quotients.

$\check{\chi}$ be the character of $G(L/A_t)$ obtained from χ' by passage to quotients.

Certainly, $\check{\chi} = \Sigma_{j=0}^{f'-1} \check{\chi}_j$, but in addition $\check{\chi}_j$ is induced by the character $\check{\psi}_j$ of $G(L/\Omega_j A_t)$ as is shown by the following

<u>Lemma</u> Let G be a group, H a subgroup of finite index, ψ a character of H whose kernel is a subgroup of H of finite index. Let χ be the induced character of G. Then there exists a subgroup g of H of finite index, invariant in G which lies in the kernels

of both ψ and χ. If $\check{H} = H/g$, $\check{G} = G/g$, $\check{\psi}$ the character of $\check{H}$ obtained from ψ by passage to quotients then $\check{\chi}$ is induced by $\check{\psi}$. (where $\check{\chi}$ is the character of $\check{G}$ obtained from χ).

Proof Let $G = \bigcup_{j=1}^{n} H\beta_j$, a disjoint union, then for $x \in G$
$\chi(x) = \Sigma_{j=1}^{n} \psi(\beta_j x \beta_j^{-1})$. If H' is the kernel of ψ in H then as the unit matrix is the only unitary matrix whose trace equals its rank we have $\psi(1) = \psi(\beta_j x \beta_j^{-1}) \Leftrightarrow \beta_j x \beta_j^{-1} \in H' \Leftrightarrow x \in \beta_j^{-1} H' \beta_j$
Hence $\chi(x) = n\,\psi(1) \Leftrightarrow x \in \bigcap_{j=1}^{n} \beta_j^{-1} H' \beta_j$, whence the kernel of χ lies in H' and is the intersection of subgroups of G of finite index. This kernel satisfies the conditions in the statement of the lemma and therefore g exists.

Now let $\check{\beta}_j$ be the image of β_j in $\check{G}$, then $(G:H) = (\check{G}:\check{H})$, and therefore $\check{G} = \bigcup_{j=1}^{n} \check{H}\check{\beta}_j$, a disjoint union. For $\check{x} \in \check{G}$, let x be a representative in G, then $\check{\chi}(\check{x}) = \Sigma_{j=1}^{n} \check{\psi}(\widecheck{\beta_j x \beta_j^{-1}}) = \Sigma\, \check{\psi}(\check{\beta}_j \check{x} \check{\beta}_j^{-1})$ whence $\check{\chi}$ is induced by $\check{\psi}$, which completes the proof of the lemma.

Continuing with the proof of the theorem,
$\mathrm{ord}_y F(\chi, K/k) = \mathrm{ord}_{P_t} f_0(\check{\chi}, L/A_t)$, while $f_0(\check{\chi}, L/A_t) =$

$$\prod_{j=0}^{f'-1} f_0(\check{\chi}_j, L/A_t) = \prod_{j=0}^{f'-1} \left\{ D_{\Omega_j A_t/A_t}^{\psi_j(1)} N_{\Omega_j A_t/A_t} f_0(\check{\psi}_j, L/\Omega_j A_t) \right\}$$

$$= \left(\prod_{j=0}^{f'-1} D_{\Omega_j A_t/A_t}\right)^{\psi(1)} \prod_{j=0}^{f'-1} N_{\Omega_j A_t/A_t} f_0(\check{\psi}_j, L/\Omega_j A_t).$$

To complete the proof we must show

(a) $\mathrm{ord}_y N_{\Omega/k} F(\psi, K/\Omega) = \mathrm{ord}_{P_t} \left\{ \prod_{j=0}^{f'-1} N_{\Omega_j A_t/A_t} f_0(\check{\psi}_j, L/\Omega_j A_t) \right\}$

(b) $\mathrm{ord}_y D_{\Omega/k} = \mathrm{ord}_{P_t} \prod_{j=0}^{f'-1} D_{\Omega_j A_t/A_t}$

Proof of (a) :

$\mathrm{ord}_y N_{\Omega/k} F(\psi, K/\Omega) = f' \,\mathrm{ord}_{\mathcal{N}} F(\psi, K/\Omega)$. As $\Omega_j A_t$ is inertial subfield of A_K/Ω, it follows from the definitions that if P_{Ω_j} is the prime of $\Omega_j A_t$ $(0 \leq j \leq f'-1)$, then $\mathrm{ord}_{\mathcal{N}} F(\psi, K/\Omega) = \mathrm{ord}_{P_{\Omega_0}} f_0(\psi_0, L/\Omega_0 A_t)$. Hence it is enough to show that

$\mathrm{ord}_{P_{\Omega_j}} f_0(\check{\psi}_j, L/A_t\Omega_j)$ is independent of j. But this is clear as $\overline{H}_0$ and $\overline{H}_j$ are related by an inner isomorphism of H which gives the relation between ψ_0 and ψ_j and therefore the same holds for the groups $G(L/\Omega_0 A_t)$ and $G(L/\Omega_j A_t)$ and their respective characters $\check{\psi}_0$, $\check{\psi}_j$ (here the relation is by an inner automorphism of $G(L/A_t)$) whence the assertion follows from the topological properties of elements of $G(L/A_t)$ so far as valuations are concerned.

Proof of (b):

$D_{\Omega_j A_t/A_t} = N_{\Omega_j A_t/A_t}[\mathfrak{d}_{KA_t/A_t}\,\mathfrak{d}_{KA_t/\Omega_j A_t}] = \mathfrak{y}^r$, r independent of j by the same argument as above (namely that $G(KA_t/\Omega_j A_t)$ is the image of $G(KA_t/\Omega A_t)$ under an inner automorphism of $G(KA_t/A_t)$). Furthermore $D_{\Omega/k} = N_{\Omega/k}\,\mathfrak{d}_{\Omega/k} \Rightarrow \mathrm{ord}_{\mathfrak{y}} D_{\Omega/k} = f'\, \mathrm{ord}_{\mathfrak{y}}\mathfrak{d}_{\Omega/k}$. Hence it is enough to show that $\mathrm{ord}_{P_{\Omega_0}} \mathfrak{d}_{\Omega A_t/A_t} = \mathrm{ord}_{\mathfrak{y}}\mathfrak{d}_{\Omega/k}$. Letting T be the inertial subfield of K/k, and $\mathfrak{y}'$ be the prime of ΩT, we have $\mathfrak{d}_{\Omega T/\Omega}\,\mathfrak{d}_{\Omega/k} = \mathfrak{d}_{\Omega T/k} = \mathfrak{d}_{\Omega T/T}\,\mathfrak{d}_{T/k}$ whence $\mathrm{ord}_{\mathfrak{y}}\mathfrak{d}_{\Omega/k} = \mathrm{ord}_{\mathfrak{y}'}\mathfrak{d}_{\Omega T/T}$

By the nature of the isomorphism between $G(KA_t/A_t)$ and $G(K/T)$ which by restriction gives the isomorphism between $G(KA_t/A_t\Omega)$ and $G(K/T\Omega)$. The assertion follows using

$$\mathfrak{d}_{\Omega A_t/A_t} = \frac{\mathfrak{d}_{KA_t/A_t}}{\mathfrak{d}_{KA_t/\Omega A_t}}, \quad \mathfrak{d}_{\Omega T/T} = \mathfrak{d}_{K/T}/\mathfrak{d}_{K/\Omega T}$$

This completes the proof of the theorem.

The treatment of the local theory is completed with:

Lemma

Let $K \supset L \supset k$, K and L normal over k, τ the topological homomorphism of $W_{K/k}$ onto $W_{L/k}$ with kernel $W^c_{K\ L}$ which extends the transfer homommorphism $\mathcal{V}_{W_{K/L} \to K^*}$. Let ψ be a character of $W_{L/k}$ then $F(\psi \circ \tau, K/k) = F(\psi, L/k)$.

Proof Let H be the inertial subgroup of $W_{K/k}$, then $\tau(H) = \bar{H}$, the corresponding subgroup of $W_{L/k}$. As the factor group $W_{K/k}/H$ is cyclic and H is closed, $H \supset$ $W^c_{K/k}$, the closure of the commutator subgroup of $W_{K/k}$. Hence $\tau^{-1}(\bar{H}) = H$. It follows that if $\bar{H}'$ is the kernel of ψ in $\bar{H}$ then $\tau^{-1}(\bar{H}') = H'$, the kernel of $\psi \circ \tau$ in H. If as above, A_t is the inertial subfield of A_K/k, then A_t/k is certainly abelian, whence $A_t \subset A_K \subset A_L$. Therefore the inertial subfield of A_L/k is $A_t \cap A_L = A_t$. Identifying H with $G(A_K/A_t)$, $\bar{H}$ with $G(A_L/A_t)$, the kernel of τ is $G(A_K/A_L)$. Hence if $\bar{H}'$ determines an extension, E, of A_t in A_L, then $\bar{H}'$ is identified with $G(A_L/E)$ and $H' = \tau^{-1}(\bar{H}')$ is identified with $G(A_K/E)$. Furthermore if $\sigma \in G(A_K/A_t)$ then $\tau(\sigma)$ may be identified with the restriction of σ to A_L, whence the restriction of σ to E is the same as the restriction of $\tau(\sigma)$ to E. Hence the characters of $G(E/A_t)$ obtained from ψ and $\psi \circ \tau$ by passage to quotients are identical. Thus, $\text{ord}_y F(\psi, L\ k) = \text{ord}_{p_t}\ f_0(\psi_E, E/A_t)$ $= \text{ord}_y F(\psi \circ \tau, K/k)$.

This completes the local treatment. The development of the global theory is deferred as it is part of a more general problem of extending local results of this type to the global case.

Application

In the following K/k is abelian of degree n, k a $\mathfrak{y}$-adic number field. The group of characters of k^* which are trivial on the norm group is $\{\tau_j\}_{j=1}^{n}$. The conductor of τ_j is $\mathfrak{y}^{1+s_j}$ ($1 \leq j \leq n$), f is the relative residue class degree and f_a is the absolute degree of $\mathfrak{y}$. Let $\mathfrak{P}$ be the prime of K and $g_{K/k}$ (or more simply, g) a mapping of integers into rationals defined by:

$$1 + g(b) = (1/f)\ \Sigma_{s_j<b}\ (b-s_j).$$

As one of the elements τ_j is the principal character of k^*, at least one of the integers, s_j, is -1. This is the smallest possible value for the s_j. We note that for $b \geq -1$, $g(b+1) > g(b)$ as the number of terms appearing in the sum is not zero for $b \geq 0$, each term is greater than zero and increases strictly with b and the number of terms increases with b. The unramified characters in $\{\tau_j\}_{j=1}^{n}$ form a subgroup of order f, from which it follows that in the set of integers, $(s_1, \ldots, s_n)$, each distinct integer occurs a multiple of f times. Hence g(b) is an integer. We now need a simple preliminary result.

Lemma If λ is any linear character of K^*, trivial on the kernel of $N_{K/k}$ in K^*, and χ is the character of $W_{K/k}$ induced by λ then there exist characters μ of k^* such that $\lambda = \mu \circ N_{K/k}$ and for any such μ, $\chi = \Sigma_{j=1}^{n} (\mu\tau_j) \circ \mathcal{V}_{W_{K/k} \to K^*}$. (The last symbol denotes the transfer homomorphism)

Proof For simplicity let $\mathcal{V}$ denote the transfer homomorphism. Certainly there exists a character, μ, of k^* such that $\lambda = \mu \circ N_{K\ k}$

and of course λ is invariant under $G(K/k)$ (i.e. for $x \in K^*$, $\alpha \in G(K/k)$, we have $\lambda(x) = \lambda(x^\alpha)$). This property shows that
$$\chi(x) = 0 \quad \text{for } x \notin K^* \qquad = n\lambda(x) \quad \text{for } x \in K^*,$$
for if $(s_\alpha)_{\alpha \in G(K\,k)}$ are a set of representatives of $G(K/k)$ in $W_{K/k}$ then for $x \in W_{K/k}$,
$\chi(x) = \Sigma_{\alpha \in G(K\,k)} \lambda(s_\alpha\, x\, s_\alpha^{-1})$, where $\lambda(x) = 0$ for $x \notin K^*$, whence

$\chi(x) = n\lambda(x)$ for $x \in K^*$, while for $x \notin K$, $s_\alpha\, x\, s_\alpha^{-1} \notin K^*$ and therefore $\chi(x) = 0$. On the other hand $x \to \mathcal{W}(x) \bmod N_{K/k}K^*$ is a homomorphism of $W_{K/k}$ onto $k^*/N_{K/k}K^*$, whence the kernel is of index n. K^* lies in the kernel and is of index n and therefore is the kernel. Hence $\mathcal{W}(x) \in N_{K/k}K^* \Leftrightarrow x \in K^*$. Now,
$$\Sigma_{j=1}^{n} (\mu\tau_j) \circ \mathcal{W}(x) = [(\mu\circ\mathcal{W})(x)] \sum_{j=1}^{n} (\tau_j \circ \mathcal{W})(x).$$
The sum is zero for $\mathcal{W}(x) \notin N_{K/k}K^*$, i.e. for $x \notin K^*$, while for x in K^* we obtain $n(\mu\circ N_{K/k})(x) = n\lambda(x)$, which proves the assertion.

<u>Definition</u> An integer m is said to be admissible with respect to K/k if there exists a character λ of K^* which is trivial on K_N^* and has conductor $\mathfrak{P}^{1+m}$. (K_N^* denotes the kernel of $N_{K/k}$ in K^*).

The theory of the conductor may be applied to the problem of determining the admissible integers.

<u>Lemma</u> If m is admissible with respect to K/k then there exists a unique integer b ($b \geq -1$), such that $m = g(b)$. If λ is a character of K^*, trivial on K_N^* and of conductor $\mathfrak{P}^{1+m}$, then there exists a character μ of k^* of conductor $\mathfrak{p}^{1+b}$ such that $\lambda = \mu\circ N_{K/k}$.

Furthermore the conductor of μ divides the conductor of $\mu\tau_j (1 \leq j \leq n)$, i.e. $b = \mathrm{Min}_{1 \leq j \leq n} \mathrm{ord}_{\mathfrak{y}} F(\mu_0\tau_j, k/k)$, where $\mu_0 \circ N_{K/k} = \lambda$.

<u>Proof</u> As λ is trivial on K_H^*, there exists μ_0, a character of k^* such that $\mu_0 \circ N_{K/k} = \lambda$. The coset $\{\mu_0\tau_j\}_{j=1}^{n}$ is the set of all characters of k^* whose composition with $N_{K/k}$ is λ. Among the elements of this set, pick one, μ, which has the property that the conductor of μ divides the conductor of each element of the set. Then $\mu \circ N_{K/k} = \lambda$ and the conductor of μ divides the conductor of $\mu\tau_j$ for each j between 1 and n. From the preceeding lemma, χ, the character of $W_{K/k}$ induced by λ is $\Sigma_{j=1}^{n} (\mu\tau_j) \circ \mathcal{W}$, whence by the properties of the conductor:

$$\prod_{j=1}^{n} F(\mu\tau_j, k/k) = \prod_{j=1}^{n} F((\mu\tau_j)\circ \mathcal{W}, K/k) = F(\chi, K/k)$$

$$= D_{K/k}^{\lambda(1)} \; N_{K/k} F(\lambda, K/K).$$

By the conductor-discriminant formula, $D_{K/k} = \prod_{j=1}^{n} F(\tau_j, k/k)$, whence

$$\mathfrak{y}^{(1+m)f} = N_{K/k} F(\lambda, K/K) = \prod_{j=1}^{n} \frac{F(\mu\tau_j, k/k)}{F(\tau_j, k/k)}$$

We now compute this last expression. If μ_1, μ_2, are characters of k^* and have conductors $\mathfrak{y}^{1+c}$, $\mathfrak{y}^{1+d}$, respectively, then the conductor of $(\mu_1\mu_2)$ divides $\mathfrak{y}^{1+\mathrm{Max}(c,d)}$ and if $c \neq d$ then the conductor of $\mu_1\mu_2$ is $\mathfrak{y}^{1+\mathrm{Max}(c,d)}$. For suppose $c < d$ then μ_1 and μ_2 are both trivial on $1+\mathfrak{y}^{1+d}$, but μ_1 is trivial on $1+\mathfrak{y}^{d}$ while μ_2 is not, whence $\mu_1\mu_2$ not trivial on $1+\mathfrak{y}^{d}$, and therefore conductor $(\mu_1\mu_2) = \mathfrak{y}^{1+d}$. On the other hand if $c=d$ then $\mu_1\mu_2$ is certainly trivial on $1+\mathfrak{y}^{1+\mathrm{Max}(c,d)}$, which proves the assertion. Applying this simple result to the characters $\mu\tau_j$, we have, letting the conductor of μ be $\mathfrak{y}^{1+b}$,

$$F(\mu\tau_j, k/k) = \begin{cases} \mathfrak{y}^{1+s_j} & \text{if } b<s_j \\ \mathfrak{y}^{1+b} & \text{if } b>s_j \end{cases}$$

If $b = s_j$ then the conductor of $\mu\tau_j$ divides $\mathfrak{y}^{1+b}$ which divides the conductor of $\mu\tau_j$ by the choice of μ. Hence $F(\mu\tau_j, k/k)$ is $\mathfrak{y}^{1+s_j}$ for $b \leq s_j$. It now follows that

$$\mathfrak{y}^{f(1+m)} = \prod_{b\leq s_j} \frac{\mathfrak{y}^{1+s_j}}{\mathfrak{y}^{1+s_j}} \prod_{b>s_j} \frac{\mathfrak{y}^{1+b}}{\mathfrak{y}^{1+s_j}} ;$$

whence $m = g(b)$. Furthermore, it now follows from the properties of the function g that b is completely determined by the conductor of λ.

<u>Corollary</u>

1. If μ is a character of k^* with conductor $\mathfrak{y}^{1+b}$, then there exists an integer, b', $-1 \leq b' \leq b$, such that the conductor of $\mu \circ N_{K/k}$ is $\mathfrak{P}^{1+g(b')}$. If b is either -1 or any integer not in the set $(s_1, \ldots, s_n)$ then the conductor of $\mu \circ N_{K/k}$ is $\mathfrak{y}^{1+g(b)}$.

2. Let S be the set of all integers, t, in the set $(s_1, \ldots, s_n)$ such that $t \neq -1$ and such that $(1 + \mathfrak{y}^{t}) \cap N_{K/k}K^* = (1+ \mathfrak{y}^{1+t}) \cap N_{K/k}K^*$, then the set of all integers which are admissible with respect to K/k is $(g(b))_{b\notin S}$.

<u>Proof</u>

1. The first part of this statement follows from the fact that if $\lambda = \mu \circ N_{K/k}$ has conductor $\mathfrak{P}^{1+m}$, then $m = g(b')$, where $b' = \mathrm{Min}_{1\leq j\leq n} \mathrm{ord}_{\mathfrak{y}} F(\mu\tau_j, k/k)$, whence $b' \leq b$. For the second part of the first statement, if $b' = b$ we are through. If $b' < b$, let μ_0 be a character of k^* of conductor $\mathfrak{y}^{1+b'}$ such that $\lambda =$

$\mu_0 \circ N_{K/k}$. Then there exists j such that $\mu = \mu_0 \tau_j$. As the conductor of $\mu \neq$ the conductor of μ_0, it follows from the proof of the lemma that $b = s_j > b'$. If $b = -1$ or if b not one of the elements $(s_1, \ldots, s_n)$ this is clearly impossible.

2. For this statement we first note that if $b \geq -1$ then $g(b)$ is certainly admissible if b is either -1 or any element not in the set $(s_1, \ldots, s_n)$. From the above lemma $g(b)$ not admissible $\Leftrightarrow$ given a character, μ, of k^*, trivial on $1+\mathcal{Y}^{1+b}$, there exists τ_j (depending on μ) such that $\mu\tau_j$ is trivial on $1+\mathcal{Y}^b$. Hence if $g(b)$ not admissible and $x \in (1+\mathcal{Y}^b) \cap N_{K/k}K^*$, $x \notin 1+\mathcal{Y}^{1+b}$ then there exists θ, a character on k^* trivial on $1+\mathcal{Y}^{1+b}$ such that $\theta(x) = 1$. But there exists j such that $(\theta\tau_j)(x) = 1$ and certainly $\tau_j(x) = 1$, i.e. $\theta(x) = 1$ which is a contradiction. Hence $g(b)$ not admissable $\Rightarrow (1+\mathcal{Y}^b) \cap N_{K/k}K^* \subset 1+\mathcal{Y}^{1+b}$. Conversely if

$(1+\mathcal{Y}^b) \cap N_{K/k}K^* \subset 1+\mathcal{Y}^{1+b}$ and if θ is a character of $1+\mathcal{Y}^b$ which is trivial on $1+\mathcal{Y}^{1+b}$, then θ is trivial on $(1+\mathcal{Y}^b) \cap N_{K/k}K^*$ and is therefore the restriction to $1+\mathcal{Y}^b$ of an element of $\{\tau_j\}_{j=1}^n$, whence there exists j such that $\theta\tau_j$ is trivial on $1+\mathcal{Y}^b$, i.e. $g(b)$ is not admissible. This proves the corollary and also shows that:

$$(1+\mathcal{Y}^t) \cap N_{K/k}K^* \subset 1+\mathcal{Y}^{1+t} \Rightarrow t \text{ lies in the set } (s_1, \ldots, s_n).$$

It is easily seen that 0 not admissible with respect to K/k $\Leftrightarrow N\mathcal{Y} - 1$ divides the ramification of K/k. Also $g(b)$ not admissible $\Leftrightarrow$ the group of all characters of $1+\mathcal{Y}^b$ which are trivial on $1+\mathcal{Y}^{1+b}$ is just the restriction to $1+\mathcal{Y}^b$ of the set of all elements of $\{\tau_j\}_{j=1}^n$ with conductor $\mathcal{Y}^{1+b}$.

The main consequence of this theory is: (Let $1+\mathfrak{y}^{\circ} = U_k$, $1+\mathfrak{P}^{\circ} = U_K$, designate $N_{K/k}$ simply by N).

__Theorem__ For $b \geq 0$,

1. $N(1+\mathfrak{P}^{1+g(b)}) = (1+\mathfrak{y}^{1+b}) \cap N K^*$

2. $N(1+\mathfrak{P}^{g(b+1)}) = (1+\mathfrak{y}^{1+b}) \cap N K^*$

3. $g(b)$ admissible with respect to $K/k \Leftrightarrow N(1+\mathfrak{P}^{g(b)}) \not\subset 1+\mathfrak{y}^{1+b}$.

__Proof__ We first note that if 2. is true then $N(1+\mathfrak{P}^{g(b)}) = (1+\mathfrak{y}^{b}) \cap N K^*$, whence 3. follows from the previous corollary. Hence we need only prove 1. and 2. We pause for an elementary result:

__Lemma__ G an abelian group, $G \supset G' \supset H$, G' and H being unequal subgroups of finite index. Given $a \in G$, $a \notin H$, then there exists a character, χ, of G, trivial on H, not trivial on G' such that $\chi(a) = 1$. (In this lemma we do not insist that characters be continuous).

__Proof__ We may assume that G is a finite group and that H is the neutral element. If $\langle a\rangle \cap G' \neq \{1\}$, let b be a non-trivial element of the intersection. If the intersection is trivial, let b be any non-trivial element of G'. Let m be the period of a, then define χ on $\langle a\rangle$ by setting $\chi(a) = \zeta$, a primitive m-th root of unity. In the first case extend χ arbitrarily (as a character) to G, then certainly $\chi(b) \neq 1$, i.e. χ not trivial on G'. In the second case, a and b are linearly independent, for if $a^s = b^t$ then $a^s \in \langle a\rangle \cap G' = \{1\}$, whence $1 = a^s = b^t$. Hence we may extend χ to $\langle a,b\rangle$ by setting $\chi(b) = \zeta'$, a root of unity of order equal to the order of b and then extend χ arbitrarily to G. In either case the conditions are satisfied.

We now return to the proof of the theorem. $b \geq 0 \Rightarrow g(b) \geq 0 \Rightarrow 1 + \mathfrak{p}^{1+g(b)} \subset 1 + \mathfrak{p} \Rightarrow N(1 + \mathfrak{p}^{1+g(b)}) \subset 1 + \mathfrak{y}$. Let $a \in 1 + \mathfrak{y}$, $a \notin 1 + \mathfrak{y}^{1+b}$, then by the above there exists a character μ of k^* such that $\mu(a) \neq 1$, conductor of $\mu = \mathfrak{y}^{1+b}$. Then by the above corollary $\lambda = \mu \circ N$ has conductor $\mathfrak{p}^{1+g(b')}$, $b' \leq b$, whence μ is trivial on $N(1 + \mathfrak{p}^{1+g(b')}) \supset N(1 + \mathfrak{p}^{1+g(b)})$. But $\mu(a)$ not one, hence $a \notin N(1 + \mathfrak{p}^{1+g(b)})$. Hence $N(1 + \mathfrak{p}^{1+g(b)}) \subset 1 + \mathfrak{y}^{1+b}$. To prove inclusion in the other direction, let $a \in (1 + \mathfrak{y}^{1+b}) \cap N K^*$. Then $a = Nz$, $z \in K^*$. We assert that $z \in K^*_N (1 + \mathfrak{p}^{1+g(b)})$. Let λ be any character of K^* which is trivial on $K^*_N(1 + \mathfrak{p}^{1+g(b)})$ then $\lambda = \mu \circ N$ for some character, μ, of k^* with the property that $F(\mu, K/k)$ divides $F(\mu\tau_j, K/k)$ for all j between one and n. Let $\mathfrak{y}^{1+b'}$ be the conductor of μ then the conductor of λ is $\mathfrak{p}^{1+g(b')} \Rightarrow g(b) \geq g(b') \Rightarrow b \geq b'$ $\Rightarrow \mu$ trivial on $1 + \mathfrak{y}^{1+b'} \supset 1 + \mathfrak{y}^{1+b} \ni a \Rightarrow \mu(a) = 1 \Rightarrow \lambda(z) = (\mu \circ N)(z) = 1$. This proves the assertion concerning z, whence $a \in N(1 + \mathfrak{p}^{1+g(b)})$. This completes the proof of 1.

2. Certainly $1 + g(b) < 1 + g(b+1)$. If $g(b)+1 = g(b+1)$, then 2. is trivial. If not, let $1+g(b) < r \leq g(b+1)$. There exists no character λ of K^* trivial on K^*_N and conductor $\mathfrak{p}^r$. If a character, λ, of K^* is trivial on $K^*_N(1+\mathfrak{p}^r)$ then certainly the conductor of λ divides $\mathfrak{p}^r$; whence from the description of admissible integers, the conductor of λ divides $\mathfrak{p}^{1+g(b)}$, i.e.

every character trivial on $(1+\mathfrak{p}^r)K_N^*$ is trivial on $1+\mathfrak{p}^{1+g(b)}$ $\Rightarrow$ $(1+\mathfrak{p}^r)K_N^* \supset (1+\mathfrak{p}^{1+g(b)})K_N^*$. Inverse inclusion is trivial and therefore $N(1+\mathfrak{p}^r) = N(1+\mathfrak{p}^{1+g(b)}) = NK^* \cap (1+\mathfrak{y}^{1+b})$, which proves 2. and in addition: $(1+\mathfrak{p}^{g(b+1)})K_N^* \supset 1+\mathfrak{p}^{1+g(b)}$.

Note: For a theory of conductor of characters of Weil groups based on the theory of the infinite ramification groups, see: Tamagawa, T., "on the Theory of Ramification Groups and Conductors", Jap.J.Math., vol.21(1951) pp.197-215 (1952)

Chapter II

Local Root Numbers

In the following k is a $\mathfrak{p}$-adic number field. If χ is a character of k^* of conductor $\mathfrak{p}^n$ and ψ is a character of the additive group, k^+, of k which is trivial on $\mathfrak{p}^n$ but not on $\mathfrak{p}^{n-1}$ ($n \geq 1$, $\mathfrak{p}^0$ is $\mathfrak{o}$, the ring of integers) then the root number, (χ, ψ), of χ with respect to ψ is defined to be

$$(N\mathfrak{p}^n)^{-\frac{1}{2}} \Sigma_{x \in U/(1+\mathfrak{p}^n)} \chi(x) \psi(x) ,$$

where U is the group of units of k. If n is one then the root number is a Gauss sum. Some interesting properties of Gauss sums have been obtained by Hasse and Davenport(8) and these shall be stated shortly as we shall have occasion to refer to them in subsequent parts of this work. The major portion of this chapter shall be devoted to the determination of multiplicative expressions for root numbers for which $n > 1$. We shall refer to $\mathfrak{p}^n$ as the conductor of the root number and also as the conductor of the additive character ψ.

These root numbers appear in the functional equation of the Hecke L-series and even more explicitly in the functional equations of the local zeta functions of Tate.

If $\alpha \in k^*$ then let ψ_α be the character of k^+: $x \to \psi(\alpha x)$. If $\alpha \in U$ then trivially, ψ_α is also a character of conductor $\mathfrak{p}^n$.

(8) H. Davenport and H. Hasse, J. Reine Angew. Math. vol.172 (1935) pp.151-182.

It is easily verified that $(\chi, \psi_\alpha) = \bar{\chi}(\alpha)(\chi, \psi)$. As $\bar{\psi} = \psi_{-1}$ it follows that $(\bar{\chi}, \psi) = \chi(-1)\overline{(\chi, \psi)}$.

It is shown by Hasse and Davenport that if χ and θ are characters of conductor $\mathfrak{y}$ and m is the order of the restriction of χ to U then: $\prod_{j=0}^{m-1}(\theta\chi^j, \psi) = (\theta^m, \psi^m)\prod_{j=1}^{m-1}(\chi^j, \psi)$, with the convention that if χ_0 is trivial on U then $(\chi_0, \psi) = 1$. Furthermore if K is an unramified extension of k of degree r then subject to the same convention: $(-1)^{r-1}(\chi \circ N_{K/k}, \psi \circ S_{K/k}) = (\chi, \psi)^r$.

It is shown by Tate that the root numbers are unimodular. This is easily verified for n = 1 and for n > 1 it is an easy consequence of the statements of this chapter.

It is an unfortunate feature of this theory that the results depend upon whether or not n is even. If n is even then the theory is quite simple.

<u>Theorem</u> If (χ, ψ) has conductor $\mathfrak{y}^{2r}$ then there exists an element $\alpha \in U$ uniquely determined modulo $\mathfrak{y}^r$ by the condition: $\bar{\psi}(\alpha z) = \chi(1+z)$ for all $z \in \mathfrak{y}^r$. For α so chosen, $(\chi, \psi) = \chi(\alpha)\psi(\alpha)$.

<u>Proof</u> For $z, z' \in \mathfrak{y}^r$, $\chi(1+z)\chi(1+z') = \chi(1+z+z'+zz') = \chi(1+z+z')$ as $zz' \in \mathfrak{y}^{2r}$. Hence $z \to \chi(1+z)$ is a character of the additive group $\mathfrak{y}^r$, and therefore is the restriction to $\mathfrak{y}^n$ of some character of k^+. As ψ is not everywhere trivial on k^+, it follows from Tate's Thesis that there exists $\alpha \in k^*$ such that $\chi(1+z) = \bar{\psi}(\alpha z)$ for all $z \in \mathfrak{y}^r$. As ψ_α coincides with the

mapping $x \to \chi(1+x)$ on $\mathcal{Y}^r$, it follows that the conductor of ψ_α is the same as that of ψ. Hence α must be a unit. The uniqueness of α modulo $\mathcal{Y}^r$ follows from the fact that if ψ_β is trivial on $\mathcal{Y}^r$ then $\beta\mathcal{Y}^r \subset \mathcal{Y}^{2r}$, whence $\beta \in \mathcal{Y}^r$. This proves the first assertion concerning α. To complete the proof we note that as z runs through a set of representatives of U modulo $1+\mathcal{Y}^r$ and w through a set of representatives of $\mathcal{Y}^r$ modulo $\mathcal{Y}^{2r}$, z+w runs through a set of representatives of the distinct residue classes of U modulo $1+\mathcal{Y}^{2r}$. Hence $N\mathcal{Y}^r(\chi,\psi)$ = $\Sigma_{z,w}\chi(z+w)\psi(z+w) = \Sigma_z\psi(z)\chi(z)\,\Sigma_w\psi(w)\chi(1+wz^{-1})$. As $z \in U$, $w \in \mathcal{Y}^r$, $\chi(1+wz^{-1}) = \bar{\psi}(\alpha wz^{-1})$, whence

$$N\mathcal{Y}^r(\chi,\psi) = \Sigma_z\psi(z)\chi(z)\,\Sigma_w\psi((1-\alpha z^{-1})w).$$

The sum over w may be considered as the sum over $\mathcal{Y}^r/\mathcal{Y}^{2r}$ of a character of that group and therefore the sum is zero unless the character is the principal one, i.e. unless $\psi((1-\alpha z^{-1})w)$ is *one* for all w in $\mathcal{Y}^r$, i.e. unless $z \equiv \alpha \mod \mathcal{Y}^r$. If $z \equiv \alpha \mod \mathcal{Y}^r$, then the sum over w is $N\mathcal{Y}^r$. Taking α to be the representative of its class modulo $\mathcal{Y}^r$, the theorem follows.

The situation is somewhat more complicated when the conductor is an odd power of the prime. In the following the root number has conductor $\mathcal{Y}^{2r+1}$, $r > 0$. The above methods permit the following reduction:"

<u>Lemma</u> There exists an element $\alpha \in U$, uniquely determined modulo $\mathfrak{p}^{r}$ by the condition: $\chi(1+z) = \bar{\psi}(\alpha z)$ for all $z \in \mathfrak{p}^{r+1}$. For this α we then have:

$$(\chi, \psi) = \chi(\alpha)\psi(\alpha)\,(N\mathfrak{p})^{-\frac{1}{2}} \sum_{z \in \mathfrak{p}^{r}/\mathfrak{p}^{r+1}} \chi(1+z)\,\psi_{\alpha}(z).$$

<u>Proof</u> Precisely as before $z \mapsto \chi(1+z)$ is an additive character on $\mathfrak{p}^{r+1}$. Hence $\chi(1+z) = \bar{\psi}(\alpha z)$ for all $z \in \mathfrak{p}^{r+1}$, for some fixed element $\alpha \in k$. As before, ψ_{α} has the same conductor as ψ, and therefore α is a unit. The uniqueness of α modulo $\mathfrak{p}^{r}$ follows from the fact that ψ_{β} trivial on $\mathfrak{p}^{r+1}$ implies $\beta\mathfrak{p}^{r+1} \subset \mathfrak{p}^{1+2r}$ which implies that $\beta \in \mathfrak{p}^{r}$. This proves the first part of the lemma.

If u, v, z run through a set of representatives of U modulo $1+\mathfrak{p}^{r}$, $\mathfrak{p}^{1+r}$ modulo $\mathfrak{p}^{2r+1}$ and $\mathfrak{p}^{r}$ modulo $\mathfrak{p}^{r+1}$ respectively, then $(u+z+v)$ runs through a set of representatives of the residue classes of U modulo $\mathfrak{p}^{2r+1}$, whence $(N\mathfrak{p}^{2r+1})^{-1/2}(\chi, \psi) = \sum_{u,z,v} \chi(u+z+v)\psi(u+z+v) = \sum_{u,z} \chi(u+z)\psi(u+z) \sum_{v} \psi(v)\chi(1+\frac{v}{u+z})$.

As $v \in \mathfrak{p}^{r+1}$, $z \in \mathfrak{p}^{r}$, $u \in U$, $\frac{v}{u+z} \equiv v/u \mod \mathfrak{p}^{2r+1}$, whence the last part of the above expression is $\sum_{v} \psi(v)\chi(1+vu^{-1})$

$$= \sum_{v} \psi((1-\alpha u^{-1})v) = \begin{cases} N\mathfrak{p}^{r} & \text{if } u \equiv \alpha \mod \mathfrak{p}^{r} \\ 0 & u \not\equiv \alpha \mod \mathfrak{p}^{r} \end{cases}.$$

Taking α to be the representative of the class of α modulo $\mathfrak{p}^{r}$,

$$(N\mathfrak{p})^{-1/2}(\chi, \psi) = \sum_{z} \chi(\alpha+z)\psi(\alpha+z) = \chi(\alpha)\psi(\alpha)\sum_{z}\psi(z)\chi(1+(z/\alpha))$$

$$= \chi(\alpha)\psi(\alpha) \sum_{z \in \mathfrak{p}^{r}/\mathfrak{p}^{r+1}} \psi(\alpha z)\chi(1+z),$$

which proves the lemma.

To complete the computation of (χ, ψ) we must determine $\Sigma_{z \in \mathfrak{y}^r/\mathfrak{y}^{r+1}} \psi(\alpha z)\chi(1+z) = \Sigma_{x \in \mathfrak{o}/\mathfrak{y}} \psi(\alpha \pi^r x)\chi(1+\pi^r x)$, π being a prime element of k. For $x \in \mathfrak{o}$, let $\Phi(x) = \psi(\alpha \pi^r x)\chi(1+x\pi^r)$. Φ satisfies a simple functional equation:

$$\Phi(x+x') = \Phi(x)\Phi(x')\overline{\psi}_{-\alpha\pi^{2r}}(xx') \text{ , as is easily verified.}$$

It follows from the functional equation that $\Phi(x)$ depends only upon the residue class of x modulo $\mathfrak{y}$, and is 1 if x is congruent to 0. As $\psi_{-\alpha\pi^{2r}}$ is a character of k^+ which is trivial on $\mathfrak{y}$ but not on $\mathfrak{o}$, we obtain by passage to quotients a function Δ on the residue class field $\overline{k}$ and a non-trivial additive character, θ, of $\overline{k}$ such that:

(1) Δ maps $\overline{k}$ into the unimodular complex numbers

(2) $\Delta(0) = 1$

(3) $\Delta(x+x') = \Delta(x)\,\Delta(x')\overline{\theta}(xx')$

Functions, Δ, of this type shall be considered in some detail. The results will then be applied to the function Φ. We shall refer to sums $\Sigma_{x \in k}\Delta(x)$ as Δ-sums.

It is interesting to determine some of the consequences of the functional equation.

<u>Lemma</u>: If k is a finite field with q elements and characteristic p, θ is a non-trivial character of k^+ and Δ is a mapping of k into the complex numbers which satisfies the functional equation (3), then, if Δ not every where zero,

1. $\Delta(0) = 1$

2. $\Delta(rx) = (\Delta(x))^r\,\theta(r(r-1)x^2/2)$, for each integer $r > 0$.

3. Δ maps k into the unimodular complex numbers (in fact into the $p(p,2)$ roots of unity)

4. If Δ' is another non-trivial solution of the functional equation, then there exists unique $c \in k$ such that $\Delta'(x) = \Delta(x)\,\overline{\theta}(cx)$ and $\Sigma_{x \in k}\Delta'(x) = \overline{\Delta}(c)\,\Sigma_{x \in k}\Delta(x)$.

5. $\left|\frac{1}{q}\,\Sigma\Delta(x)\right| = 1$

<u>Proof</u>

1. Follows directly from the functional equation by setting $x = x' = 0$, provided $\Delta(0) \neq 0$. But if $\Delta(0) = 0$ then for any $x \in k$, $\Delta(x) = \Delta(x+0) = \Delta(x)\Delta(0) = 0$ which contradicts the hypothesis that Δ is non-trivial.

2. This statement is certainly true for $r = 1$. Suppose it is true for some fixed $r \geq 1$. Then $\Delta((r+1)x) = \Delta(rx)\Delta(x)\,\overline{\theta}(rx^2) = (\Delta(x))^{r+1}\,\overline{\theta}(x^2(r+\frac{r(r-1)}{2})) = (\Delta(x))^{r+1}\,\overline{\theta}(x^2\,\frac{(r+1)r}{2})$ which proves the assertion in general.

3. Let p be the characteristic of the field k, then $px = 0$ and $1 = \Delta(0) = \Delta(px) = (\Delta(x))^p\,\overline{\theta}(\frac{p(p-1)}{2}x^2). = \begin{cases}(\Delta(x))^p & \text{for } p \neq 2\\ (\Delta(x))^2\,\overline{\theta}(x^2) & \text{for } p = 2.\end{cases}$

For $p \neq 2$, therefore $\Delta(x)$ is a p^{th} root of 1, while for $p = 2$, $\overline{\theta}(x) = \pm 1$ whence $\Delta(x)$ is a 4^{th} root of 1, which proves 3.

4. For Δ and Δ' as indicated

$(\frac{\Delta'}{\Delta})(x+x') = (\frac{\Delta'}{\Delta})(x)(\frac{\Delta}{\Delta'})(x')$, whence Δ/Δ' is an additive character of k, but all such characters are mappings $x \to \overline{\theta}(cx)$ for suitable choice of c. To complete the proof of 4, we define the Fourier transform of a complex valued function f on k to be the function $\hat{f}(x) = \frac{1}{\sqrt{q}} \Sigma_{z \in k} f(z)\, \overline{\theta}(xz)$. The inversion formula holds as is easily verified for the function $\delta(x) = \begin{cases} \sqrt{q} \text{ for } x = 0 \\ 0 \text{ for } x \neq 0 \end{cases}$ as $\hat{\delta}$ is the unit function and the transform of the unit function is again δ. For the function Δ we have: $\hat{\Delta}(0) = \frac{1}{\sqrt{q}} \Sigma_z\, \Delta(x+z) = \Delta(x) \frac{1}{\sqrt{q}} \Sigma_z\, \Delta(z)\, \overline{\theta}(xz) = \Delta(x)\hat{\Delta}(x)$ whence $\hat{\Delta}(x) = \hat{\Delta}(0)\, \overline{\Delta}(x)$ (as $|\Delta(x)| = 1$). Assertion 4 follows directly.

5. By the inversion formula

$1 = \Delta(0) = \hat{\hat{\Delta}}(0) = \hat{\Delta}(0)\, \hat{\overline{\Delta}}(0) = |\hat{\Delta}(0)|^2$ whence assertion 5 follows. This completes the proof.

In order to give an explicit representation of the Δ sums under consideration, it is necessary to establish a result analogus to that of Hasse and Davenport for Gauss sums. Their result gave the relation between a given Gauss sum in a finite field k and a particular Gauss sum in a finite extension field K. A similar result holds for the Δ sums and the same proof with very minor changes may be used for both sums. We first note some simple properties of the second symmetric function $S^{(2)}_{K/k}$, where K is an extension of finite degree of a ground field, k.

<u>Lemma</u>

If $K \supset L \supset k$, L a field, and a and b are elements of K then

1. $S^{(2)}_{K/k}(a+b) = S^{(2)}_{K/k}(a) + S^{(2)}_{K/k}(b) + S_{K/k}(a)S_{K/k}(b) - S_{K/k}(ab)$

2. $S^{(2)}_{K/k}(a) = (S_{K/L} \circ S^{(2)}_{L/k})(a) + (S^{(2)}_{K/L} \circ S_{L/k})(a)$

3. $(S_{K/k}(a))^2 = S_{K/k}(a^2) + 2S^{(2)}_{K/k}(a)$.

The proof may be dispensed with. We now give the basic result mentioned above. The proof is an almost word by word repetition of Weil's proof(9) of the theorem of Hasse and Davenport.

<u>Theorem</u> Let k be a finite field with q elements, K an extension of k of degree m, θ a non-trivial additive character of k, Δ a non- trivial solution of the functional equation: $\Delta(x+y) = \Delta(x)\Delta(y)\overline{\theta}(xy)$ (for all $x,y \in k$). Let θ' be the additive character $\theta \circ S_{K/k}$ of K and Δ' the function $(\Delta \circ S_{K/k})(\theta \circ S^{(2)}_{K/k})$ on K. Let $g(\Delta) = \Sigma_{x \in k}\Delta(x)$, $g'(\Delta') = \Sigma_{x \in K}\Delta'(x)$, then Δ' is a non trivial solution of the functional equation: $\Delta'(x+y) = \Delta'(x)\Delta'(y)\overline{\theta}'(xy)$ (for all $x,y \in K$) and

$$-g'(\Delta') = (-g(\Delta))^m.$$

<u>Proof</u> Trivially, $\Delta'(0) = \Delta(0)\,\theta(0) = 1$. For $x,y \in K$, from the previous lemma, $\Delta'(x+y)=\Delta(S(x)+S(y))\ \theta(S^{(2)}(x)+S^{(2)}(y)+S(x)S(y)-S(xy))$ $=\Delta'(x)\Delta'(y)\overline{\theta}'(xy)$ which proves the first assertion.

For the second assertion, consider the polynomials with coefficients in k and highest coefficient 1. To every such polynomial $F(X) = X^n+c_1X^{n-1} + c_2X^{n-2} + \dots + c_n$, of degree ≥ 1, we attach the number $\lambda(F) = \Delta(c_1)\,\theta(c_2)$ (where $c_2 = 0$ if $n=1$)

For two polynomials, F as above and F' whose three leading coefficients are in order $1, d_1, d_2$, we have FF' is a polynomial whose three leading coefficients are $1, c_1+d_1, c_2+c_1d_1+d_2$, whence $\lambda(FF') = \Delta(c_1+d_1)\,\theta(c_2+c_1d_1+d_2) = \lambda(F)\,\lambda(F')$ by the basic property of Δ. If we denote by $n(F)$ the degree of the

(9) A. Weil, Bull. Amer. Math. Soc. vol55(1949)pp.497-508.

polynomial F, and by Z an indeterminate, this gives the formal identity: $1 + \Sigma_F \lambda(F) Z^{n(F)} = \prod_P (1 - \lambda(P)Z^{n(P)})^{-1}$ where the sum in the left side is taken over all polynomials F over k, of degree ≥ 1, with highest coefficient 1, and the product in the right hand side is taken over all irreducible polynomials P over k, with highest coefficient 1.

In the sum on the left hand side, consider first the terms which correspond to polynomials $F(X) = X + c$ of degree 1; the sum of those terms is equal to $g(\Delta)Z$. As to the sum of the terms corresponding to any given degree $n > 1$, it is zero since it is $Z^n \Sigma_{x,y}\Delta(x)\theta(y) = Z^n g(\Delta) \Sigma_y \theta(y) = 0$. This gives

$$1 + g(\Delta)Z = \prod_P (1 - \lambda(P)Z^{n(P)})^{-1} .$$

Similarly if $F'(X) = X^n + d_1X^{n-1} + \dots + d_n$ is a polynomial over K, we write $\lambda'(F') = \Delta'(d_1)\theta'(d_2)$ and taking another indeterminate Z', get the formal identity

$$1 + g'(\Delta')Z' = \prod_{P'} (1 - \lambda'(P')Z'^{n(P')})^{-1}$$

where the product is taken over all irreducible polynomials P' over K with highest coefficient 1.

Let P be as above, let P' be one of the irreducible factors of P over K, let $-t$ be one of the roots of P'. The t generates over k an extension k(t) of degree $n = n(P)$, and over K an extension K(t) of degree $n' = n(P')$. From the uniqueness of extensions of k of given degree, $K \cap k(t)$ is an extension of k of degree $d = (m,n)$. Hence $\deg K(t)/K = \deg k(t)/K\cap k(t) = n/d$, whence $n(P') = n/d$, which clearly does not depend upon the choice of P' as irreducible factor of P over K. Hence P has over K exactly d irreducible factors each of degree n/d. Also deg $K(t)/k(t) = m/d$.

We assert that $\lambda'(P') = \lambda(P)^{m/d}$. For let $a = S_{k(t)/k}(t)$, $b = S^{(2)}_{k(t)/k}(t)$. Then $P(X) = X^n + aX^{n-1} + bX^{n-2} + \dots$, whence $\lambda(P) = \Delta(a)\theta(b)$. Similarly, if $a' = S_{K(t)/K}(t)$, $b' = S^{(2)}_{K(t)/K}(t)$, we have $\lambda'(P') = \Delta'(a')\theta'(b') =$

$$(\Delta \circ S_{K/k})(a')(\theta \circ S^{(2)}_{K/k})(a')(\theta \circ S_{K/k})(b')$$

$$= (\Delta \circ S_{K(t)/k})(t)\ \theta((S^{(2)}_{K/k} \circ S_{K(t)/K})(t) + (S_{K/k} \circ S^{(2)}_{K(t)/K})(t))$$

$$= \Delta(S_{K(t)/k}(t))\ \theta(S^{(2)}_{K(t)/k}(t)).$$

But $S_{K(t)/k}(t) = (S_{k(t)/k} \circ S_{K(t)/k(t)})(t) = ma/d$.

$$S^{(2)}_{K(t)/k}(t) = S^{(2)}_{k(t)/k}(S_{K(t)/k(t)}(t)) + S_{k(t)/k}(S^{(2)}_{K(t)/k(t)}(t))$$

$$= S^{(2)}_{k(t)/k}(mt/d) + S_{k(t)/k}(\{\tfrac{m}{d}(\tfrac{m}{d} - 1)\tfrac{1}{2}\}t^2)$$

$$= (\tfrac{m}{d})^2 b + (\tfrac{m}{d})(\tfrac{m}{d} - 1)\tfrac{1}{2}\, S_{k(t)/k}(t^2)$$

By the previous lemma, $S_{k(t)/k}(t^2) = a^2 - 2b$, whence

$\lambda'(P') = \Delta(\frac{m}{d}a)\ \theta(\frac{1}{2}\frac{m}{d}(\frac{m}{d} - 1)a^2)\ \theta(\frac{m}{d}b) = (\lambda(P))^{m/d}$, as is verified by means of the functional equation of Δ. The remainder of the proof is as given by Weil.

If k is a finite field not of characteristic 2, let $\mathfrak{y}$ be the prime of a local number field of which k is the residue class field and let (for $a \in k^*$) $\left(\frac{a}{\mathfrak{y}}\right) = +1$ or -1 depending upon whether or not a not a is a square. We assert

Lemma For $a \in k^*$, θ a non-trivial additive character of k then

$$\Sigma_{x \in k}\theta(x^2) = (\tfrac{a}{\mathfrak{p}})\, \Sigma_{x \in k}\theta(ax^2).$$

Proof If $(\frac{a}{\mathfrak{p}}) = 1$ then $a k^2 = k^2$ so that the assertion follows. If $(\frac{a}{\mathfrak{p}}) = -1$ then $k^* = k^{*2} \cup ak^{*2}$ and as θ is not trivial we have

$$0 = \Sigma_{x \in k}\theta(x) = \theta(0) + \Sigma_{x \in k^{*2}}\theta(x) + \Sigma_{x \in k^{*2}}\theta(ax).$$

But $\Sigma_{x \in k}\theta(x^2) = \theta(0) + 2\Sigma_{x \in k^{*2}}\theta(x)$

$\Sigma_{x \in k}\theta(ax^2) = \theta(0) + 2\Sigma_{x \in k^{*2}}\theta(ax)$, whence

$$\Sigma_{x \in k}\theta(x^2) + \Sigma_{x \in k}\theta(ax^2) = 2(\theta(0) + \Sigma_{x \in k^{*2}}\theta(x) + \Sigma_{x \in k^{*2}}\theta(ax)) = 0$$

which proves the lemma.

With the aid of these results we may determine the Δ-sums under consideration.

Lemma Let k be a finite field of characteristic p and of degree f over the rationals modulo p. Let $\mathfrak{p}$ be the prime of a local number field whose residue class field is k. Let θ be a non-trivial additive character of k and Δ a non-trivial solution of the functional equation: $\Delta(x+y) = \Delta(x)\Delta(y)\overline{\theta}(xy)$. Let R denote the rational numbers modulo p and let

θ_0 be the additive character of R defined by $\theta_0(1) = e^{2\pi i/p}$

θ_0' be the additive character $\theta_0 \circ S_{k/R}$ of k

η be the unique element of k^* such that $\theta(x) = \theta_0'(\eta x)$ for all $x \in k$.

(1) For $p \neq 2$, let γ be the unique element of k such that $\Delta(x) = \overline{\theta}(\frac{x^2}{2} + \gamma x)$ for all $x \in k$, then

$$\frac{1}{\sqrt{p^f}}\Sigma_{x\in k}\Delta(x) = \theta(\gamma^2/2)\left(\frac{-2\eta}{y}\right)\left(\sqrt{\left(\frac{-1}{p}\right)}\right)^f(-1)^{f-1},$$

where $\sqrt{1} = 1$, $\sqrt{-1} = i$.

(2) For $p=2$, let

β be the unique square root of $1/\eta$

γ be the unique element of k such that $\Delta(\beta x) = \Delta_0^\prime(x)\theta_0^\prime(\gamma x)$

where $\Delta_0^\prime$ is the function $(\Delta_0 \circ S_{k/R})(\theta_0 \circ S_{k/R}^{(2)})$ on k and

Δ_0 is the function on R defined by $\begin{cases}\Delta_0(0) = 1\\ \Delta_0(1) = i,\end{cases}$

then

$$\frac{1}{\sqrt{2^f}}\Sigma_{x\in k}\Delta(x) = \overline{\Delta_0^\prime(\gamma)}\left(\frac{1+i}{\sqrt{2}}\right)^f(-1)^{f-1}$$

<u>Proof</u>

(1) $p \neq 2$. Let $\Delta_0(x) = \overline{\theta}_0\left(\frac{x^2}{2}\right)$ for all $x\in R$. Then $\Delta_0(x+y) = \Delta_0(x)\Delta_0(y)\overline{\theta}_0(xy)$. Let $\Delta_0^\prime = (\Delta_0 \circ S_{k/R})(\theta_0 \circ S_{k/R}^{(2)})$, a function on k; then by the previous theorem, $(-\Sigma_{x\in R}\Delta_0(x))^f = -\Sigma_{x\in k}\Delta_0^\prime(x)$. But for $x\in k$, $\Delta_0^\prime(x) = \theta_0(-\frac{1}{2}(S(x))^2 + S^{(2)}(x))$

$$=(\overline{\theta}_0 \circ S)\left(\frac{x^2}{2}\right) = \overline{\theta}_0^\prime\left(\frac{x^2}{2}\right) = \overline{\theta}\left(\frac{1}{2\eta}x^2\right).$$

Hence by the previous lemma, $\Sigma_{x\in k}\Delta_0^\prime(x) = \left(\frac{\eta}{y}\right)\Sigma_{x\in k}\overline{\theta}(x^2/2)$.

Let $\Delta^\prime$ be the function $x \to \overline{\theta}(x^2/2)$ on k. Then $\Delta^\prime$ satisfies the same functional equation as Δ and therefore there exists unique $\gamma\in k$ such that $\Delta(x) = \Delta^\prime(x)\,\overline{\theta}(\gamma x)$ and also

$\Sigma\Delta(x) = \overline{\Delta^\prime}(\gamma)\Sigma\Delta^\prime(x) = \overline{\Delta^\prime}(\gamma)\Sigma\overline{\theta}\left(\frac{x^2}{2}\right) = \theta(\gamma^2/2)\left(\frac{\eta}{y}\right)\Sigma\Delta_0^\prime(x)$

$= \theta(\gamma^2/2)\left(\frac{\eta}{y}\right)(-1)^{f-1}(\Sigma_{x\in R}\Delta_0(x))^f$, all the sums except for the last being over k. The condition on γ is $\Delta(x) = \Delta^\prime(x)\overline{\theta}(\gamma x) =$

$\overline{\theta}(x^2/2 + \gamma x)$ and by a classical result, $\Sigma_{x \in R}\Delta_0(x) = \Sigma\overline{\theta}_0(x^2/2)$ $= (\frac{2}{p})\Sigma_{x\in R}\overline{\theta}_0(x^2) = (\frac{-2}{p})\sqrt{p}\ \sqrt{(\frac{-1}{p})}$. As $(\frac{-2}{p})^f = (\frac{-2}{y})$, assertion (1) follows.

(2) p = 2. As $\theta_0(0)=1, \theta_0(1)= -1$, it is trivial that Δ_0 satisfies the functional equation $\Delta_0(x+y) = \Delta_0(x)\Delta_0(y)\theta_0(xy)$. Hence by the theorem, $(-\Sigma_{x\in R}\Delta_0(x))^f = -\Sigma_{x\in k}\Delta_0^*(x)$, whence

$\Sigma_{x\in k}\Delta_0^*(x) = (-1)^{f-1}(\frac{1+i}{\sqrt{2}})^f\sqrt{2^f}$. Let Δ' be the function

$x \to \Delta(\beta x)$ on k. Then $\Delta'(x+y) = \Delta(\beta x+\beta y) = \Delta(\beta x)\Delta(\beta y)\overline{\theta}(\beta^2 xy)$ $= \Delta'(x)\Delta'(y)\overline{\theta}_0^*(xy)$ (by choice of β). Clearly, $\Sigma_{x\in k}\Delta'(x) =$ $\Sigma_{x\in k}\Delta(x)$ as $\eta \neq 0$. As Δ' and Δ_0^* satisfy the same functional equation, there exists a unique element $\gamma \in k$ such that

$\Delta(\beta x) = \Delta'(x) = \Delta_0^*(x)\overline{\theta}_0^*(\gamma x) = \Delta_0^*(x)\theta_0^*(\gamma x)$ (as p = 2)

Also $\Sigma\Delta'(x) = \overline{\Delta}_0^*(\gamma)\Sigma\Delta_0^*(x)$ (the sums being over k). The second assertion now follows.

Having evaluated the Δ-sums, we return to the problem of evaluating root numbers whose conductor is an odd power of the prime.

<u>Theorem</u> If k is a y-adic number field, $y \mid p$, (χ, ψ) a root number of conductor y^{2r+1} $(r \geq 0)$, R the p-adic completion of the rational numbers, T the inertial subfield of k/R, let θ_0 be an additive character of R of conductor p such that $\theta_0(1)= e^{2\pi i/p}$, α be the unit of k uniquely determined modulo y^r by the condition: $\chi(1+z) = \overline{\psi}(\alpha z)$ for all $z \in y^{r+1}$, π be a prime element of k, also let η be the unit in T

uniquely determined modulo p by the condition that

$$\overline{\psi}(\alpha\pi^{2r}x) = (\theta_o \circ S_{T/R})(\eta x) \quad \text{for all } x \in \mathfrak{O}_T \text{ (= the ring of integers of T)}$$

Then:
<u>if p ≠ 2,</u> there exists an integer γ in T uniquely determined modulo $\mathfrak{p}$ by the condition

$$\psi(\alpha\pi^{r}x)\chi(1 + x\pi^{r}) = \psi(\alpha\pi^{2r}(\tfrac{x^2}{2} + \gamma x)) \text{ for all } x \in \mathfrak{O}_T$$

and

$$(\chi, \psi) = \chi(\alpha)\psi(\alpha)\overline{\psi}(\alpha\pi^{2r}\gamma^2/2)\left(\frac{-2\eta}{\mathfrak{p}}\right)(-1)^{f-1}\left(\sqrt{\left(\tfrac{-1}{p}\right)}\right)^{f}$$

<u>if p = 2,</u> let $\beta \in U_T$ be chosen such that $\eta \equiv 1/\beta^2 \mod \mathfrak{p}$

Δ_o be the function on $\mathfrak{O}_R$ which is 1 on $2U_R$ and i on U_R (where U_R is the group of units of R)

Δ_o^{*} be the function $(\Delta_o \circ S_{T/R})(\theta_o \circ S_{T/R}^{(2)})$ on $\mathfrak{O}_T$

θ_o^{*} be the character $\theta_o \circ S_{T/R}$ on T^{+}

then there exists an integer γ of T, uniquely determined modulo $\mathfrak{p}$ such that

$$\psi(\alpha\pi^{n}\beta x)\chi(1 + x\beta\pi^{n}) = \Delta_o^{*}(x)\theta_o^{*}(\gamma x) \quad \text{for all } x \in \mathfrak{O}_T$$

and

$$(\chi, \psi) = \chi(\alpha)\psi(\alpha)\overline{\Delta_o^{*}}(\gamma)\left(\frac{1+i}{\sqrt{2}}\right)^{f}(-1)^{f-1}$$

(in any case f is the absolute degree of the prime $\mathfrak{p}$)

<u>Proof.</u> This theorem is a direct consequence of the first lemma of this chapter and of the final result for Δ-sums. We recall that Δ was obtained by passage to quotients from the function $x \Rightarrow \chi(1 + \alpha\pi^{n}x)\psi(\alpha\pi^{n}x)$ and θ was obtained in the same way from the character $\psi_{\alpha\pi^{2n}}$. The inertial subfield T is used in defining γ and η because $\theta_o \circ S_{T/R}$ is related in the proper manner to the corresponding character of the residue class field of k.

This completes our treatment of root numbers of a given local number field. The analogue of the Hasse-Davenport theorem, that the relations between root numbers of different fields will be the subject of the next chapter. The multiplicative formulae developed above will provide the tool for this work.

Note: For $p \neq 2$ it is possible to unify to some extent the formulae for the root numbers. The result is stated without proof. If (χ, ψ) is a root number of conductor $\mathfrak{y}^n$, $n > 1$, let s be the smallest integer such that $3s \geq n$; then there exists a unit α uniquely determined modulo $\mathfrak{y}^{n-s}$ by the condition

$$\chi(1 - z) = \psi(\alpha(z + (z^2/2))) \quad \text{for all } z \in \mathfrak{y}^s$$

and

$$(\ , \ ) = \chi(\alpha)\psi(\alpha)\, t ,$$

where

$$t = 1 \qquad \text{if } n \text{ is even}$$

$$t = \left(\frac{-2\eta}{\mathfrak{y}}\right)\left(\sqrt{\left(\frac{-1}{p}\right)}\right)^f (-1)^{f-1} \qquad \text{if } n \text{ is odd } (\eta \text{ as defined in the last theorem}).$$

This statement remains valid if s is taken to be $n - [\frac{n}{2}]$.

Chapter III

The Abelian Norm Theorem

In the following k is a local number field, K is an abelian extension of degree n, $(\tau_1, \ldots, \tau_n)$ is the group of characters of k^* which are trivial on $N_{K/k}K^*$, K_N^* is the kernel in K^* of $N_{K/k}$ and C is the field of complex numbers. Following Tate, a continuous homomorphism of k^* into C is a quasi-character of k^*. By means of his local zeta functions Tate has defined a canonical complex valued function, ρ, on the group of quasi-characters of k^*. We shall distinguish between the function on the group of quasi-characters of K^* and the corresponding function associated with the field k by referring to the former as ρ_K and to the latter as ρ_k. Let Θ be the group of all quasi-characters of K which are trivial on K_N^*. Let $Q_{K/k}$ be the complex valued function

$$\chi \to \left[\prod_{\mu \circ N_{K/k} = \chi} \rho_k(\mu)\right] / \rho_K(\chi)$$

on Θ, the product being over all quasi-characters of k^* whose composition with the relative norm is χ. This function is certainly well defined whenever the denominator is not zero. The definition is made precise by interpreting the function, Q, from the usual point of view of identifying a coset of the unramified quasi-characters with a group locally isomorphic with the complex plane.

The function $Q_{K/k}$ is fully investigated in this chapter. The results are:

1. $Q_{K/k}(\chi)$ is a fourth root of unity and the square is one if and only if $(-1)^{n/(n,2)} \in N_{K/k}K^*$.

2. If the valuation is archimedean and $K \neq k$ then $Q_{K/k}(\chi) = -1$.

3. If K is a $\mathfrak{p}$-adic number field and the conductor of χ is $\mathfrak{p}^{m+1}$ then $Q_{K/k}(\chi) = \kappa(m, K/k)$, a fourth root of unity which depends only upon the conductor. Furthermore let f' be the relative residue class degree and e' the relative ramification, also let p be the prime of the rationals which $\mathfrak{p}$ divides and let e" be the largest divisor of e' which is relatively prime to 2p then

$$\frac{\kappa(m, K/k)}{\kappa(-1, K/k)} \begin{array}{ll} = 1 & \text{if } m = 0 \\ = \left(\frac{N\mathfrak{p}}{e''}\right)^{1+m} & \text{if } m \neq 0 \end{array}$$

and if 2 does not divide e' then

$$\kappa(-1, K/k) = (-1)^{e'(f'-1)\,\mathrm{ord}_y \mathfrak{g}_k} \left(\frac{N\mathfrak{g}_{K/k}}{e''}\right)$$

It is remarkable that the first statement above, which is the major result, could be easily obtained if it were known that $Q(\bar{\chi}) = Q(\chi)$. However I have been unable to prove this last relation without proving the first sentence in statement 3. The proof of the above statements is carried out by first considering cyclic extensions of prime degree and then generalizing.

Archimedean Case

K = field of complex numbers

k = field of real numbers

K_N^* = the unimodular complex numbers.

The generic quasi-character, χ, of K^* trivial on K_N^* is $r\, e^{i\theta} \to r^{2s}$ and for this character

$\rho_K(\chi) = (2\pi)^{1-2s}\, \Gamma(s)/\Gamma(1-s)$.

The two quasi-characters of k^* whose composition with the relative norm is χ are

μ_1: $x \to |x|^s$

μ_2: $x \to |x|^s (\text{sign } x)$. For these characters

$\rho_k(\mu_1) = 2^{1-s}\pi^{-s} \cos(\frac{s\pi}{2})\, \Gamma(s)$

$\rho_k(\mu_2) = -i\, 2^{1-s}\, \pi^{-s} \sin(\frac{s\pi}{2})\, \Gamma(s)$.

Using well known properties of the gamma function it is easily seen that $Q(\chi) = -1$, which disposes of the archimedean primes.

Finite Primes

We first tabulate the Tate function ρ. Let $\mathfrak{y}$ be the prime of k, $\mathfrak{d}_k$ the absolute different of k. Let R be the p-adic completion of the rational numbers ($\mathfrak{y}\,|\,p$) and let λ be the mapping of R into the reals modulo 1 defined by the conditions

(1) $\lambda(x)$ is a rational number with only a power of p in the denominator.

(2) $\lambda(x) - x$ is a p-adic integer.

Let θ be the additive character $x \to \exp(2\pi i\, \lambda(x))$ of R. The <u>standard additive character</u> ψ of k is then defined to be the character $\theta \circ S_{k/R}$ of k. If μ is a quasi-character of k^* then the value of the Tate function at μ is

$$\rho_k(\mu) = N_{k/R}(\mathfrak{d}_k F(\mu))^{-1/2} \mu(\pi^{-\mathrm{ord}\, \mathfrak{d}_k F(\mu)})(\mu, \psi_{\pi^{-\mathrm{ord}\, \mathfrak{d}_k F(\mu)}})$$

where $F(\mu)$ = conductor of μ

$(\mu, \psi_{\pi^{-\mathrm{ord}\, \mathfrak{d}_k F(\mu)}})$ = root number as defined in Chapter II if $\mathfrak{y} | F(\mu)$

$= \dfrac{1 - N\mathfrak{y}^{-1}\mu(\pi^{-1})}{1-\mu(\pi)}$ if $\mathfrak{y} \nmid F(\mu)$

π is an arbitrary prime element of k.

This notation is used to uniformize the treatment and of course the symbol $(\mu, \psi_{\pi-d})$ has none of the properties of root numbers if $F(\mu)$ is not divisible by $\mathfrak{y}$.

For K/k abelian and χ a quasi-character of K^* trivial on K_N^*

$$\rho_{K/k}(\chi) = \frac{\prod_{\mu \circ N = \chi} \left\{ N_{k/R}(\mathfrak{d}_k F(\mu))^{-\frac{1}{2}} \mu(\pi^{-\mathrm{ord}\, \mathfrak{d}_k F(\mu)})(\mu, \psi_{\pi^{-\mathrm{ord}\, \mathfrak{d}_k F(\mu)}}) \right\}}{N_{K/R}(\mathfrak{d}_K F(\chi))^{-\frac{1}{2}} \chi(\Pi^{-\mathrm{ord}\, \mathfrak{d}_K F(\chi)})(\chi, \Psi_{\Pi^{-\mathrm{ord}\, \mathfrak{d}_K F(\chi)}})}$$

where the product is over all quasi-characters of k^* whose composition with $N_{K/k}$ is χ, and where Π is a prime element of K, Ψ is the standard additive character of K and ord means $\mathrm{ord}_{\mathfrak{y}}$ in the numerator and $\mathrm{ord}_{\mathfrak{P}}$ in the denominator.

As shown in the proof of the lemma on admissible integers (Chapter I), $\prod_{\mu \circ N_{K/k} = \chi} F(\mu) = N_{K/k}(\mathfrak{d}_{K/k} F(\chi))$

whence

$$N_{K/R}(\mathcal{J}_K F(\chi)) = (N_{k/R} \circ N_{K/k})(\mathcal{J}_k \mathcal{J}_{K/k} F(\chi))$$

$$= N_{k/R}(\mathcal{J}_k^n \prod_{\mu \circ N = \chi} F(\mu)) = \prod_{\mu \circ N = \chi} N_{k/R}(\mathcal{J}_k F(\mu)).$$

It follows that

$$Q_{K/k}(\chi) = \frac{\prod_{\mu \circ N_{K/k} = \chi} \{\mu(\pi^{-\mathrm{ord}\, \mathcal{J}_k F(\mu)})(\mu, \psi_{\pi^{-\mathrm{ord}\, \mathcal{J}_k F(\mu)}})\}}{\chi(\Pi^{-\mathrm{ord}\, \mathcal{J}_K F(\chi)})(\chi, \Psi_{\Pi^{-\mathrm{ord}\, \mathcal{J}_K F(\chi)}})}$$

This relation may be greatly simplified by proper choice of Π if K/k is either unramified or purely ramified.

Lemma

(a) If K/k is unramified and $F(\chi) = \mathfrak{p}^{m+1}$, $\mathcal{J}_k = \mathfrak{z}^d$ then
$Q_{K/k}(\chi) = (-1)^{(n-1)(d+1+m)} [\prod_\mu (\mu, \psi_{\pi^{-d-1-m}})] / (\chi, \Psi_{\pi^{-d-1-m}})$

(b) If K/k is purely ramified, set $\pi = N_{K/k}\Pi$ and then

$$Q_{K/k}(\chi) = [\prod_\mu (\mu, \psi_{\pi^{-\mathrm{ord}\, \mathcal{J}_k F(\mu)}})] / (\chi, \Psi_{\Pi^{-\mathrm{ord}\, \mathcal{J}_K F(\chi)}})$$

in both cases the product being over all quasi-characters of k^* whose composition with $N_{K/k}$ is χ.

Proof

(a) As K/k is unramified, we may set $\Pi = \pi$. In the notation of Chapter I, $s_j = -1$ $(1 \le j \le n)$ whence $\mu \circ N_{K/k} = \chi \Rightarrow$
$F(\mu) = \mathfrak{z}^{1+m}$. Also $d = \mathrm{ord}_{\mathfrak{z}} \mathcal{J}_k = \mathrm{ord}_{\mathfrak{p}} \mathcal{J}_K$. Hence it only remains to compute (μ_0 fixed, $\mu_0 \circ N_{K/k} = \chi$)

$$\frac{\prod_\mu \mu(\pi^{-d-1-m})}{\chi(\pi^{-d-1-m})} = \frac{\prod_{j=1}^n (\mu_0 \tau_j)(\pi^{-d-1-m})}{(\mu_0(\pi^{-d-1-m}))^n} = \left(\prod_{j=1}^n \tau_j(\pi)\right)^{-d-1-m}$$

A more general method for computing $\prod_{j=1}^n \tau_j(\pi)$ will be determined subseqently, but in this case we may set $\tau_j = \tau^j$ $(1 \le j \le n)$

where τ is an unramified quasi-character such that $\tau(\pi) = z$, a primitive n-th root of one, whence by an elementary computation $\prod_{j=1}^{n} \tau_j(\pi) = (-1)^{n-1}$. The first statement follows directly.

(b) As K/k is purely ramified, $N_{K/k}(\Pi)$ is a prime element of k and we may set $\pi = N_{K/k}\Pi$. Again let μ_0 be a fixed character of k^* such that $\mu_0 \circ N_{K/k} = \chi$. We need only compute

$$\frac{\prod_{j=1}^{n} (\mu_0 \tau_j)(\pi^{-\mathrm{ord}\, \mathfrak{d}_k F(\mu_0 \tau_j)})}{\chi(\Pi^{-\mathrm{ord}\, \mathfrak{d}_K F(\chi)})}$$

As $\tau_j(\pi) = 1$, $\chi(\Pi) = \mu_0(\pi)$, this is simply

$(\mu_0(\pi)^{-1})^{\Sigma_\mu \mathrm{ord}_{\mathfrak{y}} \mathfrak{d}_k F(\mu) - \mathrm{ord}_{\mathfrak{P}} \mathfrak{d}_K F(\chi)}$ which is one as

$N_{K/k}(\mathfrak{d}_{K/k} F(\chi)) = \prod_\mu F(\mu) \Rightarrow \Sigma_\mu \mathrm{ord}_{\mathfrak{y}} F(\mu) = \mathrm{ord}_{\mathfrak{P}} (\mathfrak{d}_{K/k} F(\chi))$

and as $\mathfrak{d}_K = \mathfrak{d}_{K/k} \mathfrak{d}_k \Rightarrow \mathrm{ord}_{\mathfrak{P}} \mathfrak{d}_K = \mathrm{ord}_{\mathfrak{P}} \mathfrak{d}_{K/k} + n\ \mathrm{ord}_{\mathfrak{y}} \mathfrak{d}_k$ (using the fact that K/k is purely ramified).

In this way the problem is reduced to the study of root numbers. We now consider the unramified case.

K/k <u>Unramified</u>

$\chi = \mu \circ N_{K/k}$, $\tau_j = \tau^j$, τ trivial on U_k, $\tau(\pi) = \zeta$, a primitive n-th root of 1. $\mathfrak{d}_k = \mathfrak{y}^d$, $F(\chi) = \mathfrak{P}^{1+m}$, $F(\mu) = \mathfrak{y}^{1+m}$

$\{\mu\tau_j\}_{j=1}^{n}$ is the set of all characters whose composition with $N_{K/k}$ is χ.

$$Q(\chi)\ (-1)^{(n-1)(d+1+m)} = \frac{\prod_{j=1}^{n} (\mu\tau_j,\ \psi_{\pi^{-d-1-m}})}{(\chi,\ \Psi_{\pi^{-d-1-m}})} \qquad (\S)$$

Case 1. m = -1.

$$(\mu\tau^j,\psi_{\pi^{-d}}) = \left[1-\frac{1}{N\mathfrak{y}\,\mu(\pi)\zeta^j}\right]\Big/\left[1-\mu(\pi)\zeta^j\right]$$

$$(\chi,\Psi_{\pi^{-d}}) = \left[1-\frac{1}{(N\mathfrak{y}\,\mu(\pi))^n}\right]\Big/\left[1-(\mu(\pi))^n\right]$$

whence the right side of ($\S$) is 1. Hence for $m = -1$, $Q(\chi) = (-1)^{d(n-1)}$.

Case 2. $m \geq 0$.

As $\mathfrak{y}$ divides $F(\mu\tau^j)$, $(\mu\tau_j,\psi_{\pi^{-d-1-m}})$ is a root number in the sense of Chapter II and therefore depends only upon the behavior of $\mu\tau_j$ on the group of units. It follows that

$$Q_{K/k}(\chi)\ (-1)^{(n-1)(d+1+m)} = \frac{(\mu,\ \psi_{\pi^{-d-1-m}})^n}{(\chi,\ \Psi_{\pi^{-d-1-m}})} \qquad (\S\S)$$

The notation may now be simplified. From the definition of standard additive characters, $\Psi = \psi\circ S_{K/k}$, hence setting $\varphi = \psi_{\pi^{-d-1-m}}$, $\Phi = \Psi_{\pi^{-d-1-m}}$, we have $\Phi = \varphi\circ S_{K/k}$ and the right side of ($\S\S$) is $(\mu,\varphi)^n/(\chi,\Phi)$. We assert that this ratio is $(-1)^{(m+1)(n-1)}$. For $m = 0$ this is the result of Hasse and Davenport stated in the previous chapter. Hence we may assume that $m > 0$.

m + 1 even

There exists α such that $\mu(1+z) = \bar{\varphi}(\alpha z)$ for all $z \in \mathfrak{y}^r$, $r = (1+m)/2$. For $w \in \mathfrak{P}^r$, $\chi(1+w) = \mu(1+Sw + S^{(2)}w + \ldots + Nw)$

$= \mu(1 + S_{K/k}w) = (\bar{\varphi} \circ S_{K/k})(\alpha w) = \bar{\varphi}(\alpha w)$, as $S_{K/k}(\mathcal{P}^r) \subset \mathcal{Y}^r$ and $S^{(j)}_{K/k}(\mathcal{P}^r) \subset \mathcal{Y}^{1+m}$ for $j \geq 2$. It follows that $(\chi, \varphi) =$ $(\mu \circ N_{K/k})(\alpha)\ (\varphi \circ S_{K/k})(\alpha) = \mu(\alpha^n)\ \varphi(n\alpha) = (\mu(\alpha)\ \varphi(\alpha))^n$ $=(\mu, \varphi)^n$, which proves the assertion for (m+1) even.

m + 1 odd

Let $r = m/2$. There exists $\alpha \in U_{k}$, unique modulo $\mathcal{Y}^r$ such that $\mu(1+z) = \bar{\varphi}(\alpha z)$ for all $z \in \mathcal{Y}^{r+1}$. For $j \geq 2$, $S^{(j)}_{K/k}(\mathcal{P}^{r+1})$ lies in $\mathcal{Y}^{m+1}$, while $S(\mathcal{P}^{r+1}) \subset \mathcal{Y}^{r+1}$, whence for $w \in \mathcal{P}^{r+1}$, $\chi(1 + w) = (\mu \circ N)(1 + w) = \mu(1 + S(w))$

$$= (\bar{\varphi} \circ S)(\alpha w) = \Phi(\alpha w).$$

As usual let R be the p-adic completion of the rational numbers and θ_0 be an additive character of R of conductor p such that $\theta_0(1) = \exp(2\pi i/p)$. Let T be the inertial subfield of k/R and T' the corresponding field for K/R.

There exists $\eta \in T$, unique modulo $\mathcal{Y}$ such that

$$\bar{\varphi}(\alpha \pi^{2r} x) = (\theta_0 \circ S_{T/R})(\eta x) \quad \text{for} \quad x \in \mathcal{O}_T$$

As $T = k \cap T'$, $K = kT'$, it follows that for $x \in \mathcal{O}_{T'}$, $S_{K/k}(x) = S_{T'/T}(x)$, whence

$$\bar{\Phi}(\alpha \pi^{2r} x) = (\theta_0 \circ S_{T'/R})(\eta x) \quad \text{for} \quad x \in \mathcal{O}_{T'}$$

To complete this computation we must distinguish between primes which divide 2 and those that do not.

(a) $\mathcal{Y} \nmid 2$

There exists $\gamma \in \mathcal{O}_T$ such that

$$\mu(1 + x\pi^r)\,\varphi(x\pi^r\alpha) = \varphi(\alpha\,\pi^{2r}(\tfrac{x^2}{2} + \gamma x)) \quad \text{for all } x \in \mathcal{O}_R$$

Hence for $z \in \mathcal{O}_K$

$$\chi(1+z\pi^r)\,\Phi(\alpha z\pi^r) = (\mu \circ N_{K/k})(1 + z\pi^r)\,(\varphi \circ S_{K/k})(\alpha z\pi^r)$$

$$= \mu(1 + \pi^r S(z) + \pi^{2r} S^{(2)}(z))\,(\varphi \circ S)(\alpha z\pi^r)$$

$$= \mu(1 + \pi^r S(z))\,\varphi(\alpha\pi^r S(z))\,\mu(1 + \pi^{2r} S^{(2)}(z))$$

$$= \varphi\left(\alpha\pi^{2n}\left[\frac{(S(z))^2}{2} + \gamma S(z)\right]\right)\,\bar{\varphi}(\alpha\pi^{2n} S^{(2)}(z))$$

$$= \Phi\left(\alpha\pi^{2n}\left(\frac{z^2}{2} + \gamma z\right)\right)$$

Letting f be the absolute degree of $\mathcal{Y}$, we obtain

$$\frac{(\mu,\varphi)^m}{(\chi,\Phi)} = \frac{\left\{\mu(\alpha)\varphi(\alpha)\bar{\varphi}(\alpha\pi^{2n}\gamma^2/2)\left(\frac{2\eta}{\mathcal{Y}}\right)(-1)^{f-1}\left(\sqrt{\left(\frac{-1}{p}\right)}\right)^f\right\}^m}{\Phi(\alpha)\chi(\alpha)\bar{\Phi}(\alpha\pi^{2n}\gamma^2/2)\left(\frac{2\eta}{\mathcal{P}}\right)(-1)^{mf-1}\left(\sqrt{\left(\frac{-1}{p}\right)}\right)^{mf}} = (-1)^{m-1} = (-1)^{(m-1)(m+1)}$$

(b) $\mathcal{Y} | 2$

Let T, T', θ_0 be as above. Let

A_0 be the function on $\mathcal{O}_R$ defined by $A_0(x) = 1$ for $x \in 2U_R$

$= i$ for $x \in U_R$

A' be the function $(A_0 \circ S_{T/R})(\theta_0 \circ S^{(2)}_{T/R})$ on $\mathcal{O}_T$

A'' be the function $(A_0 \circ S_{T'/R})(\theta_0 \circ S^{(2)}_{T'/R})$ on $\mathcal{O}_{T'}$

θ' be the character $\theta_0 \circ S_{T/R}$ on $\mathcal{O}_T$

θ'' be the character $\theta_0 \circ S_{T'/R}$ on $\mathcal{O}_{T'}$

Then as a function on $\mathcal{O}_{T'}$, $(A' \circ S_{T'/T})(\theta' \circ S_{T'/T})$

$= (\Delta_o \circ S_{T'/R})(\theta_o \circ S^{(2)}_{T/R} \circ S_{T'/T})(\theta_o \circ S_{T/R} \circ S^{(2)}_{T'/T})$

$= (\Delta_o \circ S_{T'/R})(\theta_o \circ S^{(2)}_{T'/R}) = \Delta''$, i.e. Δ'' may be obtained from Δ' in much the same way that Δ' is obtained from Δ_o.

There exists a unit, β, of T such that $\beta^2 \equiv 1/\eta \mod \mathfrak{y}$ and there exists $\gamma \in \mathcal{O}_T$ such that for $x \in \mathcal{O}_T$

$\mu(\beta\pi^r x + 1)\varphi(\alpha\beta\pi^r x) = \Delta'(x)\theta'(\gamma x)$.

For $x \in \mathcal{O}_T$, (precisely as in paragraph (a)) $S_{K/k}(x) = S_{T'/T}(x)$, $S^{(2)}_{K/k}(x) = S^{(2)}_{T'/T}(x)$ and also

$(\mu \circ N_{K/k})(1 + \beta\pi^r x)\ (\varphi \circ S_{K/k})(\alpha\beta\pi^r x) =$

$\mu(1 + S_{K/k}(\beta\pi^r x) + S^{(2)}_{K/k}(\beta\pi^r x))\ (\varphi \circ S_{K/k})(\alpha\beta\pi^r x)$

$= \mu(1 + S_{K/k}(\beta x)\pi^r)\ \varphi(S_{K/k}(\alpha\beta x)\pi^r)\ \mu(1 + \pi^{2r} S^{(2)}_{K/k}(\beta x))$

$= \Delta'(S_{K/k}(x))\ \theta'(\gamma S_{K/k}(x))\ \bar{\varphi}(\pi^{2r}\alpha S^{(2)}_{K/k}(\beta x)) =$

$(\Delta' \circ S_{T'/T})(x)\ \theta''(\gamma x)(\theta_o \circ S_{T/R})(\eta S^{(2)}_{K/k}(\beta x))$ (from definition of η)

As $\eta S^{(2)}_{K/k}(\beta x) = \eta\beta^2 S^{(2)}_{T'/T}(x) \equiv S^{(2)}_{T'/T}(x) \mod \mathfrak{y}$ and as $\theta_o \circ S_{T/R}$ is trivial on $\mathfrak{y} \cap T$, it follows that the above expression may be written

$(\Delta' \circ S_{T'/T})(x)\ \theta''(\gamma x)\ (\theta' \circ S^{(2)}_{T'/T})(x) = \Delta''(x)\ \theta''(\gamma x)$ (the last equality following from the previously derived relation between Δ'' and Δ').

By the theory of local root numbers we now have

$$\frac{(\mu,\varphi)^n}{(\chi,\Phi)} = \frac{\{\varphi(\alpha)\mu(\alpha)\bar{\Delta}'(\gamma)\left(\frac{1+i}{\sqrt{2}}\right)^f(-1)^{f-1}\}^n}{\Phi(\alpha)\chi(\alpha)\bar{\Delta}''(\gamma)\left(\frac{1+i}{\sqrt{2}}\right)^{nf}(-1)^{nf-1}} = (-1)^{n-1}\frac{(\bar{\Delta}'(\gamma))^n}{\bar{\Delta}''(\gamma)}$$

$= (-1)^{n-1}\,(\bar{\Delta}'(\gamma))^n/\bar{\Delta}''(\gamma))$ which is $(-1)^{n-1}$ as $\Delta''(\gamma)$

$= (\Delta' \circ S_{T'/T})(\gamma)(\theta' \circ S^{(2)}_{T'/T})(\gamma) = \Delta'(n\gamma)\ \theta'(\frac{n}{2}(n-1)\gamma)$

$= (\Delta'(\gamma))^n$ (using the fact that $\gamma \in T$ and using one of the elementary properties of the function Δ')

It thus follows that in any case the right hand side of (§§) is $(-1)^{(m+1)(n-1)}$ and therefore for $m \geq 0$, $Q_{K/k}(\chi) = (-1)^{d(n-1)}$, which was the result for $m = -1$. Thus for K/k unramified Q is completely independent of m. This completes the treatment of the unramified case.

K/k Purely Ramified

As in the unramified case, estimates of $S^{(j)}_{K/k}(\mathfrak{P}^m)$ will be needed. The following will be adequate for our purposes.

Lemma K/k of degree n and relative ramification e then

1. $S_{K/k}(\mathfrak{P}^m) \subset \mathfrak{p}^{m'} \Leftrightarrow m' \leq \left[\frac{m + ord_{\mathfrak{P}}\,\vartheta_{K/k}}{e}\right]$
   (valid for K/k not normal)

2. If K/k is normal, j an integer between 1 and n-1 and if no non-trivial element of the galois group has order which divides j then $S^{(j)}_{K/k}(\mathfrak{P}^m) \subset \mathfrak{p}^{\left[\frac{jm + ord_{\mathfrak{P}}\,\vartheta_{K/k}}{e}\right]}$

Proof

1. Let π be a prime element of k and let $\mathfrak{d}_{K/k} = \mathfrak{P}^d$. The set of all $A \in K$ such that $S_{K/k}(A\mathfrak{P}^m) \subset \mathfrak{o}_k$ is $\mathfrak{P}^{-m}\mathfrak{d}_{K/k}^{-1}$.
Hence $S(\mathfrak{P}^m) \subset \mathfrak{p}^{m'} \Leftrightarrow S(\pi^{-m'}\mathfrak{P}^m) \subset \mathfrak{o}_k \Leftrightarrow \pi^{-m'} \in \mathfrak{P}^{-m-d}$
$\Leftrightarrow -em' \geq -m-d \Leftrightarrow m' \leq (m+d)/e \Leftrightarrow m' \leq \left[\frac{m+d}{e}\right]$

2. Consider the family, V, of all subsets of the galois group, G(K/k), which contain j elements. Two such subsets X, Y will be said to be equivalent if there exists an element, σ, in the group such that $\sigma X = Y$. This is obviously a true equivalence relation and therefore V may be split into non-overlapping equivalence classes. There are at most n subsets in each equivalence class. We assert that under the hypothesis of this lemma there are exactly n subsets in each equivalence class. Suppose otherwise then there exists a subset $X \in V$ and an element σ of the group such that $\sigma X = X$. Hence if $\delta \in X$ then $\sigma\delta \in X$. Let $\langle\sigma\rangle$ be the cyclic group generated by σ. It follows that if one element of a right coset $\langle\sigma\rangle\delta$ of $\langle\sigma\rangle$ lies in X, then the whole coset lies in X. Certainly X is covered by right cosets of $\langle\sigma\rangle$, these do not overlap and we have shown the cosets which meet X lie completely in X. It follows that the order of σ divides j, which contradicts the hypothesis. Hence in each equivalence class there are n distinct subsets and it follows from the definition of $S_{K/k}^{(j)}$ and of equivalence that for $x \in K$, $S_{K/k}^{(j)}(x)$ is the sum of traces of products of j conjugates of x. Hence $S_{K/k}^{(j)}(\mathfrak{P}^m) \subset$

with the reservation that 0 is not admissible if the intersection of U_k with the norm group is $(1+\mathcal{Y})$, i.e. if $n = (U_k : NU_K) = (U_k : 1+\mathcal{Y}) = N\mathcal{Y} - 1$.

The previous estimates on traces reduces now to

$$S^{(j)}(\mathcal{P}^r) \subset \mathcal{Y}^{\left[\frac{jr+n-1}{n}\right]} \qquad \text{for } 1 \leq j \leq n-1.$$

The computations are greatly simplified by the existance of π, a prime element in k such that $x^n + (-1)^n \pi$ is the polynomial of which K/k is the splitting field. The existance follows from the fact that k contains the n-th roots of unity and that there exists π, a prime element of k which lies in the norm group. Then the splitting field K' of the above polynomial is of degree n and ramified. Hence K'/k is purely ramified and class field to the union of group $<\pi>\cdot(1+\mathcal{Y})$ with the unique subgroup of index n of the $(N\mathcal{Y}-1)$ roots of 1 in k. Hence $K' = K$. Furthermore the roots of the above polynomial are prime elements of K. Hence we may pick Π, a prime element in K such that $\pi = N_{K/k}(\Pi) = (-1)^{n+1}\Pi^n$. This choice of π and Π will be used throughout the analysis of this case.

Let τ be a fixed non-trivial character of k^* which is trivial on the norm group. If χ is a character of K^* trivial on K_N^*, let μ be a character of k^* such that $\mu \circ N_{K/k} = \chi$, and <u>such that the conductor of μ has the smallest possible exponent</u>. The set of all characters of k^* whose composition with the relative norm

$S_{K/k}(\mathfrak{P}^{mj})$ and so the second part of the lemma follows from the first.

We now consider cyclic ramified extension of prime degree. As may be expected the computation is more difficult if the prime, $\mathfrak{y}$, divides the degree.

Notation

T is the inertial subfield of k/R

θ is the standard additive character of R

θ_o is the character θ_{p-1} of R^+

θ' is the character $\theta_o \circ S_{T/R}$ of T^+

For p = 2 :

Δ_o is the function on $\mathcal{O}_R$ which is 1 on the ideal (2) and is i on the group of units.

Δ' is the function $(\Delta_o \circ S_{T/R})(\theta_o \circ S^{(2)}_{T/R})$ on $\mathcal{O}_T$

K/k Ramified Cyclic of Prime degree n, p ≠ n.

Introduction

Conductor of K/k = $\mathfrak{y}$, $\mathfrak{d}_{K/k} = \mathfrak{P}^{n-1}$

Let $\mathfrak{d}_k = \mathfrak{y}^d$, then $\mathfrak{d}_K = \mathfrak{P}^{n(d+1)-1}$

The group of characters of k^* which are trivial on the norm group, $N_{K/k}K^*$, is cyclic of order n. Each non-trivial character in this group generates the group and has conductor $\mathfrak{y}$. Hence in the notation of Chapter I, $s_1 = -1$, $s_2 = s_3 = \dots = s_n = 0$, and therefore the integers admissible with respect to K/k are -1, 0, nt, where t runs through all integers greater than 0 and gives χ, is $(\mu, \tau\mu, \dots, \tau^{n-1}\mu)$.

In the following let the conductor of χ be $\mathfrak{P}^{1+m}$.

1. <u>$m = -1$</u> (i.e. χ unramified)

conductor $\mu = \mathfrak{y}^0$

conductor $\mu\tau_j = \mathfrak{y}$ for $1 \leq j \leq n-1$

Hence by a previous lemma,

$$Q_{K/k}(\chi) = \frac{(\mu, \psi_{\pi^{-d}})}{(\chi, \Psi_{\Pi^{-nd-n+1}})} \prod_{j=1}^{n-1} (\mu\tau_j, \psi_{\pi^{-d-1}})$$

As $\pi = N_{K/k}\Pi$, $N\mathfrak{P} = N\mathfrak{y}$,

$$\frac{(\mu, \psi_{\pi^{-d}})}{(\chi, \Psi_{\Pi^{-nd-n+1}})} = \frac{1 - N\mathfrak{y}^{-1}\mu(\pi^{-1})}{1-\mu(\pi)} \cdot \frac{1-\chi(\Pi)}{1-N\mathfrak{P}^{-1}\chi(\Pi^{-1})} = 1$$

whence $Q_{K/k}(\chi) = \prod_{j=1}^{n-1} (\tau_j, \psi_{\pi^{-d-1}})$, as the symbols appearing on the right are local root numbers in the sense of chapter II and therefore depend only upon the behavior of the characters on U_k. The product on the right does not depend upon the particular choice of unramified chracter, χ, and therefore must be an invariant of the fields K/k. The product is easily computed if n is odd as then $Q_{K/k}(\chi) = \prod_{j=1}^{(n-1)/2} \{(\tau^j, \psi_{\pi^{-d-1}})(\tau^{n-j}, \psi_{\pi^{-d-1}})\}$

But $\tau^{n-j} = \tau^{-j} = \overline{\tau^j}$, whence $(\tau^{n-j}, \psi_{\pi^{-d-1}}) = \tau^j(-1)\overline{(\tau^j, \psi_{\pi^{-d-1}})}$

As n is odd $\tau(-1) = 1$ (as -1 lies in the norm group). It follows that

$$Q_{K/k}(\chi) = 1 \quad \text{for n odd}$$
$$= (\tau, \psi_{\pi^{-d-1}}) \quad \text{for } n = 2.$$

2. <u>$m \geq 0$</u>

By the previous determination of integers admissible with respect to K/k, $m = nt$, $t \geq 0$. By the analysis of Chapter I.

the conductor of $\mu = \mathfrak{y}^{1+t}$ $(0 \leq j \leq n-1)$, whence

$$Q_{K/k}(\chi) = \frac{\prod_{j=0}^{n-1} (\mu\tau^j, \psi_{\pi^{-d-1-t}})}{(\chi, \Psi_{\Pi^{-n(d+1+t)}})}$$

but $\Pi^{n(d+1+t)} = (-1)^{(n+1)(d+1+t)} \pi^{d+1+t}$

Hence the denominator is $(\chi(-1))^{(n+1)(d+1+t)} (\chi, \Psi_{\pi^{-d-1-t}})$

Also $\chi(-1) = (\mu(-1))^n$. It follows that if we set

$\varphi = \psi_{\pi^{-d-1-t}}$, $\Phi = \Psi_{\pi^{-d-1-t}}$, then $\Phi = \varphi \circ S_{K/k}$ and

$Q_{K/k}(\chi) = \left[\prod_{j=0}^{n-1} (\mu\tau^j, \varphi)\right] / (\chi, \Phi)$

2.1. <u>m=0</u>

Conductor of $\chi = \mathfrak{P}$. $N\mathfrak{P} = N\mathfrak{y}$, hence

$\sqrt{N\mathfrak{y}}(\chi, \Phi) = \Sigma_{x \in U_K/(1+\mathfrak{P})} \chi(x)\Phi(x)$. Taking as representatives

of the residue classes of U_K modulo $(1+\mathfrak{P})$ the $(N\mathfrak{y}-1)$ roots

of 1 in K, all of which lie in k, the sum on the right becomes

$\Sigma_{x \in U_k/(1+\mathfrak{y})} \mu^n(x)\varphi^n(x) = \sqrt{N\mathfrak{y}}(\mu^n, \varphi^n)$, whence

$Q_{K/k}(\chi) = \left[\prod_{j=0}^{n-1} (\mu\tau^j, \varphi)\right] / (\mu^n, \varphi^n)$, which, by a previously quoted result of Hasse and Davenport, is just $\prod_{j=1}^{n-1} (\tau^j, \varphi)$

As $t = 0$, $\varphi = \psi_{\pi^{-d-1}}$ and therefore the result is the same as for the case $m = -1$.

2.2. <u>$t > 0$</u>

2.2.1.1 <u>$1+t$ even, $n \neq 2$</u>

Here $1+nt$ is even. There exists $\alpha \in U_K$ such that

$\mu(1+z) = \overline{\varphi}(\alpha z)$ for all $z \in \mathcal{Y}^{(1+nt)/2}$. From the estimates on traces it is readily verified that for $\operatorname{ord}_{\mathcal{P}} w \geq (1+nt)/2$, we have $S(w) \in \mathcal{Y}^{(1+t)/2}$, $S^{(j)}(w) \in \mathcal{Y}^{1+t}$ for $2 \leq j \leq n-1$, $N(w) \in \mathcal{Y}^{1+t}$, whence $\chi(1+w) = \mu(1 + S(w)) = \overline{\varphi}(\alpha S(w))$

$$= \Phi(\alpha w).$$

Furthermore, $(\mu\tau^j)(1+z) = \overline{\varphi}(\alpha z)$ for $z \in \mathcal{Y}^{(1+t)/2}$, as τ is trivial on $1+\mathcal{Y}$

Applying the formula for the root numbers,

$$C_{K/k}(\chi) = \frac{\prod_{j=0}^{n-1}\left[(\mu\tau^j)(\alpha)\,\varphi(\alpha)\right]}{\chi(\alpha)\,\Phi(\alpha)} = \prod_{j=0}^{n-1}\tau^j(\alpha) = \tau(\alpha)^{n(n-1)/2} = 1$$

2.2.1.2. <u>1+t even, n=2</u>

Here the conductor of χ is $\mathcal{P}^{1+2t}$, $(1+2t)$ of course odd. Also $\pi = N(\Pi) = -\Pi^2$. Certainly $\mathcal{Y} \nmid 2$.

As in the previous case there exists unit α in k such that

$\mu(1+z) = \overline{\varphi}(\alpha z) = (\mu\tau^j)(1+z)$ for all $z \in \mathcal{Y}^{(1+t)/2}$

For $w \in \mathcal{P}^{1+t}$, $\operatorname{ord}_{\mathcal{Y}} S(w) \geq (1+t)/2$, $\operatorname{ord}_{\mathcal{Y}} N(w) \geq 1+t$, whence $\chi(1+w) = \mu(1+S(w)+N(w)) = \mu(1+S(w)) = \overline{\varphi}(\alpha S(w)) = \overline{\Phi}(\alpha w)$.

There exists an element η of T such that $\overline{\Phi}(\alpha\ \pi^{2t} x) = (\theta_0 \circ S_{T/R})(\eta x)$ for all $x \in \mathcal{O}_T$. Hence,

$(\theta_0 \circ S_{T/R})(\eta x) = \overline{\Phi}(\alpha(-1)^t \pi^t x) = \varphi(2\alpha\pi^t x)$ for $x \in \mathcal{O}_T$, a relation which we hold for future use.

Finally there exists $\gamma \in \mathcal{O}_T$ such that for all integers x in T, $\Phi(\alpha\Pi^{2t}(\frac{x^2}{2}+\gamma x)) = \chi(1+x\Pi^{t})\Phi(\alpha x\Pi^{t})$. Using the relations between χ and μ and between φ and Φ, the right side becomes: $\varphi(\alpha S(x\Pi^{t}))\ \mu(1+S(x\Pi^{t})+N(x\Pi^{t}))$

$= \varphi(\alpha S(x\Pi^{t}))\ \mu(1+S(x\Pi^{t}))\ \mu(1+x^2\pi^{t}) = \overline{\varphi}(\alpha\ x^2\pi^{t})$

$= \overline{\varphi}(\frac{1}{2}\alpha x^2\pi^{t}) = \overline{\Phi}((-1)^t\frac{1}{2}\alpha x^2\Pi^{2t})$

$= \overline{\Phi}(\alpha\Pi^{2t}\frac{x^2}{2})$; comparing this with the left side of the condition on γ, clearly $\gamma = 0$.

Applying the root number formulae,

$$Q_{K/k}(\chi) = \frac{[\mu(\alpha)\varphi(\alpha)][(\mu\tau)(\alpha)\varphi(\alpha)]}{\chi(\alpha)\Phi(\alpha)\left(\frac{-2\eta}{\mathcal{y}}\right)(-1)^{f-1}\left(\sqrt{\left(\frac{-1}{p}\right)}\right)^f} = \frac{\tau(\alpha)}{\left(\frac{-2\eta}{\mathcal{y}}\right)(-1)^{f-1}\left(\sqrt{\left(\frac{-1}{p}\right)}\right)^f}$$

where f is the absolute degree of $\mathcal{y}$. As τ is of order 2 and $\alpha\in U_k$, $\tau(\alpha) = \left(\frac{\alpha}{\mathcal{y}}\right)$, whence

$$Q_{K/k}(\chi) = \left[\left(\frac{-2\alpha\eta}{\mathcal{y}}\right)(-1)^{f-1}\left(\sqrt{\left(\frac{-1}{p}\right)}\right)^f\right]^{-1}$$

. We assert that this is $(\tau, \psi_{\pi^{-d-1}})$, i.e. the result is the same as previously when $n = 2$, $m = -1, 0$.

To prove this let δ be a unit of T, $\delta \equiv 2\alpha/\eta \mod \mathcal{y}$, then $(Q(\chi))^{-1} = \left(\frac{-\delta}{\mathcal{y}}\right)(-1)^{f-1}\left(\sqrt{\left(\frac{-1}{p}\right)}\right)^f$, and also by the relation between Θ_δ and φ, $(\Theta_\delta \circ S_{T/R})(x) = \varphi(\delta\pi^{t}x) = \psi_{\pi^{-d-1}}(\delta x)$ for all $x\in\mathcal{O}_T$. Let τ' be the restriction of τ to $\mathcal{O}_T$. As $(\tau,\psi_{\pi^{-d-1}})$ depends only upon the behavior of the additive and multiplicative characters on the $(N\mathcal{y}-1)$ roots of 1 in k, all of which lie in T, and as $\psi_{\pi^{-d-1}}$ coincides with $(\Theta^*)_{\delta^{-1}}$ on $\mathcal{O}_T$, it is clear that

$$(\tau, \psi_{\pi^{-d-1}}) = (\tau', \theta'_{\delta^{-1}}) = \tau'(\delta^{-1})(\tau', \theta') = \left(\frac{\delta}{\mathfrak{y}}\right)(\tau', \theta').$$

Let c be the unique character of the group of units of R which is of order 2 (it exists as $p \neq 2$). Then $\tau' = c \circ N_{T/R}$, $\theta' = \theta_0 \circ S_{T/R}$, whence by Hasse and Davenport and by a classical formula: $(\tau', \theta') = (c, \theta_0)^f(-1)^{f-1} = (-1)^{f-1}\left(\sqrt{\left(\frac{-1}{p}\right)}\right)^f$.

Hence $(\tau, \psi_{\pi^{-d-1}}) = \left(\frac{-\delta}{\mathfrak{y}}\right)(-1)^{f-1}\left(\sqrt{\left(\frac{-1}{p}\right)}\right)^f\left(\frac{-1}{\mathfrak{y}}\right) = Q_{K/k}(\chi)$ as $\left(\sqrt{\left(\frac{-1}{p}\right)}\right)^{2f} = \left(\frac{-1}{\mathfrak{y}}\right)$. This proves the assertion which shows that $Q_{K/k}(\chi)$ has the same value (if $n = 2$) for $m = -1, 0, 2t$ provided t is odd. We shall show at the proper time that this remains valid for t even.

Remark: This analysis gives an explicit formula for $(\tau, \psi_{\pi^{-d-1}})$ ($n = 2$). By the definition of ψ and from the relation between θ' and ψ obtained above, $(\theta \circ S_{T/R})(x/p) = \theta'(x) = \psi_{\pi^{-d-1}}(\delta x)$ $= (\theta \circ S_{k/R})(\delta x/\pi^{d+1}) = (\theta \circ S_{T/R})(\delta x(S_{k/T}(\pi^{-1}/\pi^d)))$,

whence $\delta^{-1} \equiv p\, S_{k/T}(\pi^{-1}/\pi^d) \mod \mathfrak{y}$ and so

$$(\tau, \psi_{\pi^{-d-1}}) = \left(\frac{p\, S_{k/T}(\pi^{-d-1})}{\mathfrak{y}}\right)(-1)^{f-1}\left(\sqrt{\left(\frac{-1}{p}\right)}\right)^f$$

2.2.2.1. <u>1+t odd, p ≠ 2.</u>

conductor of $\mu = \mathfrak{y}^{1+t}$

conductor of $\chi = \mathfrak{P}^{1+nt}$, here the exponents of both conductors are odd. There exists $\alpha \in U_k$, $\eta \in U_T$, $\gamma \in \mathcal{O}_T$ such that

$$\mu(1+z) = \overline{\varphi}(\alpha z) \quad \text{for all } z \in \mathcal{Y}^{1+(t/2)}$$

$$\theta'(\eta x) = \overline{\varphi}(\alpha \pi^{t} x) \quad \text{for all } x \in \mathcal{O}_T$$

$$\varphi(\alpha \pi^{t}(\tfrac{x^2}{2} + \gamma x)) = \varphi(\alpha \pi^{t/2} x)\ \mu(1+x\pi^{t/2}) \quad \text{for all } x \in \mathcal{O}_T$$

We assert that

$$\chi(1+w) = \overline{\Phi}(\alpha' w) \quad \text{for all } w \in \mathfrak{p}^{1+(nt/2)}$$

$$\Theta'(\eta' x) = \overline{\Phi}(\alpha' \Pi^{nt} x) \quad \text{for } x \in \mathcal{O}_T$$

$$\Phi(\alpha' \Pi^{nt}(\tfrac{x^2}{2} + \gamma' x)) = \Phi(\alpha' \Pi^{\frac{nt}{2}} x)\ \chi(1+x\Pi^{nt/2}) \quad \text{for } x \in \mathcal{O}_T$$

where

$$\alpha' = \alpha, \quad \eta' = n\eta, \quad \gamma' = (-1)^{1+(n+1)t/2}\gamma$$

For the first assertion the estimates on traces give

$$\text{ord}_{\mathcal{Y}} S(w) \geq 1 + (t/2)$$

$$\text{ord}_{\mathcal{Y}} S^{(j)}(w) \geq 1 + t$$

$\text{ord}_{\mathcal{Y}} N(w) \geq 1 + (nt/2) \geq 1 + t$, where the symmetric functions are with respect to K/k.

Hence $\chi(1+w) = \mu(1+S(w)) = \overline{\varphi}(\alpha S(w)) = \overline{\Phi}(\alpha w)$, which is the first assertion.

For the second assertion we observe that for $x \in \mathcal{O}_T$

$$\overline{\Phi}(\alpha \Pi^{nt} x) = \overline{\Phi}(\alpha (-1)^{(n+1)t} \pi^{t} x) = \overline{\Phi}(\alpha \pi^{t} x) = \overline{\varphi}(n \alpha \pi^{t} x) = \Theta'(n\eta x),$$

which is the second assertion.

For the third assertion the estimates on traces are

$$S(\mathfrak{p}^{nt/2}) \subset \mathcal{Y}^{t/2}$$

$$S^{(j)}(\mathfrak{p}^{nt/2}) \subset \mathcal{Y}^{t} \quad \text{for } 2 \leq j \leq n-1$$

$$N(\mathfrak{p}^{nt/2}) = \mathcal{Y}^{nt/2} \subset \mathcal{Y}^{1+t} \quad \text{for } n > 2$$

$$\subset \mathcal{Y}^{t} \quad \text{for } n = 2$$

For $n = 2$ we may write $S^{(2)} = N$, and therefore in any case

$$\phi(\alpha \Pi^{nt/2}) \quad \chi(1+x\Pi^{nt/2})$$

$$= \varphi(\alpha\, S(x\Pi^{nt/2}))\ \mu(1+S(x\Pi^{nt/2})+S^{(2)}(x\Pi^{nt/2})) =$$

$$\varphi(\alpha\pi^{t}\Big[\tfrac{1}{2}\Big(\frac{S(x\Pi^{nt/2})}{\pi^{t/2}}\Big)^2 + \gamma\Big(\frac{S(x\Pi^{nt/2})}{\pi^{t/2}}\Big)\Big])\ \bar\varphi(\alpha S^{(2)}(x\Pi^{nt/2}))$$

$$= \varphi(\alpha(\tfrac{1}{2}(S(x\Pi^{nt/2}))^2 - S^{(2)}(x\Pi^{nt/2})))\bar\varphi(\alpha\gamma\Pi^{t/2}S(x\Pi^{nt/2}))$$

$$= \varphi(\alpha\tfrac{1}{2}S(x^2\Pi^{nt}))\ \bar\varphi(\alpha\gamma\pi^{t/2}x\Pi^{nt/2})$$

$$= \Phi\Big\{\alpha\Pi^{nt}\Big(\frac{x^2}{2} - \gamma x\Big(\frac{\pi}{\Pi^n}\Big)^{t/2}\Big)\Big\} \qquad = \Phi\Big(\alpha\Pi^{nt}\Big(\frac{x^2}{2}+\gamma' x\Big)\Big)$$

which is the third assertion.

Finally we note that $(\tau^{j}\mu)(1+x) = \bar\varphi(\alpha x)$ for $x \in \mathcal{Y}^{1+(t/2)}$

Hence by the theory of local root numbers

$$Q_{K/k}(\chi) = \frac{\prod_{j=0}^{n-1}\Big\{(\tau^j\mu)(\alpha)\varphi(\alpha)\bar\varphi(\alpha\pi^t\gamma^2/2)\Big(\frac{-2\eta}{\mathcal{Y}}\Big)(-1)^{f-1}\Big(\sqrt{\big(\tfrac{-1}{p}\big)}\Big)^f\Big\}}{\chi(\alpha)\,\Phi(\alpha)\,\bar\Phi(\alpha\Pi^{nt}\gamma^2/2)\Big(\frac{-2n\eta}{\mathcal{Y}}\Big)(-1)^{f-1}\Big(\sqrt{\big(\tfrac{-1}{p}\big)}\Big)^f}$$

$$= \frac{\tau(\alpha)^{n(n-1)/2}\Big(\frac{n}{\mathcal{Y}}\Big)\Big(\frac{-2\eta}{\mathcal{Y}}\Big)^{n-1}\Big\{(-1)^{f-1}\Big(\sqrt{\big(\tfrac{-1}{p}\big)}\Big)^f\Big\}^{n-1}}{\bar\varphi\Big(\frac{\alpha\gamma^2}{2}\{S(\Pi^{nt})-n\pi^t\}\Big)}$$

The denominator is 1 as $S(\Pi^{nt}) = (-1)^{(n+1)t}S(\pi^t) = n\pi^t$.

We must now distinguish between n odd and n even.

(a) <u>$n \neq 2$</u>

Here $n-1$ is even and therefore $(\tau(\alpha))^{n(n-1)\frac{1}{2}} = 1$ and $\big(\frac{-2\eta}{\mathcal{Y}}\big)^{n-1} = 1$, so that

$$Q(\chi) = \Big(\frac{n}{\mathcal{Y}}\Big)\Big((-1)^{f-1}\Big(\sqrt{\big(\tfrac{-1}{p}\big)}\Big)^f\Big)^{n-1} = \Big(\Big(\frac{n}{p}\Big)\Big(\sqrt{\big(\tfrac{-1}{p}\big)}\Big)^{n-1}\Big)^f$$

whence by the quadratic law of reciprocity. $Q_{K/k}(\chi) = (\frac{p}{\pi})^f$.

(b) n = 2

Here $\tau(\alpha) = (\frac{\alpha}{y})$, hence $Q(\chi) = (\frac{-\alpha\eta}{y})(-1)^{f-1}(\sqrt{(\frac{-1}{p})})^f$.

By definition of η, for all $x \in \mathcal{O}_T$

$\theta'(\eta x) = \overline{\varphi}(\alpha\pi^t x) = \psi_{\pi^{-d-1}}(-\alpha x)$

whence $\theta'(x) = \psi_{\pi^{-d-1}}(\delta x)$, where $\delta \equiv -\alpha/\eta \mod y$, $\delta \in U_T$.

It follows from the analysis of case 2.2.1.2. that

$(\tau, \psi_{\pi^{-d-1}}) = (\frac{\delta}{y})(-1)^{f-1}(\sqrt{(\frac{-1}{p})})^f$, from which it follows that

$Q_{K/k}(\chi) = (\tau, \psi_{\pi^{-d-1}})$

2.2.2.2. 1+t odd, n = 2

Here $n \neq 2$, exponent of the conductor of χ is $1+nt$, that of the conductor of μ is $1+t$, both are odd.

There exists $\alpha \in U_k$, $\eta \in U_T$, $\beta \in U_T$, $\gamma \in \mathcal{O}_T$ such that

$\mu(1+z) = \overline{\varphi}(\alpha z)$ for $z \in y^{1+(t/2)}$

$\theta'(\eta x) = \overline{\varphi}(\alpha\pi^t x)$ for $x \in \mathcal{O}_T$

$\Delta'(x)\theta'(\gamma x) = \varphi(\alpha\pi^{t/2}\beta x)\,\mu(1+\beta x\pi^{t/2})$ for $x \in \mathcal{O}_T$

$\eta \equiv 1/\beta^2 \mod y$

$(\mu\tau^j)(1+z) = \overline{\varphi}(\alpha z)$ for all integers j, $z \in y^{1+(t/2)}$

The proofs in 2.2.2.1 show that

$\chi(1+w) = \overline{\Phi}(\alpha w)$ for $w \in \mathfrak{p}^{1+(nt/2)}$

and also

$\theta^*(n\eta x) = \overline{\varphi}(\alpha\Pi^{nt}x)$ for $x \in \mathcal{O}_T$

Let β' be a unit in T such that $\beta'^2 \equiv (n\eta)^{-1}$, i.e. $(\frac{\beta}{\beta'})^2 \equiv n^{-1}$.

We assert that

$\Delta^*(x)\theta^*(\gamma' x) = \varphi(\alpha\Pi^{nt/2}\beta' x)\ \chi(1+\beta' x\Pi^{nt/2})$ for $x \in \mathcal{O}_T$ (§)

where $\gamma' = \gamma + (n-1)/2$.

Precisely as in case 2.2.2.1. the right side of (§) is

$\varphi(\alpha\beta\pi^{t/2}W)\ \mu(1+\alpha\beta\pi^{t/2}W)\ \mu(1+S^{(2)}(x\beta'\Pi^{nt/2}))$,

where $W = (\beta\pi^{\frac{t}{2}})^{-1}S(x\beta'\Pi^{nt/2}) = nx\beta'/\beta$

Trivially, $S^{(2)}(x\beta'\Pi^{nt/2}) = x^2\beta'^2\pi^t\ n\ (n-1)/2$, so that the right side of (§) is

$\Delta^*(n\frac{\beta'}{\beta}x)\theta^*(\gamma\ n\frac{\beta'}{\beta}x)\overline{\varphi}(x^2\alpha\beta'^2\pi^t\ n(n-1)/2) =$

$\Delta^*(n\frac{\beta'}{\beta}x)\theta^*(\gamma\ n\frac{\beta'}{\beta}x)\overline{\theta^*}(x^2\beta'^2\eta\ n(n-1)/2)$.

$n \equiv 1,\ -1 \equiv 1,\ \beta'^2 n\eta \equiv 1,\ (\frac{\beta'}{\beta})^2 \equiv n^{-1} \equiv 1 \Rightarrow \beta/\beta' \equiv 1$,

(modulo γ). Also for $x \in \mathcal{O}_T$, $\theta^*(x^2) = \theta^*(x)$ as $S_{T/R}(x^2) \equiv S_{T/R}(x)$ mod p. As Δ^* and θ^* are functions on residue classes mod γ it follows that the right side of (§) is $\Delta^*(x)\theta^*(x(\gamma + \frac{n-1}{2}))$ which proves the assertion. It now follows that

$$Q_{K/k}(\chi) = \frac{\prod_{j=0}^{n-1}\{(\mu\tau^j)(\alpha)\varphi(\alpha)\overline{\Delta'}(\gamma)\left(\frac{1+i}{\sqrt{2}}\right)^f(-1)^{f-1}\}}{\chi(\alpha)\,\Phi(\alpha)\,\overline{\Delta'}(\gamma+\frac{n-1}{2})\left(\frac{1+i}{\sqrt{2}}\right)^f(-1)^{f-1}}$$

$$= \frac{[\overline{\Delta'}(\gamma)]^n\{\left(\frac{1+i}{\sqrt{2}}\right)^f(-1)^{f-1}\}^{n-1}}{\overline{\Delta'}(\gamma+\frac{n-1}{2})}$$

By the functional equation of Δ^*

$\Delta^*(\gamma + \frac{n-1}{2}) = \Delta^*(\gamma)\Delta^*(\frac{n-1}{2})\overline{\theta^*}((n-1)\gamma/2)$

As shown in Chapter II, $(\Delta'(\gamma))^n = \Delta'(n\gamma)\Theta'(\gamma\, n(n-1)/2)$, also $\Theta' = \overline{\Theta}'$ on $\mathfrak{v}_\tau$, whence

$$Q(\chi) = \frac{\left\{\left(\frac{1+i}{\sqrt{2}}\right)^f (-1)^{f-1}\right\}^{n-1}}{\Delta'\left(\frac{n-1}{2}\right)}$$

Using the relations between Δ', Θ', Θ_0, Δ_0 and the elementary properties of the Δ functions and the expression for $\left(\frac{2}{n}\right)$ given by the quadratic reciprocity law, the right side of the above relation reduces to $\left(\frac{2}{n}\right)^f$.

Thus we have shown:

<u>Lemma</u> If k is a $\mathfrak{p}$-adic number field, K a cyclic ramified extension of prime degree n, $\mathfrak{p} \nmid n$, τ a generator of the characters of k^* which are trivial on the norm group and π a prime element of k which lies in the norm group then

1. If $n = 2$, $Q(\chi) = (\tau, \psi_{\gamma-d-1}) = \left(\frac{p\, S_{k/T}(\pi^{-d-1})}{\mathfrak{p}}\right)(-1)^{f-1}\left(\sqrt{\left(\frac{-1}{p}\right)}\right)^f$

2. If $n \neq 2$,

$Q(\chi) = 1$ if the conductor of χ is $\mathfrak{p}^0$ or $\mathfrak{p}$

$\quad = \left(\frac{p}{n}\right)^{f(1+m)}$ if the conductor of χ is $\mathfrak{p}^{1+m}$, $m > 0$

where

f is the absolute degree of $\mathfrak{p}$

d is the exponent of the absolute different of k

p is the rational prime which $\mathfrak{p}$ divides

K/k Ramified cyclic of degree p

Introduction

Let v be the largest integer such that the v-th ramification subgroup of G(K/k) is not trivial. It follows from the classical relation between the discriminant and the orders of the ramification subgroups that $\mathfrak{d}_{K/k} = \mathfrak{p}^{(p-1)(1+v)}$. Hence

$$\mathfrak{d}_k = \mathfrak{y}^{d}, \quad \mathfrak{d}_K = \mathfrak{p}^{d'}, \quad \text{where } d' = pd + (p-1)(1+v).$$

It follows from the conductor discriminant formula that the conductor of K/k is $\mathfrak{y}^{1+v}$. Hence each of the non-trivial characters of k which are trivial on the norm group have conductor $\mathfrak{y}^{1+v}$ and therefore in the notation of Chapter I, $s_1 = -1$, $s_j = v$ for $2 \leq j \leq p$. If χ is a character of K^* trivial on K^*_N, conductor of $\chi = \mathfrak{p}^{1+m}$, τ is a fixed non-trivial character of k^* trivial on the norm group, μ is a character of k^* such that $\mu \circ N_{K/k} = \chi$ and whose conductor is $\mathfrak{y}^{1+b}$, where $m = g_{K/k}(b)$ then:

1) if $b \leq v$ then $m = b$ and $\mu\tau^j$ has conductor $\mathfrak{y}^{1+v}$ for $1 \leq j \leq p-1$

2) if $b > v$ then $1 + m = p(1 + b) - (p-1)(1+v) = 1+v + p(b-v)$ and $\mu\tau^j$ has conductor $\mathfrak{y}^{1+b}$ for $1 \leq j \leq p-1$.

It follows that the set of all integers, m, admissible with respect to K/k is given by these relations as b runs through the set of all integers ≥ -1 with the possible exception of

$m = v$ (corresponding to $b = v$). We assert that:

v is admissible $\Leftrightarrow$ absolute degree of $\mathfrak{p}$ is not 1. To prove this we first note that the index $((1+\mathfrak{p}^v)NK^* : NK^*)$ is not 1(as $1+\mathfrak{p}^v \not\subset NK^*$) and divides $(k^* : NK^*) = p$, whence the index is p. But v admissible $\Leftrightarrow$ $(1+\mathfrak{p}^v) \cap NK^* \neq (1+\mathfrak{p}^{1+v}) \cap NK^* = (1+\mathfrak{p}^{1+v})$

$\Leftrightarrow$ $((1+\mathfrak{p}^v) : (1+\mathfrak{p}^{1+v})) > ((1+\mathfrak{p}^v) : (1+\mathfrak{p}^v) \cap NK^*)$

$\Leftrightarrow$ $N\mathfrak{p} > p$, which proves the assertion.

For future reference it is noted that the estimate on traces may be written

$$S^{(j)}_{K/k}(\mathfrak{P}^r) \subset \mathfrak{p}^{\left[\frac{jr+(p-1)(v+1)}{p}\right]} \qquad \text{for } 1 \leq j \leq p-1$$

For the ramified extension studied previously, it was posible to choose a prime element, Π, of K such that $\Pi^n + (-1)^n N(\Pi) = 0$. For the exten sion now being considered this is no longer true, but the relation remains valid if equality is replaced by congruence:

__Lemma__ If Π is a prime element of K, $\pi = N_{K/k}(\Pi)$, then

$\Pi^p/\pi(-1)^{p-1} \equiv 1 \mod \mathfrak{P}^{(p-1)v}$ and furthermore

a) if $p|v$ then the congruence is valid mod $\mathfrak{P}^{1+(p-1)v}$

b) if $p \nmid v$ then the congruence is never valid mod $\mathfrak{P}^{1+(p-1)v}$

__Proof__ Let $h(x) = x^p + a_1x^{p-1} + \ldots + a_p$ be the irreducible polynomial in k of which Π is a root. Then $a_p = (-1)^p\pi$ and $a_j \in \mathfrak{p}$ $(1 \leq j \leq p)$. Clearly

$$\Pi^p/\pi(-1)^{p-1} = 1 + (-1)^p\left[\frac{a_1}{\pi}\Pi^{p-1} + \cdots + \frac{a_{p-1}}{\pi}\Pi\right]$$

Also $h'(\Pi) = p\Pi^{p-1} + (p-1)a_1\Pi^{p-2} + \cdots + a_{p-1}$

As is well known, each of the terms in the expression for $h'(\Pi)$ has a different valuation, the smallest $\mathrm{ord}_{\mathfrak{P}}$ being $(1+v)(p-1)$. Either $p\Pi^{p-1}$ is or is not the term with the smallest ordinal. The two cases must be considered seperately.

(a) $(1+v)(p-1) = \mathrm{ord}_{\mathfrak{P}}(p\Pi^{p-1}) = pe+p-1$ (i.e. $v = ep/(p-1)$)
then for $1 \leq j \leq p-1$, $\mathrm{ord}_{\mathfrak{P}}(a_j\Pi^{p-j-1}) > pe+p-1 \Rightarrow$

$\mathrm{ord}_{\mathfrak{P}}(\frac{a_j}{\pi}\Pi^{p-j}) > pe+p-1+(1-p) = pe = (p-1)v$ (where e is the absolute ramification of $\mathfrak{Y}$)

whence $\mathrm{ord}_{\mathfrak{P}}\left[\frac{\Pi^p}{\pi(-1)^{p-1}}-1\right] \geq (p-1)v+1$

(b) $(1+v)(p-1) = \mathrm{ord}_{\mathfrak{P}}(a_i\Pi^{p-i-1})$ $(p \nmid i)$, then
$\mathrm{ord}_{\mathfrak{P}} a_i - i = v(p-1) \Rightarrow p(v-\mathrm{ord}_{\mathfrak{Y}} a_i) = v-i$ (i.e. $v \equiv i \mod p$)
For $j \neq i$, $1 \leq j \leq p-1$,

$\mathrm{ord}_{\mathfrak{P}}(a_i\Pi^{p-i-1}) < \mathrm{ord}_{\mathfrak{P}}(a_j\Pi^{p-j-1}) \Rightarrow$

$\mathrm{ord}_{\mathfrak{P}}(\frac{a_i}{\pi}\Pi^{p-i}) < \mathrm{ord}_{\mathfrak{P}}(\frac{a_j}{\pi}\Pi^{p-j}) \Rightarrow$

$\mathrm{ord}_{\mathfrak{P}}\left[\frac{\Pi^p}{(-1)^{p-1}\pi}-1\right] = \mathrm{ord}_{\mathfrak{P}}(\frac{a_i}{\pi}\Pi^{p-i}) = \mathrm{ord}_{\mathfrak{P}} a_i - i = v(p-1).$

The lemma follows immediately and in addition it follows that $1 \leq v \leq ep/(p-1)$, $p \mid v \Rightarrow v = ep/(p-1)$, which are well known.

During the analysis of this extension, Π is some fixed prime element of K, $\pi = N(\Pi)$.

As before let ψ be the standard additive character of k, andd let Ψ be the corresponding character of K. Let $\varphi = \Psi_{\pi^{-d-1-v}}$. There exists $\alpha_0 \in U_k$ (α_0 unique mod $\mathfrak{y}^{(1+v)/2}$ or mod $\mathfrak{y}^{v/2}$ depending upon which statement makes sense) and there exists $\beta_0 \in U_T$ (β_0 unique mod $\mathfrak{y}$) such that

$$\tau(1+z) = \bar{\varphi}(\alpha_0 z) \quad \text{for} \quad z \in \mathfrak{y}^{(1+v)/2} \quad \text{if } v \text{ is odd}$$
$$z \in \mathfrak{y}^{1+(v/2)} \quad \text{if } v \text{ is even}$$

$$\bar{\varphi}(\alpha_0 x \pi^v \beta_0^p) = \theta'(x) \quad \text{for} \quad x \in \mathcal{O}_T$$

Some elementary properties of the extension K/k shall now be listed.

1) $N(1+\mathfrak{p}^a) = (1+\mathfrak{y}^a) \cap NK^*$ for $1 \leq a \leq v$

$N(Z) \equiv 1 \bmod \mathfrak{y}^a \Rightarrow Z \equiv 1 \bmod \mathfrak{p}^a$

2) For $r \geq 0$, $1+\mathfrak{y}^{1+v+r} = N(1+\mathfrak{p}^{p+v+pr}) = N(1+\mathfrak{p}^{1+v+pr})$

$N(Z) \equiv 1 \bmod \mathfrak{y}^{1+v+r} \Rightarrow$ there exists $A \in K^*$ such that

$Z \equiv A^{\sigma-1} \bmod \mathfrak{p}^{p+v+pr}$ where σ generates $G(K/k)$

3) $N(1+\mathfrak{p}^v) = 1+\mathfrak{y}^{v+1} \Leftrightarrow$ absolute degree of $\mathfrak{y}$ is 1.

4) $(1+\mathfrak{p}^{1+r+v}) \cap (K^*)^{\sigma-1} = (1+\mathfrak{p}^{1+r})^{\sigma-1}$ for $r \geq 0$

5) $S^{(j)}(\mathfrak{p}^a) \subset \mathfrak{y}^{\left[\frac{aj+(p-1)(1+v)}{p}\right]}$ for $1 \leq j \leq p-1$

6) Let $v' = v - \left[\frac{v}{p}\right]$, then $\text{ord}_{\mathfrak{y}}\, p \geq v'$ and

$v' \geq (1+v)/2$ if v is odd
$\geq 1+(v/2)$ if v is even, $p \neq 2$
$= v/2$ if v is even, $p = 2$.

7) If $1 \leq a \leq v'$ then $x \to N(x) \bmod \mathfrak{y}^a$ is an additive homomorphism of $\mathfrak{O}_K$ onto $\mathfrak{O}_k/\mathfrak{y}^a$ with kernel $\mathfrak{p}^a$.

8) For $Z \in K^*$, $N(Z)/Z^p \equiv 1 \bmod \mathfrak{p}^{v(p-1)}$

$Z \in U_K$, $N(Z)/Z^p \equiv 1 \bmod \mathfrak{p}^{pv'}$

9) $\varphi(\alpha_0 S(Z)) = \bar{\varphi}(\alpha_0 N(Z))$ for $Z \in \mathfrak{p}^{(1+v)/2}$ if v is odd

$Z \in \mathfrak{p}^{1+(v/2)}$ if v is even

10) If $u \in U_K$ then $S(u\pi^v)/N(u\pi^v)$ is a unit in k and is congruent modulo $\mathfrak{p}$ to $-(\beta_0/u)^{p-1}$ and if u lies in k then the congruence is modulo $\mathfrak{y}$.

Proofs

1,2) The statements concerning images under the mapping $N_{K/k}$ follows directly from the results of Chapter I. If $N(Z) \in 1+\mathfrak{y}^a$ then from what has just been said, there exists $Z' \in 1+\mathfrak{p}^a$ such that $N(Z/Z') = 1$, whence $Z \in Z'(K^*)^{\sigma-1} \subset Z'(1+\mathfrak{p}^v) \subset (1+\mathfrak{p}^a)$. A similar argument completes the proof of (2).

3) The proof of this statement is contained in the analysis of whether or not v is admissible with respect to K/k.

4) For $Z \in \mathfrak{p}^{1+r}$, $(1+Z)^{\sigma-1} = 1 + Z(Z^{\sigma-1}-1)/(1+Z) \in 1+\mathfrak{p}^{1+r+v}$. For inclusion in the opposite direction, induction is used. The statement is first proven for r=0. It is first noted that

$$(\pi^p)^{\sigma-1} = (\pi^p(-1)^{p-1}/\pi)^{\sigma-1} \in (1+\mathfrak{p}^{(p-1)v})^{\sigma-1} \subset (1+\mathfrak{p}^{pv}).$$

If $x \in (1+\mathfrak{p}^{1+v}) \cap (K^*)^{\sigma-1}$ then $x = w^{\sigma-1}$, $w \in K^*$. As the $(N\mathfrak{y}-1)$

roots of unity in K lie in k, we may write $v = u\pi^{ap+b}$, where $0 \leq b \leq p-1$, $u \in (1+\mathfrak{p})$. As $v^{\sigma-1}$, $u^{\sigma-1}$, $(\pi^{ap})^{\sigma-1}$ all lie in $1+\mathfrak{p}^{1+v}$ it follows that $(\pi^{b})^{\sigma-1}$ lies in $1+\mathfrak{p}^{1+v}$, whence $b = 0$ as otherwise π lies in the group generated by π^{b} and π^{p} which implies that $\pi^{\sigma-1} \in 1+\mathfrak{p}^{1+v}$, a contradiction. Thus $x = (u\pi^{ap})^{\sigma-1} \in (1+\mathfrak{p})^{\sigma-1}(1+\mathfrak{p}^{(p-1)v})^{\sigma-1} \subset (1+\mathfrak{p})^{\sigma-1}$, which proves the assertion for $r = 0$. If the statement is true for some $r \geq 0$, let $x \in (1+\mathfrak{p}^{2+r+v}) \cap (K^{*})^{\sigma-1}$, then $x = z^{\sigma-1}$, $z \in 1+\mathfrak{p}^{1+r}$. There exists c, either 0 or a $(N\mathfrak{y} - 1)$ root of unity, such that $z \in (1+c\pi^{1+r})(1+\mathfrak{p}^{2+r})$. If $c = 0$ we are through; hence we may assume $c \neq 0$. As $z^{\sigma-1}$ and $(1+\mathfrak{p}^{2+r})^{\sigma-1}$ lie in $1+\mathfrak{p}^{2+r+v}$, the same must be true for $(1+c\pi^{1+r})^{\sigma-1}$. Hence $(\pi^{1+r})^{\sigma-1} \in 1+\mathfrak{p}^{1+v}$ and therefore by an argument used above $p \mid (1+r)$. Let $1+r = ps$, then $(1+c\pi^{1+r})-(1+c(\pi(-1)^{p-1})^{s}) \in \mathfrak{p}^{1+r+v(p-1)}$, whence there exists a unit, y, in k such that $y^{-1}(1+c\pi^{1+r}) \in 1+\mathfrak{p}^{2+r}$ and therefore $x = z^{\sigma-1} \in (1+\mathfrak{p}^{2+r})^{\sigma-1}$ which completes the proof.

5) As has been noted earlier this statement follows directly from the general relations concerning the ordinals of traces.

6) Let $v = rp + s$, $0 \leq s < p$, then $pe \geq (p-1)v = p(v-r)-s$. Hence, as e is an integer, $e \geq v-r = v'$. The estimates on v' are easily verified.

7) If the mapping is an additive homomorphism then the kernel is $\mathfrak{p}^{a}$, whence by index considerations the mapping is onto.

It is therefore enough to show that $x \to Nx \bmod \mathfrak{y}^{v'}$ is an additive homomorphism on $\mathfrak{O}_K$. Let x, y be integers in K, there are three cases to be considered:

a) $|x| > |y|$, then $z = y/x \in \mathfrak{p}$, and by (5), $N(1+z) \equiv 1+Nz$ mod $\mathfrak{y}^{v'}$, whence $N(x+y) = Nx\, N(1+z) \equiv Nx\,(1+Nz) \equiv Nx+Ny$ mod $\mathfrak{y}^{v'}$.

b) $|x| \geq |y|$, $x \in \mathfrak{p}$, then by (5), $N(1+z) \equiv 1+Nz$ mod $\mathfrak{y}^{v'-1}$, whence by the same manipulation as above $N(x+y) \equiv Nx+Ny$ mod $\mathfrak{y}^{v'}$.

c) $x, y \in U_K$, then $x = a+x'$, $y = b+y'$, where a, b are $(N\mathfrak{y}-1)$ roots of 1 and $x', y' \in \mathfrak{p}$. Hence $N(x+y) = N(a+b+x'+y')$ $\equiv N(a+b) + N(x'+y')$ mod $\mathfrak{y}^{v'}$ (valid by (a) if $a+b \neq 0$, trivially true if $a+b = 0$). Applying (6) and cases (a),(b) it follows that $N(x+y) \equiv (Na+Nx') + (Nb+Ny') \equiv N(a+x')+N(b+y') = Nx+Ny$.

8) It has already been shown that $\Pi^p/N(\Pi) \equiv (-1)^{p-1}$ mod $\mathfrak{p}^{v(p-1)}$. As $pv' \geq (p-1)v$, it follows from (6) that the right side of the congruence may be replaced by $+1$. Hence it is enough to prove the assertion concerning elements of U_K. As a direct consequence of (6), $x \to x^p$ mod $\mathfrak{p}^{pv'}$ is an additive homomorphism of $\mathfrak{O}_K$. For $Z \in U_K$, we may write $Z = a_0 + a_1\Pi + \dots + a_{p-1}\Pi^{p-1}$, $a_0 \in U_K$, $a_j \in \mathfrak{O}_K$, whence $N(Z)/Z^p \equiv \dfrac{a_0^p + a_1^p\pi + \dots + \pi^{p-1}a_{p-1}^p}{a_0^p + a_1^p\Pi^p + \dots + a_{p-1}^p\Pi^{p(p-1)}}$ mod $\mathfrak{p}^{pv'}$. The right is congruent to 1 mod $\mathfrak{p}^{p(\frac{\Pi^p}{\pi}-1)} = \mathfrak{p}^{pv}$, which proves the assertion.

9) For $1+Z \in K^*$, $1 = (\tau \circ N)(1+Z)$. Let a be the integer in the set $(1+(v/2), (1+v)/2)$. For $Z \in \mathfrak{p}^a$, $N(1+Z) \equiv 1+S(Z)+N(Z)$ mod $\mathfrak{y}^{1+v}$ as is verified with the aid of (5). Furthermore $S(Z), N(Z) \in \mathfrak{y}^a$ and therefore $1 = \tau(1+S(Z)+N(Z)) = \overline{\varphi}(\alpha_0 S(Z) + \alpha_0 N(Z))$

from which the assertion follows.

10) Let $E = S(u\pi^{v})/N(u\pi^{v})$, let x be an arbitrary integer in T. Applying (9) to $xu\pi^{v}$, it is found that

$1 = \overline{\varphi}\{\alpha_0(xS(u\pi^{v})+x^pN(u\pi^{v}))\} = \overline{\varphi}(\alpha_0\pi^{v}Nu\ (xE+x^p))$. By (5) E is an algebraic integer. Let E' be an element of T congruent mod $\mathfrak{y}$ to E and u' an element of T congruent mod $\mathfrak{p}$ to u, then $1 = \overline{\varphi}(\alpha_0\pi^{v}u'^{p}(xE'+x^p))$ and therefore by the definition of β_0, $1 = \theta'((\frac{\mu'}{\beta_0})^p(xE'+x^p))$. As $S_{T/R}(x) \equiv S_{T/R}(x^p)$ mod p,

$\overline{\theta}'((\frac{\mu'}{\beta_0})^pE'x) = \theta'((\frac{\mu'}{\beta_0})x)$. The assertion follows using the fact that θ' has conductor p in T.

To facilitate reference these statements shall be designated by the letters E.P. followed by the proper number.

Some of the symbols which will be used consistently through the remainder of the treatment of this type of cyclic extension are listed:

χ is a character of K^* which is trivial on K^*_N

$1+m$ = exponent of the conductor of χ

b is the unique integer such that $m = S_{K/k}(b)$

μ is a character of k^*, of conductor $\mathfrak{y}^{1+b}$, such that $\chi = \mu \circ N_{K/k}$

ψ, Ψ are the standard additive characters of k and K respectively

$$\left.\begin{array}{l}\varphi = \psi_{\pi^{-d-1-v}} \\ \varphi' = \psi_{\pi^{-d-1-b}}\end{array}\right\} \quad \text{additive characters of } k$$

$\Phi = \Psi_{\Pi^{-d'-1-m}}$, an additive character of K

$B = 1$ if $\begin{cases} b \equiv v \\ p \neq 2 \end{cases}$ or if $b < v$

$= (\pi/\Pi^{p})^{d+1+b}$ otherwise

ς is a fixed primative $(p-1)^{st}$ root of unity

a_j is an integer such that $a_j \equiv \varsigma^j \mod p \quad (1 \leq j \leq p-1)$

$\tau_j = \tau^{a_j}$.

The relations between the characters φ, φ', Φ may be easily established.

Lemma
$\varphi' = \varphi_{\pi^{v-b}}$, $B \equiv 1 \mod p^{v(p-1)}$

On $\mathcal{O}_{K'}$ $\Phi = (\varphi \circ S)_{\Pi^{v-b}}$ if either $\begin{matrix} b = v \\ p \neq 2 \end{matrix}$ or if $b < v$.

On K, $\Phi = (\varphi' \circ S)_B$ if $b \geq v$.

Proof
The first assertion follows directly from the definitions and the estimate for B has already been proven. The relations concerning Φ follow from the definitions, the relations between n, b, v and from E.F.(5).

Finally $Q(\chi)$ may be expressed in terms of the characters φ, φ', Φ. It follows from the determination of the various conductors that:

Lemma
$$Q(\chi) = \frac{(\mu,\varphi')\prod_{j=1}^{p-1}(\mu\tau^j,\varphi)}{(\chi,\Phi)} \qquad \text{for } b \leq v$$

$$= \frac{(\mu,\varphi')\prod_{j=1}^{p-1}(\mu\tau^j,\varphi')}{(\chi,\Phi)} \qquad \text{for } b \geq v$$

Detailed Computations

1. $b = -1, m = -1$

Here μ, χ, are unramified. Hence $(\mu\tau^j,\varphi) = (\tau^j,\varphi)$ for $1 \leq j \leq p-1$.

$$(\mu,\varphi')/(\chi,\Phi) = \frac{1-N\mathfrak{y}^{-1}\mu(\pi^{-1})}{1-\mu(\pi)} \cdot \frac{1-\chi(\pi)}{1-N\mathfrak{p}^{-1}\chi(\pi^{-1})} = 1.$$

Hence $Q(\chi) = \prod_{j=1}^{p-1}(\tau^j,\varphi) = 1$ for $p \neq 2$
$= (\tau,\varphi)$ for $p = 2$, the result for $p \neq 2$ being obtained by pairing (τ^j,φ) with (τ^{p-j},φ) for $1 \leq j \leq (p-1)\ 2$.

The remainder of the analysis of this extension consists of the verification of the validity of this result for all b.

Let A be 1 if $p\neq 2$, (τ,φ) if $p=2$.

2. $b = 0 = m$

$$Q(\chi) = \frac{(\mu,\varphi')}{(\chi,\Phi)} \prod_{j=1}^{p-1}(\mu\tau^j,\varphi).$$ The quotient and the product are computed seperately.

Contention : $\prod_{j=1}^{p-1}(\mu\tau^j,\varphi) = A\ \mu((-1)^p\alpha_0^{p-1})$

Proof :

$p \neq 2$, $1+v$ even

If $\text{ord}_{\mathfrak{y}}\, z \geq (1+v)/2$, $\tau(1+z) = \bar{\varphi}(\alpha_0 z) \Rightarrow \tau^{a_j}(1+z) = \bar{\varphi}(a_j\alpha_0 z) \Rightarrow \tau_j(1+z) = \bar{\varphi}(\varsigma^j\alpha_0 z) \Rightarrow (\mu\tau_j)(1+z) = \bar{\varphi}(\varsigma^j\alpha_0 z)$ as μ is trivial on $1+\mathfrak{y}$. Hence $(\mu\tau_j,\varphi) = (\mu\tau_j)(\alpha_0\varsigma^j)\varphi(\alpha_0\varsigma^j)$, whence the contention is easily verified using the fact that ς lies in the norm group.

$p \neq 2$, $1+v$ odd.

As above, if $\text{ord}_{\mathfrak{y}}\, z \geq 1+(v/2)$, $(\mu\tau_j)(1+z) = \bar{\varphi}(\alpha_0\varsigma^j z)$

There exists $\eta_0 \in U_T$ such that $\theta'(\eta_0 x) = \overline{\varphi}(\alpha_0 \pi^v x)$ for $x \in \mathcal{O}_T$.

Hence $\theta'(\zeta^j \eta_0 x) = \overline{\varphi}(\alpha_0 \zeta^j \pi^v x)$. There exists $\gamma_0 \in \mathcal{O}_T$ such that
$\tau(1+x\pi^{v/2})\varphi(\alpha_0 x \pi^{v/2}) = \varphi(\alpha_0 \pi^v(\frac{x^2}{2} + \gamma_0 x))$, whence
$\tau_j(1+x\pi^{v/2})\varphi(\alpha_0 \zeta^j x \pi^{v/2}) = \varphi(\alpha_0 \zeta^j \pi^v(\frac{x^2}{2} + \gamma_0 x))$.

Hence $\prod_{j=1}^{p-1} (\mu\tau^j, \varphi) = \prod_{j=1}^{p-1} \{(\mu\tau_j)(\alpha_0\zeta^j)\varphi(\alpha_0\zeta^j)\left(\frac{-2\zeta^j\eta_0}{\mathcal{Y}}\right)\overline{\varphi}(\alpha_0\zeta^j\pi^v\frac{\gamma_0^2}{2})(-1)^{f-1}(\sqrt{(\frac{-1}{p})})^f\}$

$= \mu(-\alpha_0^{p-1})(\frac{-1}{\mathcal{Y}})(\frac{-1}{p})^{f\frac{p-1}{2}} = \mu(-\alpha_0^{p-1})$, as $(\frac{-1}{\mathcal{Y}}) = (\frac{-1}{p})^f$, which proves the contention for $p \neq 2$.

For $p = 2$, the product is just $(\mu\tau, \varphi)$.

If $1+v$ is even, $\tau(1+z) = \overline{\varphi}(\alpha_0 z)$ for $\text{ord}_{\mathcal{Y}}\, z \geq (1+v)/2$, whence $(\mu\tau)(1+z) = \overline{\varphi}(\alpha_0 z)$. Hence $(\mu\tau, \varphi) = (\mu\tau)(\alpha_0)\varphi(\alpha_0)$ $= \mu(\alpha_0)\{\tau(\alpha_0)\varphi(\alpha_0)\} = A\,\mu(\alpha_0)$.

If $1+v$ is odd, $(\mu\tau)(1+z) = \overline{\varphi}(\alpha_0 z)$ for $\text{ord}_{\mathcal{Y}}\, z \geq 1+(v/2)$,

$$\overline{\varphi}(\alpha_0 \pi^v x) = \theta'(x/\beta_0^2) \quad \text{for } x \in \mathcal{O}_T$$

$$\tau(1+\pi^{v/2}x)\varphi(\alpha_0\pi^{v/2}x) = A'(x/\beta_0)\theta'(\gamma_0 x/\beta_0) \quad \text{for } x \in \mathcal{O}_T$$

whence $(\mu\tau)(1+\pi^{v/2}x)\varphi(\alpha_0\pi^{v/2}x) = A'(x/\beta_0)\theta'(\gamma_0 x/\beta_0)$.
Hence precisely as before $(\mu\tau, \varphi) = \mu(\alpha_0)(\tau, \varphi)$, which completes the proof of the contention.

To compute $(\mu, \varphi')/(\chi, \theta)$, let μ_0 be the restriction of μ to T^*. As μ and χ have conductors $\mathcal{Y}$ and $\mathcal{P}$ respectively, the corresponding root numbers depend upon the behavior of μ, χ, φ', θ at the $(N\mathcal{Y}-1)$ roots of 1 and therefore can be expressed in terms of the root number (μ_0, θ').

$\varphi' = \psi_{\pi^{-d-1}} = (\theta \circ S_{K/R})_{\pi^{-d-1}}$; $\theta' = \theta_{p^{-1}} \circ S_{T/R}$, whence

$(\theta' \circ S_{k/T}) = (\theta \circ S_{k/R})_{p-1} = \varphi'_{\pi^{d+1}/p}$; hence $\varphi' = (\theta' \circ S_{k/T})_{p\pi^{-d-1}}$ and therefore the restriction of φ' to $\mathcal{O}_T$ is $(\theta')_{pS_{k/T}(1/\pi^{d+1})}$.

It follows that $(\mu, \varphi') = (\mu_0, \theta')\bar{\mu}_0\{p\, S_{k/T}(1/\pi^{d+1})\}$. As $x \to x^p$ is an automorphism of the residue class field and $\theta'(x^p) = \theta'(x)$ for $x \in \mathcal{O}_T$, it is easily shown that $(\mu_0^p, \theta') = (\mu_0, \theta')$, a result which shall be used shortly.

On $\mathcal{O}_K$, $\Phi = (\varphi \circ S_{K/k})_{\Pi^\nu} = (\varphi'_{\pi^{-\nu}} \circ S_{K/k})_{\Pi^\nu} =$

$((\theta' \circ S_{k/T})_{p\pi^{-d-1-\nu}} \circ S_{K/k})_{\Pi^\nu}$, whence the restriction of Φ to $\mathcal{O}_T$ is:

$$(\theta')_{p\, S_{k/T}(\pi^{-d-1}S_{K/k}(\Pi^\nu)/N_{K/k}(\Pi^\nu))},$$

while the restriction of χ to $\mathcal{O}_T$ is $\mu_0^{\,p}$. From E.P.(10),

$S_{K/k}(\Pi^\nu)/N_{K/k}(\Pi^\nu) \equiv -\beta_0^{\,p-1} \mod \mathcal{Y}$, whence by E.P.(5)

$$\mathrm{ord}_p \left[pS_{k/T}\{\pi^{-d-1}(-\beta_0^{\,p-1})\} - pS_{k/T}\{\pi^{-d-1}S_{K/k}(\Pi^\nu)/N_{K/k}(\Pi^\nu)\}\right] \geq 1.$$

As θ' is trivial on $p\,\mathcal{O}_T$, it follows that the restriction of Φ to $\mathcal{O}_T$ is $\theta'_{p(-\beta_0^{\,p-1})S_{k/T}(\pi^{-d-1})}$ and the subscript is a unit, whence

$$(\chi, \Phi) = \bar{\mu}^p\{p(-\beta_0^{\,p-1})S_{k/T}(\pi^{-d-1})\}\ (\mu_0^{\,p}, \theta').$$

Hence $Q_{K/k}(\chi)/A = \mu(\delta)$,

where $\delta = \{\alpha_0\beta_0^{\,p}pS_{k/T}(\pi^{-d-1})\}^{p-1}$.

The analysis of the case $b = 0$ is completed by showing that $\delta \equiv 1 \mod \mathcal{Y}$.

To prove this last assertion we recall that on $\mathfrak{O}_{T}$, $\theta' = (\bar{\varphi})_{\alpha_0 \beta_0^{\rho} \pi^{v}}$, whence on the same ring, $\bar{\theta}' = \varphi'_{\alpha_0 \beta_0^{\rho}} = (\theta' \circ S_{k/T})_{\alpha_0 \beta_0^{\rho} p \pi^{-d-1}} = \theta' S_{k/T}(\alpha_0 \beta_0^{p} p \pi^{-d-1})$, whence $-1 \equiv \beta_0^{p}\, p\, S_{k/T}(\alpha_0 \pi^{-d-1}) \mod \mathfrak{y}$. Letting α_0' be an element of U_T congruent to α_0 modulo $\mathfrak{y}$ and using E.P.(5), $-1 \equiv \beta_0^{p} \alpha_0' p S_{k/T}(\pi^{-d-1}) \mod \mathfrak{y}$ and the assertion then follows. Hence $\mu(\delta) = 1$ and therefore $Q(\chi) = A$ if $b = 0$.

For $b > 0$, $Q(\chi)$ is computed by means of the formulae of Chapter II. These formulae depend upon whether or not $p = 2$ and whether or not the exponents of the conductors are even. It will be found necessary to consider twenty cases (ten for $p \neq 2$, ten for $p = 2$, each set of ten consisting of four cases in which $0 < b < v$, two cases in which $b = v$ and finally four cases in which $b > v$). The work is simplified by determining all parameters needed for the formulae before performing the detailed case by case computations.

<u>Determination of Parameters</u> ($b > 0$)

The parameter α_0 (unique mod $\mathfrak{y}^{(1+v)/2}$ or mod $\mathfrak{y}^{v/2}$) associated with the behavior of τ on $1+\mathfrak{y}^{(1+v)/2}$ or $1+\mathfrak{y}^{1+v/2}$ has already been defined. We know that there exists $\alpha \in U_k$ unique mod $\mathfrak{y}^{(1+b)/2}$ (resp: $\mathfrak{y}^{b/2}$) such that $\mu(1+z) = \bar{\varphi}(\alpha z)$ for $z \in \mathfrak{y}^{(1+b)/2}$ (resp: $\mathfrak{y}^{1+(b/2)}$).

Lemma 1. Given χ, it is possible to choose α_0 and α in such a manner that there exists $\delta \in U_K$ for which $\alpha = \alpha_0 \, N_{K/k}(\delta)$.

<u>Proof</u>

Let α_0, α be chosen so as to satisfy the conditions involving the possibility of expressing the restrictions of μ and τ to certain subgroups of U_k in terms of additive characters. These conditions remain satisfied if α_0 is replaced by an element congruent modulo $\mathfrak{y}^a$, where $a = (1+v)/2$ or $1+(v/2)$. In any case by N.P.(7) there exists $\delta \in U_K$ such that $N(\delta) \equiv \alpha/\alpha_0 \mod \mathfrak{y}^a$. Replacing α_0 with $\alpha/N(\delta)$, the assertion follows.

Throughout the remainder, α, α_0, δ are to be understood to have been chosen in this manner. The corresponding parameters for χ and $\mu\tau_j$ may now be determined.

<u>Lemma</u> 2:

(a) For $1 \leq j \leq p-1$,

$(\mu\tau_j)(1+z) = \overline{\varphi}(\alpha_j z)$ if $b \leq v$ for $\operatorname{ord}_{\mathfrak{y}} z \geq (1+v)/2$ if v odd, $\geq 1+(v/2)$, if v even

$\overline{\varphi}'(\alpha_j z)$ if $b \geq v$ for $\operatorname{ord}_{\mathfrak{y}} z \geq (1+b)/2$, if b odd, $\geq 1+(b/2)$, if b even

(b) $\chi(1+w) = \overline{\Phi}(\alpha' w)$ for $\operatorname{ord}_{\mathfrak{P}} w \geq (1+m)/2$ if m odd, $1+(m/2)$ if m even

where

$$\alpha_j = \zeta^j \alpha_0 + \alpha\, \pi^{v-b} \qquad \text{if } b \leq v$$
$$\alpha_j = \alpha + \alpha_0 \zeta^j \pi^{b-v} \qquad \text{if } b \geq v$$
$$\alpha' = \alpha\left(\frac{\pi}{\Pi}\right)^{v-b} - \delta\alpha_0 \qquad \text{if } b < v$$
$$\alpha' = \left[\alpha - \alpha_0\delta\left(\frac{\pi}{\Pi}\right)^{b-v}\right]/B \qquad \text{if } b \geq v$$

<u>Proof</u>

(a) For $b \leq v$, conductor of $(\mu\tau_j) = \mathfrak{y}^{1+v}$, conductor of $\mu = \mathfrak{y}^{1+b}$,

$\mu(1+z) = \overline{\varphi}'(\alpha z)$ for $\operatorname{ord}_{\mathfrak{y}} z \geq b''$ (b'' is the integer in the set: $(1+b)/2$, $1+(b/2)$)

Let v'' be the integer in the set: $(1+v)/2$, $1+(v/2)$. It is easily verified that $b \leq v \Rightarrow b'' \leq v''$. Hence for $\text{ord}_{\mathcal{Y}} z \geq v''$, $\mu(1+z) = \bar{\varphi}'(\alpha z)$, whence $(\mu\tau_j)(1+z) = (\mu\tau^{a_j})(1+z) = \bar{\varphi}'(\alpha z)\bar{\varphi}(a_j\alpha_0 z) = \bar{\varphi}(\alpha_j z)$ as $a_j \equiv \zeta^j \bmod p$, $\text{ord}_{\mathcal{Y}} z + \text{ord}_{\mathcal{Y}} p \geq v''+v' \geq 1+v$.

For $b \geq v$, conductor of $\mu\tau_j$ = conductor of $\mu = \mathcal{Y}^{1+b}$. For $\text{ord}_{\mathcal{Y}} z \geq v''$, $\tau(1+z) = \bar{\varphi}(\alpha_0 z)$. But now $b'' \geq v''$ and therefore for $\text{ord}_{\mathcal{Y}} z \geq b''$ $\mu(1+z) = \bar{\varphi}'(\alpha z)$, $\tau(1+z) = \bar{\varphi}(\alpha_0 z)$, whence $(\mu\tau_j)(1+z) = \bar{\varphi}'(\alpha z)\bar{\varphi}(a_j\alpha_0 z)$. The assertion then follows using: $a_j \equiv \zeta^j \bmod p$, $b-v+\text{ord}_{\mathcal{Y}}(pz) \geq b-v+v'+b'' \geq 1+b$.

(b) For $b \leq v$, conductor of $\chi = \mathcal{P}^{1+b}$. If $\text{ord}_{\mathcal{P}} z \geq b''$ it follows from E.P.(5) that $\chi(1+z) = (\mu \circ N_{K/k})(1+z) = \mu(1 + S(z) + S^{(2)}(z) + \ldots + N(z)) = \mu(1 + S(z) + N(z)) = \bar{\varphi}'(\alpha S(z) + \alpha N(z))$ as $S(z), N(z) \in \mathcal{Y}^{b''}$. As $v-b+b'' \geq v''$ it follows from E.P.(9) that $\varphi'(\alpha N(z)) = \varphi(\alpha_0 N(\delta\pi^{v-b} z)) = (\bar{\varphi} \circ S)(\alpha_0 \delta\pi^{v-b} z)$. Hence $\chi(1+z) = \bar{\varphi}'(S(\alpha z))\,(\varphi' \circ S)(\alpha_0\delta\pi^{v-b} z) = \Phi(\alpha' z)$.

For $b>v$, conductor of χ is $\mathcal{P}^{1+m}$, $1+m = p(1+b) - (p-1)(1+v)$. If $p \neq 2$ then $2|m \Leftrightarrow 2|b$

$p = 2$ then $2|m \Leftrightarrow 2|v$. Let m'' be the integer in the set: $(1+m)/2$, $1+(m/2)$. For $\text{ord}_{\mathcal{P}} z \geq m''$ it again follows from E.P.(5) that $\chi(1+z) = \mu(1+S(z)+N(z)) = \bar{\varphi}'(\alpha S(z) + \alpha N(z))$ as $S(z), N(z) \in \mathcal{Y}^{b''}$. As $v-b+m'' \geq v''$ it again follows from E.P.(9) that $\varphi'(\alpha N(z)) = \varphi(\alpha_0 N(\delta z\pi^{v-b})) = (\bar{\varphi} \circ S)(\alpha_0 \delta z\pi^{v-b})$

The proof is completed by substituting this last result in the expression for $\chi(1+z)$ and then expressing φ in terms of φ'.

We now introduce parameters η (with various subscripts) which give the relations between θ' and the restrictions to $\mathcal{V}_T$ of the characters φ_{π^v}, φ'_{π^b}, $\hat{\Phi}_{\Pi^m}$. There has already been occasion to introduce η_0, β_0, units of T such that $(\bar{\varphi})_{\alpha_0\pi^v/\eta_0}$ coincides with θ' on $\mathcal{V}_T$ and $\beta_0^p\eta_0 \equiv 1 \mod \mathfrak{y}$.

<u>Lemma</u> 3.

On $\mathcal{V}_T$ $\bar{\theta}' = \varphi'_{\alpha\pi^b/\eta} = \varphi_{\alpha_j\pi^v/\eta_j} = \varphi'_{\alpha_j\pi^b/\eta_j} = \Phi_{\alpha'\Pi^m/\eta'}$

where:

$\eta \equiv$	$\eta_0\delta^p$				
$\eta_j \equiv$	$\eta_0\zeta^j$	if $b < v$			
$\equiv$	$\eta_0(\zeta^j+\delta^p)$	if $b=v$			
$\equiv$	$\eta_0\delta^p$	if $b > v$			
$\eta' \equiv$	$\beta_0^{p-1}\delta\,\eta_0$	if $b < v$	$\eta' \equiv$	δ/β_0	if $b<v$
$\equiv$	$-\beta_0^{p-1}(\delta^p-\delta)\eta_0$	if $b = v$	$\equiv$	$-(\delta^p-\delta)/\beta_0$	if $b=v$
$\equiv$	$-\beta_0^{p-1}\,\delta^p\eta_0$	if $b > v$	$\equiv$	$-\delta^p/\beta_0$	if $b>v$

<u>Proof</u> As $\varphi'_{\pi^b} = \varphi_{\pi^v}$ and the conductor of φ is $\mathfrak{y}^{1+v}$, the conditions to be imposed on η, η_j, are: $\alpha_0/\eta_0 \equiv \alpha/\eta \equiv \alpha_j/\eta_j \mod \mathfrak{y}$. As $\alpha/\alpha_0 = N(\delta) \equiv \delta^p$, the assertions concerning η, η_j follow without difficulty. For $b < v$, $\Phi_{\alpha'\Pi^m/\eta'} = (\varphi \circ S_{K/k})_{\alpha'\Pi^v/\eta'}$. The restriction of this last character to $\mathcal{V}_T$ is readily found to be $(\bar{\theta}')_h$, where $h \equiv \dfrac{\eta_0}{\eta'}\dfrac{S_{K/k}(\alpha'\Pi^v)}{\alpha_0\pi^v}$. η' is therefore de-

termined by the condition $h \equiv 1$ and the assertion involving η' follows easily with the help of E.P.(10). The proof for $b \geq v$ of the congruence involving η', differs only slightly from the proof just given.

The parameters corresponding to the symbol γ in the results of Chapter II remain to be discussed. We have already introduced γ_0 defined modulo p (when $2 \mid v$) by the conditions:

$$\gamma_0 \in \mathfrak{O}_T, \quad \tau(1+x\pi^{v/2})\varphi(\alpha_0 x\pi^{v/2}) = \begin{cases} \varphi(\alpha_0\pi^v(\frac{x^2}{2}+\gamma_0 x)) & \text{if } p \neq 2 \\ \Delta'(x/\beta_0)\theta'(\gamma_0 x/\beta_0) & \text{if } p = 2 \end{cases}$$

for all $x \in \mathfrak{O}_T$. Likewise if $2 \mid b$, $\gamma \in \mathfrak{O}_T$ may be chosen so that

$$\mu(1+x\pi^{b/2})\varphi'(\alpha x\pi^{b/2}) = \begin{cases} \varphi'(\alpha\pi^b(\frac{x^2}{2}+\gamma x)) & \text{if } p \neq 2 \\ \Delta'(x/\beta)\theta'(\gamma x/\beta) & \text{if } p = 2, \text{ where} \end{cases}$$

in the latter case $\beta \in U_T$, $\beta^2\eta \equiv 1$

The corresponding parameter for χ may now be specified.

Lemma 4

Let β' be an element of U_T such that $\beta'^p\eta' \equiv 1$, then if $2 \mid m$, $x \in \mathfrak{O}_T$,

$$\chi(1+x\Pi^{m/2})\varphi(\alpha' x\Pi^{m/2}) = \begin{cases} \varphi(\alpha'\Pi^m(\frac{x^2}{2}+\gamma' x)) & \text{if } p \neq 2 \\ \Delta'(x/\beta')\theta'(\gamma' x/\beta') & \text{if } p = 2 \end{cases}$$

where γ' is an integer of T such that

if $b < v$: $\gamma'^p \equiv \gamma$

if $b > v$: $\gamma' = 0$ if $p \neq 2$

$\gamma'^2 \equiv 1 + \gamma_0$ if $p = 2$

if $b = v$: $\gamma' \equiv \dfrac{(\eta\gamma)^{1/p} - \delta(\eta_0\gamma_0)^{1/p}}{\eta'}$ if $p \neq 2$

$$\gamma'^2 \equiv \frac{\gamma + \gamma_0\delta+\delta+\sqrt{\delta}}{\delta+1} \qquad \text{if} \quad p = 2$$

Proof. Let H be the function $x \to \chi(1+x\pi^{m/2})\phi(\alpha' x\pi^{m/2})$ on $\mathcal{O}_T$. If $\mathrm{ord}_{\mathfrak{p}} z \geq (\frac{m}{2})$ then by E.P.(5),

$$\mathrm{ord}_y S(z) \geq b''$$

$$\left.\begin{array}{lll} \mathrm{ord}_y S^{(2)}(z) \geq 1+b & \text{if} & v > b \\ \qquad\qquad \geq b & \text{if} & v \leq b \end{array}\right\} \text{ for } p \neq 2$$

$$\mathrm{ord}_y S^{(j)}(z) \geq 1+b \quad \text{for } 3 \leq j \leq p-1,\ p > 3.$$

For $b < v$:

$m = b$, b is even and it follows from the above estimates that for $x \in \mathcal{O}_T$, $H(x) = \mu(1+S(x\pi^{b/2})+N(x\pi^{b/2}))\phi(\alpha' x\pi^{b/2})$

$= \mu(1+S(x\pi^{b/2}))\phi(\alpha(\frac{\pi}{\Pi})^{v-b}x\pi^{b/2})\,\mu(1+N(x\pi^{b/2}))\overline{\Phi}(\delta\alpha_0 x\pi^{b/2})$.

But $\Phi(\alpha(\frac{\pi}{\Pi})^{v-b}x\pi^{b/2}) = \varphi^*(\alpha S(x\pi^{b/2}))$ and the product of this with $\mu(1+S(x\pi^{b/2}))$ is 1 by the defining relation for α.

Furthermore by the relation between Φ and φ and E.P.(9), ($v-(b/2) \geq v''$) $\overline{\Phi}(\delta\alpha_0 x\pi^{b/2}) = \varphi^*(\alpha N(x)\pi^{b/2})$. Hence

$H(x) = \mu(1+\pi^{b/2}N(x))\varphi^*(\alpha\pi^{b/2}N(x)) =$

$$\begin{cases} \varphi^*(\alpha\pi^{b}(\frac{x^{2p}}{2}+\gamma x^p)) \\ \Delta^*(x^2/\beta)\theta^*(\gamma x^2/\beta) \end{cases} = \begin{cases} \overline{\theta}^*(\eta(\frac{x^{2p}}{2}+\gamma x^p)) & \text{if } p \neq 2 \\ \Delta^*(x/\beta')\theta^*(\gamma' x/\beta') & \text{if } p = 2 \end{cases}$$

(using the fact that $\beta'^p \equiv \beta$, $\eta'^p \equiv \eta$). This proves the assertion for $b < v$, $p = 2$. The proof for $p = 2$ may be completed by using the relation between θ' and θ indicated in Lemma 3.

For $b > v$; $p \neq 2$ $\quad 2|b$ and for $x \in \mathcal{O}_T$,

$$H(x) = \mu(1+S(x\Pi^{m/2})+S^{(2)}(x\Pi^{m/2})+N(x\Pi^{m/2})) \cdot (\varphi' \circ S)((\alpha - \alpha_0\delta(\tfrac{\pi}{\Pi})^{b-v})x\Pi^{m/2})$$

For $\mathrm{ord}_{\mathfrak{p}}\, z \geq m/2$, $\quad 2S^{(2)}(z) \equiv -S(z^2) \bmod \mathfrak{y}^{1+b}$.

Also $1 = \mu(1+S(z))\,\varphi'(\alpha S(z))$. Hence

$$H(x) = \mu(1+N(x\Pi^{m/2}))(\overline{\varphi'} \circ S)(\alpha_0\delta(\pi/\Pi)^{b-v}x\Pi^{m/2})\,\mu(1-S(x^2\Pi^{m})/2).$$

The last factor is easily shown to be $\varphi(\alpha'\Pi^{m}x^2/2)$, while with the aid of E.P.(9) the middle factor is $\varphi'(\alpha N(x\Pi^{m/2}))$ (as $(m/2)-(b-v) \geq v''$) and therefore the product of the first two factors in the expression for $H(x)$ is 1 (as $m/2 \geq 1+(b/2)$). This proves the assertion for $b > v$, $p \neq 2$.

For $b > v$; $p = 2$ $\quad 2|v$ and for $x \in \mathcal{O}_T$

$$H(x) = \mu(1+S(x\Pi^{m/2})+N(x\Pi^{m/2}))\varphi(\alpha' x\Pi^{m/2}).$$

As $\mu(1+S(x\Pi^{m/2}))\varphi'(\alpha S(x\Pi^{m/2})) = 1$ and

$\varphi(\alpha x\Pi^{m/2}/B) = \varphi'(\alpha S(x\Pi^{m/2}))$, it follows that

$H(x) = \overline{\varphi}(\alpha_0 N(\delta x\Pi^{v/2}) + \alpha_0 S(\delta x\Pi^{v/2})) = \overline{\varphi}(\alpha_0 W)$, where $1+W = N(1+x\delta\Pi^{v/2})$. Clearly $\mathrm{ord}_{\mathfrak{y}}\, W = v/2$. As $\tau(1+W) = 1$,

$H(x) = \varphi(\alpha_0 W)\,\tau(1+W) = A'(Z)\theta'(\gamma_0 Z)$, where Z is an integer of T which is congruent modulo $\mathfrak{y}$ to $W/\beta_0\Pi^{v/2}$, which is readily found to be congruent to x^2/β'^2. Hence $H(x) = A'(x^2/\beta'^2)\theta'(\gamma_0 x^2/\beta'^2)$ $= A'(x/\beta')\theta'(\gamma_0^{1/2}x/\beta')$. But $\overline{A}'(x) = A'(x)\theta'(x)$, whence the assertion follows for $b > v$, $p = 2$.

If $b = v$, then $m = v$. Again odd and even primes are considered seperately.

For $\begin{matrix} b = v \\ p \neq 2 \end{matrix}$: $2|v$, $\varphi = \varphi'$, $\alpha' = \alpha - \alpha_0\delta$, whence (letting $y = x\pi^{v/2}$)

$$H(x) = \mu(1+S(y)+S^{(2)}(y)+N(y))\ (\varphi \circ S)((\alpha - \alpha_0\delta)y)$$

$$= \mu(1+S(y))\varphi(\alpha S(y))\mu(1+N(y))\ \frac{(\varphi \circ S)(\alpha y^2/2)}{(\varphi \circ S)(\alpha_0 \delta y)}$$

$$= \mu(1+N(y))\ \frac{(\varphi \circ S)(\alpha y^2/2)}{(\varphi \circ S)(\alpha_0 \delta y)}$$

$$= \frac{\mu(1+N(y))(\varphi \circ S)(\alpha y^2/2)}{(\tau \circ N)(1+\delta y)(\varphi \circ S)(\alpha_0 \delta y)}$$

But $\tau(1+S(\delta y)+S^{(2)}(\delta y)+N(\delta y)) = \dfrac{(\bar{\varphi} \circ S)(\alpha_0 \delta y)\ \tau\ (1+N(\delta y))}{\bar{\varphi}(\alpha_0 S(\delta^2\ y^2/2)}$

whence,

$$H(x) = \frac{\mu(1+N(y))(\varphi \circ S)(\alpha y^2/2)}{\tau(1+N(\delta y))\ (\varphi \circ S)(\alpha_0 \delta^2 y^2/2)}\ ,\ \text{while}$$

$$\frac{\mu(1+N(y))\ \ \varphi(\alpha N(y))}{\tau(1+N(\delta y))\ \varphi(\alpha_0 N(\delta y))} = \frac{\varphi(\alpha\pi^v(\frac{1}{2}N(x)^2 + \gamma N(x)))}{\varphi(\alpha_0\pi^v(\frac{1}{2}N(x\delta)^2 + \gamma_0 N(x\delta)))}$$

$= \bar{\theta}'(\frac{1}{2}x^2(\eta^{1/p} - \delta^2\eta_0^{1/p}) + x((\eta\gamma)^{1/p} - (\eta_0\gamma_0)^{1/p}\delta))$ (using the relation between θ' and φ). Furthermore,

$\dfrac{(\varphi \circ S)(\frac{1}{2}\alpha x^2\pi^v)}{(\varphi \circ S)(\frac{1}{2}\alpha_0\delta^2 x^2\pi^v)} = \dfrac{\bar{\theta}'(\frac{1}{2}\eta' x^2\alpha/\alpha')}{\theta'(\frac{1}{2}\eta'\delta^2 x^2\alpha_0/\alpha')}$. These statements together with Lemma 3 yield: $H(x) = \bar{\theta}'(\eta'(\frac{1}{2}x^2 + \gamma' x)$. The assertion then follows from the relation between θ' and θ.

For $\begin{matrix} b = v \\ p = 2 \end{matrix}$: letting $y = x\pi^{v/2}$, it follows from the same procedure as for $b > v$, $p \neq 2$ that

$$N(x) = \mu(1+Ny)\overline{\varphi}(\alpha_0 \delta y/B) = \mu(1+N(y))\overline{\varphi}(\alpha_0 S(\delta y))$$

$$= \frac{\mu(1+N(y))\varphi(\alpha_0 N(\delta y))}{\varphi(\alpha_0 S(\delta y))\varphi(\alpha_0 N(\delta y))}. \text{ But } 1 = (\tau \circ N)(1+\delta y) =$$

$$\tau(1+S(\delta y)+N(\delta y)) = \tau(1+S(\delta y))\tau(1+N(\delta y)) = \overline{\varphi}(\alpha_0 S(\delta y))\tau(1+N(\delta y)).$$

Hence, $$N(x) = \frac{\mu(1+N(y))\varphi(\alpha N(y))}{\tau(1+N(\delta y))\varphi(\alpha_0 N(\delta y))} = \frac{\Delta'(x^2/\beta)\theta'(\gamma x^2/\beta)}{\Delta'(x^2\delta^2/\beta_0)\theta'(\gamma_0 x^2\delta^2/\beta_0)}$$

The assertion follows, using the functional equation of Δ' and the relations between parameters indicated in Lemma 3.

This completes the proof of the lemma. The final parameter to be considered is γ_j which is associated with the character $\mu\tau_j$ $(1 \leq j \leq p-1)$ whenever its conductor is an odd power of y.

Lemma 5

Let β_j be a unit of T such that $\beta_j^\rho \eta_j \equiv 1$. Then for $x \in \mathcal{O}_T$, $1 \leq j \leq p-1$,

$$(\mu\tau_j)(1+x\pi^{v/2})\varphi(\alpha_j x\pi^{v/2}) = \begin{cases} \varphi(\alpha_j\pi^v(\tfrac{1}{2}x^2+\gamma_j x)), & p \neq 2 \\ \Delta'(x/\beta_j)\theta'(\gamma_j x/\beta_j), & p = 2 \end{cases} \quad \text{if } \begin{matrix} b \leq v \\ 2|v \end{matrix}$$

$$(\mu\tau_j)(1+x\pi^{b/2})\varphi'(\alpha_j x\pi^{b/2}) = \begin{cases} \varphi'(\alpha_j\pi^b(\tfrac{1}{2}x^2+\gamma x)), & p \neq 2 \\ \Delta'(x/\beta_j)\theta'(\gamma x/\beta_j), & p = 2 \end{cases} \quad \text{if } \begin{matrix} b > v \\ 2|b \end{matrix}$$

where

$\gamma_j = \gamma_0$ if $b < v$

$\equiv (\delta^\partial\gamma_0 + \delta^\rho\gamma)/(\delta^\partial + \delta^\rho)$ if $b = v$, $2|v$, $p \neq 2$

$\equiv (\gamma_0 + \gamma\delta + \sqrt{\delta})/(\delta+1)$. if $b = v$, $2|v$, $p = 2$.

Proof The proof follows almost directly fom the definitions. For $p = 2$, $b = v$, use is made of the functional equation of Δ'.

<u>Computation of</u> $Q(\chi)$, $b > 0$.

Hav_ing determined the relations between the various parameters, the computation of $Q(\chi)$ may be completed. It is no longer convenient to handle odd and even primes simultaneously.

<u>$p \neq 2$</u> It is our purpose to show that for p odd, $Q(\chi) = 1$. An important step in this direction is taken by showing that $Q(\chi)$ may be computed as though all the conductors have even exponents.

<u>Lemma</u> 6

$$Q(\chi) = \frac{\mu(\alpha)\varphi'(\alpha)}{\chi(\alpha')\Phi(\alpha')} \prod_{j=1}^{p-1} (\tau_j\mu)(\alpha_j)\varphi(\alpha_j) \quad \text{for } b \leq v$$

$$\frac{\mu(\alpha)\varphi'(\alpha)}{\chi(\alpha')\Phi(\alpha')} \prod_{j=1}^{p-1} (\tau_j\mu)(\alpha_j)\varphi'(\alpha_j) \quad \text{for } b \geq v.$$

<u>Proof</u> The assertion is trivial if μ, $\mu\tau_j$, χ, all have conductors with even exponents. This will certainly be the case if both b and v are odd. If $b \geq v$, it is enough if b is odd. Excluding these trivial cases, there remain five situations to be checked individually.

(1) $\left.\begin{array}{l} 1+v \text{ even} \\ 1+b \text{ odd} \\ b < v \end{array}\right\}$ $\quad \dfrac{(\mu,\varphi')}{\mu(\alpha)\varphi'(\alpha)} = \left(\frac{-2\eta}{y}\right)\bar{\varphi}'(\alpha\pi^b\gamma^2/2)\left(\sqrt{\left(\frac{-1}{p}\right)}\right)^f(-1)^{f-1}$

$\mu\tau_j$ has conductor with even exponent

$$\frac{(\chi,\Phi)}{\chi(\alpha')\Phi(\alpha')} = \left(\frac{-2\eta'}{y}\right)\bar{\Phi}(\alpha'\pi^b\gamma'^2/2)\left(\sqrt{\left(\frac{-1}{p}\right)}\right)^f(-1)^{f-1}$$

Hence it is enough to show that $\left(\frac{\eta\eta'}{y}\right)\dfrac{\bar{\varphi}'(\alpha\pi^b\gamma^2/2)}{\bar{\Phi}(\alpha'\pi^b\gamma'^2/2)} = 1$

It follows from Lemma 3 that the Legendre symbol is 1 and the ratio between the two characters is shown to be one by expressing the characters in terms of θ' and using the relations between $\eta\gamma'^2$ and $\eta\gamma^2$.

(2) $\left.\begin{matrix} l+v \text{ odd} \\ l+b \text{ even} \\ b<v \end{matrix}\right\}$ μ, χ have conductors with even exponents.

$$\frac{(\mu\tau_j, \varphi)}{(\mu\tau_j)(\alpha_j)\varphi(\alpha_j)} = \left(\frac{-2\eta_j}{y}\right)\bar{\varphi}(\alpha_j\pi^v\gamma_0^2/2)\left(\sqrt{\left(\frac{-1}{p}\right)}\right)^f(-1)^{f-1}$$

Hence it is enough to show that

$$1 = \prod_{j=1}^{p-1}\left\{\left(\frac{\eta_j}{y}\right)\bar{\varphi}(\alpha_j\pi^v\gamma_0^2/2)\left(\sqrt{\left(\frac{-1}{p}\right)}\right)^f\right\}.$$

But $\prod_{j=1}^{p-1}\eta_j \equiv \eta_0^{p-1}\varsigma^{p(p-1)/2} = -\eta_0^{p-1}$, whence the product of the Legendre symbols involving the prime y, is $\left(\frac{-1}{p}\right)^f$. Furthermore $\left(\frac{-1}{y}\right)\left(\sqrt{\left(\frac{-1}{p}\right)}\right)^{(p-1)f} = \left\{\left(\frac{-1}{p}\right)^{1+(p-1)/2}\right\}^f = 1$ as is easily verified. The product of the terms involving the character φ is 1 as $\sum_{j=1}^{p-1}\alpha_j \equiv 0 \mod y$.

(3) $\left.\begin{matrix} l+v \text{ odd} \\ l+b \text{ odd} \\ b<v \end{matrix}\right\}$ Here all the root numbers have conductors whose exponents are odd. It is easily verified that the "error" factor in this case is just the product of the error factors involved in cases (1) and (2), whence the assertion follows directly. This proves the lemma for $b < v$.

(4) $\begin{matrix} l+b \text{ odd} \\ b > v \end{matrix}$ Here all conductors have odd exponents.

$$\frac{(\mu, \varphi')}{\mu(\alpha)\varphi'(\alpha)} = \left(\frac{-2\eta}{y}\right)\bar{\varphi}'(\alpha\pi^b\gamma^2/2)\left(\sqrt{\left(\frac{-1}{p}\right)}\right)^f(-1)^{f-1}.$$

$$\frac{(\mu\gamma_j,\varphi')}{(\mu\gamma_j)(\alpha_j)\varphi'(\alpha_j)} = \left(\frac{-2\eta_j}{y}\right)\overline{\varphi}'(\alpha_j\pi^b\gamma_j^2/2)\left(\sqrt{\left(\tfrac{-1}{p}\right)}\right)^f(-1)^f$$

$$\frac{(\chi,\Phi)}{\chi(\alpha')\,\Phi(\alpha')} = \left(\frac{-2\eta'}{y}\right)\overline{\Phi}(\alpha'\pi^m\gamma'^2/2)\left(\sqrt{\left(\tfrac{-1}{p}\right)}\right)^f(-1)^{f-1}$$

The product of all these expressions is again shown to be 1 by using the relations between the η parameters to show that the product of all the Legendre symbols (both in p and in y) is 1, and then expressing all the characters in terms of θ' and applying the relations between the γ parameters to the resulting expression.

(5) $b = v$, $1+v$ odd. Here all the conductors have odd exponents. It is easily verified that "error"" factor is the product, YZ, where

$$Z = \left(\frac{\eta\eta'}{y}\right)\left(\sqrt{\left(\tfrac{-1}{p}\right)}\right)^{f(p-1)}\prod_{j=1}^{p-1}\left(\frac{-2\eta_j}{y}\right)$$

$$Y = \frac{\overline{\varphi}(\alpha\pi^v\gamma^2/2)}{\overline{\Phi}(\alpha'\pi^v\gamma'^2/2)}\prod_{j=1}^{p-1}\overline{\varphi}(\alpha_j\pi^v\gamma_j^2/2).$$

The proof is completed by showing that $Z = 1 = Y$.

It has already been noted that $\left(\sqrt{\left(\tfrac{-1}{p}\right)}\right)^{p-1} = \left(\tfrac{-1}{p}\right)$. Certainly $(-2)^{p-1}$ is a square. The relations between the η parameters for $b = v$ give: $\eta\eta' \equiv -\eta_0\delta^{p+1}(\delta^{p-1}-1)/\beta_0$,

$$\prod_{j=1}^{p-1}\eta_j \equiv \eta_0^{p-1}(\delta^{p(p-1)}-1) \equiv \eta_0^{p-1}(\delta^{p-1}-1)^p,$$

and discarding squares the product of the two lines is $-\eta_0^p/\beta_0$. The assertion for Z now follows from $\eta_0\beta_0^p \equiv 1$. Expressing φ and Φ in terms of θ', it is readily seen that $Y = \theta'(W)$, where

$2W = \eta\gamma^2 - \eta'^p\gamma'^{2p} + \Sigma_{j=1}^{p-1} \eta_j \gamma_j^2$. (equality in the sense of the residue class field)

The proof of the lemma is completed by showing that $2W = 0$. It is first noted that $\eta_j/\eta_0 = \zeta^j + \delta^p \neq 0$, whence it follows that δ is not a $(p-1)^{st}$ root of 1. Let $x_j = \eta_j\gamma_j^2/\eta_0$, also let $W' = \Sigma_{j=1}^{p-1} x_j$. Then $x_j = (\zeta^j\gamma_0 + \delta^p\gamma)^2/(\zeta^j + \delta^p)$ and it must be noted that x_j may be obtained from x_1 by replacing ζ with ζ^j.

Furthermore $(\zeta^j+\delta^p)^{-1} = \delta^{-p}(1+(\zeta^j/\delta^p))^{-1} = \delta^{-p} \dfrac{\Sigma_{i=0}^{p-2}(-\zeta/\delta^p)^i}{1-\delta^{p(p-1)(-1)}}$

It follows that $x_1 = \Sigma_{r=0}^{p-2} c_r\zeta^r$, where ζ does not appear explicitly in the formula for c_r, and in particular

$$c_0 = \gamma_0\gamma\delta^p + \frac{\gamma-\gamma_0}{1-\delta^{-p(p-1)}}\left[\gamma\delta^p + \gamma_0\left(\frac{-1}{\delta^p}\right)^{p-2}\right]$$

We may now compute $W' = \Sigma_{j=1}^{p-1}\Sigma_{r=0}^{p-2} c_r\zeta^{rj} = \Sigma_{r=0}^{p-2} c_r \Sigma_{j=1}^{p-1}\zeta^{rj}$. The inner sum is zero unless $\zeta^r = 1$, whence $W' = -c_0$. The remainder of the computation of W is completely straightfoward, using the relations between the η and the γ parameters.

Having established Lemma 6, the treatment is almost completely uniformized by proving!

Lemma 7 Let $t = \delta/\pi^{b-v}$, $Z = -N(t)/t$, then $Q(X) = \varphi(\alpha_0 X)$, where

$$X = S(t)+N(t)\left[\frac{N(1+Z)}{1+N(Z)} - 1\right] + \Sigma_{j=1}^{p-1}\zeta^j\left[\frac{N(t+\zeta^j)}{Nt+\zeta^j} - 1\right]$$

Proof It was shown in lemma 6 that $Q(X) = MA$, where

$$M = \mu\left(\alpha\left(\prod_{j=1}^{p-1}\alpha_j\right)/N\alpha'\right)\prod_{j=1}^{p-1}\tau_j(\alpha_j)$$

$$A = \varphi'(\alpha)\overline{\varphi}(\alpha')\varphi(\Sigma_{j=1}^{p-1}\alpha_j) \qquad \text{if } b \leq v$$
$$\varphi'(\alpha)\overline{\varphi}(\alpha')\varphi'(\Sigma_{j=1}^{p-1}\alpha_j) \qquad \text{if } b \geq v.$$

But $\Sigma_{j=1}^{p-1}\alpha_j = \begin{cases}(p-1)\alpha\pi^{v-b} & \text{if } b \leq v\\ (p-1)\alpha & \text{if } b \geq v.\end{cases}$

Using the relation between φ and φ', it follows that in any case $A = \overline{\varphi}(\alpha')\varphi(p\alpha\pi^{v-b})$. Furthermore

if $b \leq v$, $\varphi(\alpha') = (\varphi \circ S)(\alpha\pi^{v-b} - \delta\alpha_0\pi^{v-b}) = \varphi(p\alpha\pi^{v-b})\overline{\varphi}(\alpha_0 S(\delta\pi^{v-b}))$

if $b \geq v$, $\varphi(\alpha') = (\varphi' \circ S)(\alpha - \alpha_0\delta(\pi/\pi)^{b-v}) = \varphi(p\alpha\pi^{v-b})\overline{\varphi}(\alpha_0 S(\delta\pi^{v-b}))$.

Hence in any case $A = \varphi(\alpha_0 S(t))$, which accounts for one of the terms in the expression for X. The computation of M is somewhat more lenghty. Direct computation shows that $\alpha\left[\prod_{j=1}^{p-1}\alpha_j\right]/N(\alpha') = (1+NZ)/N(1+Z)$, both for $b \geq v$ and for $b \leq v$. Furthermore $\prod_{j=1}^{p-1}\tau_j(\alpha_j) = \prod_{j=1}^{p-1}\tau_j(\alpha_j/\alpha_0)$, as $\prod_{j=1}^{p-1}\tau_j(\alpha_0) = \prod_{j=1}^{p-1}\tau^j(\alpha_0) = \tau(\alpha_0^{(p-1)/2})^p = 1$.

Also $\alpha_j/\alpha_0 = \zeta^j + Nt \qquad \text{if } b \leq v$

$= \pi^{b-v}(\zeta^j + Nt) \quad$ if $b \geq v$. As τ is trivial on the norm group, it follows that

$M = \mu(Z')\prod_{j=1}^{p-1}\tau_j(x_j)$, where $Z' = N(1+Z)/(1+NZ)$

$x_j = N(t+\zeta^j)/(\zeta^j + Nt)$.

With the aid of E.P.(7) it is readily shown that $\text{ord}_y(Z'-1) \geq b''$, whence $\mu(Z') = \overline{\varphi}'(\alpha(Z'-1)) = \overline{\varphi}(\alpha_0 Nt(Z'-1))$. Likewise $\text{ord}_y(x_j - 1) \geq v''$ (Note: v'', b'' are defined in the proof of Lemma 2), whence

$\tau_j(x_j) = \bar{\varphi}(\alpha_0 a_j(x_j-1)) = \bar{\varphi}(\alpha_0 \zeta^j(x_j-1))$ as $a_j \equiv \zeta^j$ mod p. Collecting these results, N may be written entirely in terms of φ and combining this with the expression for A, the lemma is verified.

The treatment of odd primes is completed by:

<u>Lemma</u> 8 $X \in \mathfrak{y}^{1+v}$, and therefore $Q(X) = 1$ if $p \neq 2$.

<u>Proof</u> If $\operatorname{ord}_{\mathfrak{y}} X \geq 1+v$, then the assertion concerning Q follows directly from the previous lemma. In the notation of the previous lemma, $X = S(t) + Nt(Z'-1) + \Sigma_{j=1}^{p-1} \zeta^j(x_j-1)$. We first compute the summation term by the method used in the proof of Lemma 6. The j-th term in the summation may be obtained from the first by substituting ζ^j for ζ, and therefore if the first term, $\zeta(x_1-1)$, is written as a polynomial of degree (p-2) in ζ, then the summation term appearing in the expression for X is the product of (p-1) with the term in the polynomial of zero order. It follows that if $x_1-1 = \Sigma_{r=0}^{p-2} c_r \zeta^r$, then $\Sigma_{j=1}^{p-1} \zeta^j(x_j-1) = c_{p-2}(p-1)$ (where the coefficients, c_r, do not explicitly involve ζ). To determine c_{p-2}, we write $x_1 = N(1+(t/\zeta))/(1+N(t/\zeta)) =$

$(1-N(-t/\zeta)^{p-1})^{-1}(\Sigma_{i=0}^{p-2} N(-t/\zeta)^i)(\Sigma_{j=0}^{p} s^{(j)}(t/\zeta))$ (where $s^{(p)}$ denotes N)

$=(1-Nt^{p-1})^{-1} \Sigma_{i=0}^{p-2} \Sigma_{j=0}^{p} N(-t)^i s^{(j)}(t) \zeta^{-(i+j)}$. The terms involving the $(p-2)^{nd}$ power of ζ are those terms for which either $i+j = 1$ or $i+j = p$. It follows that $c_{p-2} =$

$(1-Nt^{p-1})^{-1}\left\{S(t)-N(t)+\Sigma_{i=0}^{p-2}N(-t)^{i}S^{(p-i)}(t)\right\}$. We now compute

$$Z' N(t) = Nt\, N(1+Z)/(1+NZ) = Nt\, N(1-(Nt/t))/(1-N(Nt/t))$$
$$= N(t-Nt)/(1-Nt^{p-1}) = -Nt^{p}(1-Nt^{p-1})^{-1}N(1-(t/Nt))$$
$$= -Nt^{p}(1-Nt^{p-1})^{-1}\Sigma_{i=0}^{p} S^{(i)}(-t/Nt) = -(1-Nt^{p-1})\Sigma_{i=0}^{p}(-1)^{i}S^{(i)}(t)Nt^{p-i}$$

Combining these results it is found that

$X = p(1-Nt^{p-1})^{-1}\left\{S(t)+\Sigma_{j=1}^{p-2}(-1)^{j}Nt^{j}S^{(p-j)}(t)\right\}$. Using E.P.(5),(6) the lemma is immediately verified for $b \leq v$, as for $b < v$, $t \in \mathcal{P}$ while for $b = v$, $t = \delta$ and it has already been shown that $N\delta$ is not a $(p-1)^{st}$ root of unity. If $b > v$ then t is no longer an integer and therefore $1-Nt^{p-1}$ is not a unit, but the proof may be completed by using the same E.P. to show that both $pS(t)Nt^{1-p}$ and $pNt^{1-j}S^{(j)}(t)$ $(2 \leq j \leq p-1)$ lie in $\mathcal{Y}^{1+v}$.

Having completed the computation of $Q(\chi)$ for odd primes, the even prime may be considered.

<u>$p = 2$</u> It is first shown that a result analagous to Lemma 6 holds.

<u>Lemma</u> 6'. $\dfrac{Q(\chi)}{(\tau,\varphi)} = FE$,

where

$$F = \frac{\mu(\alpha)\varphi'(\alpha)(\mu\tau)(\alpha_1)\varphi(\alpha_1)}{\chi(\alpha')\varphi(\alpha')\ \tau(\alpha_0)\varphi(\alpha_0)} \quad \text{if } b < v$$

$$= \frac{\mu(\alpha)\varphi'(\alpha)(\mu\tau)(\alpha_1)\varphi'(\alpha_1)}{\chi(\alpha')\varphi(\alpha')\ \tau(\alpha_0)\varphi(\alpha_0)} \quad \text{if } b \geq v.$$

$E = 1$ if either $b < v$, or $(1+b)$ even

$= \theta'(\gamma)\, i^{f}$ if $b>v$, $(1+b)$ odd

$= \theta'(\gamma, \delta/(1+\delta))\Delta'(\delta/(1+\delta))$ if $b=v$, $1+b$ odd.

Proof Let $E' = Q(\chi)\,(\tau,\varphi)^{-1}\,F^{-1}$.

a) For $b < v$, E' is trivially 1 if both $1+b$ and $1+v$ are even, $\Delta'(\gamma)\,\Delta'(\gamma')$ if $\begin{smallmatrix}1+v \text{ even,}\\ 1+b \text{ odd}\end{smallmatrix}$ $\Delta'(\gamma_1)\,\Delta'(\gamma_0)$ if $\begin{smallmatrix}1+v \text{ odd}\\ 1+b \text{ even}\end{smallmatrix}$, and is the product of these ratios if both $1+b$ and $1+v$ are odd. But for $b < v$, $\gamma_1 \equiv \gamma_0$, $\gamma'^2 \equiv \gamma$, and in any case $\Delta'(x^2) = \Delta'(x)$ if x lies in the residue class field. Hence $E' = 1$ if $b < v$.

b) For $b > v$, $\gamma_1 \equiv \gamma$, $\gamma'^2 \equiv 1 + \gamma_0$, $1+v$ even $\Leftrightarrow$ $1+m$ even, $1+b$ even $\Rightarrow$ conductor of $\mu\tau$ has even exponent. Hence

$E' = 1$ - - - - - - - - - - - - - - - - if $1+v$ and $1+b$ are even

$= \Delta'(\gamma)\Delta'(\gamma_1)\left(\frac{1-i}{\sqrt{2}}\right)^{2f}$ if $1+v$ is even and $1+b$ is odd.

$= \overline{\Delta}'(\gamma')\overline{\Delta}'(\gamma_0)\left(\frac{1+i}{\sqrt{2}}\right)^{2f}$ if $1+v$ is odd and $1+b$ is even.

= product of the two previous lines if both $1+v$ and $1+b$ are odd

The assertion follows directly from the functional equation and the fact that $\Delta'(1) = i^f = \left(\frac{1+i}{\sqrt{2}}\right)^{2f}$.

c) For $b = v$, we may assume that v is even. Using equality in the sense of residue class fields, $\gamma'^2 = (1+\delta)^{-1}(\gamma + \gamma_0\delta + \delta + \sqrt{\delta})$, $\gamma_1 = (1+\delta)^{-1}(\gamma_0 + \gamma\delta + \sqrt{\delta})$, whence $\gamma_1 + \gamma'^2 = \gamma + \gamma_0 + \delta(1+\delta)^{-1}$, which may be written: $\delta(1+\delta)^{-1} + \gamma + \gamma_1 = \gamma_0 + \gamma'^2$. Using the functional equation it follows that

$E'\Delta'(\delta/(1+\delta)) = \Delta'(\gamma)\Delta'(\gamma_1)\Delta'(\delta/(1+\delta))/[\Delta'(\gamma_0)\Delta'(\gamma')]$

$= \Theta'(W + \delta(1+\delta)^{-1}\gamma_1)$, where $W = \gamma_0\gamma'^2 + \gamma\gamma_1 + \gamma\delta(1+\delta)^{-1}$. Straightforward manipulation shows that $W = x + x^2$, where $x = \dfrac{(\gamma_0 + \gamma)(\delta + \sqrt{\delta})}{1+\delta}$ and therefore $\Theta'(W) = 1$. The assertion follows directly.

Corresponding to Lemma 7, valid for p odd, we now have:

Lemma 7'

$$\frac{Q(X)}{(\tau,\varphi)} = \varphi(\alpha_0 X)\,\sigma,$$

where

$$X = S(t)+xN(t)+y \qquad 1+x = N(1+Z)/(1+NZ)$$
$$t = \delta\pi^{v-b} \qquad 1+y = N(1+t)/(1+Nt)$$
$$Z = Nt/t \qquad x' = x/(\beta\pi^{b/2})$$
$$y' = y/(\beta_0\pi^{v/2})$$

$$\sigma = 1 \qquad \text{if either } b < v \text{ or } 1+b \text{ even}$$
$$= i^f\theta'(\gamma)\bar{\Delta}'(x')\theta'(\gamma x') \qquad \text{if } b > v \text{ and } 1+b \text{ odd}$$
$$= \theta'(\gamma_1\delta/(1+\delta))\Delta'(\delta/(1+\delta))\Delta'(x')\theta'(\gamma x')\Delta'(y')\theta'(\gamma_0 y') \text{ if } b = v \text{ and } 1+b \text{ odd.}$$

Proof

Repeating the first part of the proof of Lemma 7 with very minor modifications, it is found that in the notation of Lemma 6' $F = \varphi(\alpha_0 S(t))\bar{\mu}(1+x)\bar{\tau}(1+y)$. It follows from our usual methods of estimation that

$$\text{ord } x \geq b'' \quad \text{if either } b < v \text{ or } 1+b \text{ even}$$
$$\geq b/2 \quad \text{if both } b \geq v \text{ and } 1+b \text{ odd}$$

$$\text{ord } y \geq v'' \quad \text{if either } b \neq v \text{ or } 1+v \text{ even}$$
$$\geq v/2 \quad \text{if both } b = v \text{ and } 1+v \text{ odd.}$$

The estimates cannot be improved and therefore it is not always possible to express F in terms of the additive character. However for 1+b odd we do have $\mu(1+x)\varphi'(\alpha x) = \Delta'(x')\theta'(\gamma x')$, while for 1+v odd $\tau(1+y)\varphi(\alpha_0 y) = \Delta'(y')\theta'(\gamma_0 y')$, the left side of the first relation being 1 if $b < v$, the same being true for the second relation if $b \neq v$. The lemma now follows with the aid of Lemma 6'.

The computation is finally completed with:

Lemma 8'
$\varphi(\alpha_0 X)\ \sigma = 1$, and therefore $Q(\chi) = (\tau, \varphi)$.

Proof. $1+x = N(1+Z)/(1+NZ) = N(1-t^{-1}Nt)/(1+Nt) =$
$N(t^{-1}Nt)N(1-t/Nt)/(1+Nt) = (1-S(t/Nt)+Nt^{-1})Nt/(1+Nt)$, whence
$x = -S(t)/(1+Nt)$. Likewise $1+y = N(1+t)/(1+Nt) =$
$(1+S(t)+N(t))/(1+Nt)$, whence $y = S(t)/(1+Nt)$, and therefore
$X = 2S(t)/(1+Nt)$. It follows from the usual estimates that

$$\begin{aligned} \text{ord } X &\geq 1+v \quad \text{if either } b \neq v \text{ or } (1+v) \text{ even} \\ &\geq v \quad \text{if } b = v. \end{aligned}$$

As the conductor of φ has exponent $1+v$, it follows that (as $X = -2x$)

$$\begin{aligned} \varphi(\alpha_0 X)\ \sigma &= 1 && \text{if } b < v \text{ or } 1+b \text{ even} \\ &= i^f \theta'(\gamma)\overline{\Delta}'(x')\theta'(\gamma x') && \text{if } b > v \text{ and } 1+b \text{ odd.} \\ &= \sigma\ \theta'(\eta\, 2x/\pi^v) && \text{if } b = v \text{ and } 1+v \text{ odd.} \end{aligned}$$

For $\left.\begin{matrix} b > v \\ 1+b \text{ odd} \end{matrix}\right\}$ We know that in any case $x = -S(t)/(1+Nt)$,
$t = \delta\Pi^{v-b}$, whence
$x/\pi^{b/2} = -(1+\pi^{b-v}N(\delta^{-1}))^{-1}\, S(\delta(\frac{\pi}{\Pi^2})^{b/2}\Pi^v)/N(\delta(\pi/\Pi^2)^{b/2}\Pi^v)$ and
it follows from E.P.(10) that this is a unit congruent to β_0/δ.
Hence (Lemma 3) $x' = 1$ and the proof is immediate.

For $\left.\begin{matrix} b = v \\ 1+v \text{ odd.} \end{matrix}\right\}$ Here $t = \delta$. Let $w = (\pi/\Pi^2)^{v/2}\Pi^v$, then
$2/\pi^{v/2} = S(w)/N(w)$, $S(t)\pi^{-v/2}(1+N\delta)^{-1} = (N\delta^{-1}+1)^{-1}S(\delta w)/N(\delta w)$.
Using E.P.(10) and the relations between the η parameters, it
follows that (again using equality in the sense of elements of

the residue class field) $x' = \delta^2/(1+\delta^2)$, $\eta_0 2S(t)\pi^{-v}(1+Ht)^{-1} =$ $\delta/(1+\delta^2) = y'$. Consequently,

$\varphi(\alpha_0 X)\ \sigma = \Delta'(\delta/(1+\delta))\overline{\Delta}'(\delta^2/(1+\delta^2))\overline{\Delta}'(\delta/(1+\delta^2))\ \theta'(a_1)$, where

$$a_1 = \gamma_1\delta/(1+\delta) + \gamma\delta^2/(1+\delta^2) + \gamma_0\delta/(1+\delta^2) + \delta/(1+\delta^2).$$

But $\Delta'(\delta^2/(1+\delta^2))\Delta'(\delta/(1+\delta^2)) = \Delta'((\delta+\delta^2)/(1+\delta^2))\ \theta'(\delta^3/(1+\delta^4))$, and $(\delta+\delta^2)/(1+\delta^2) = \delta/(1+\delta)$, whence

$\varphi(\alpha_0 X)\ \sigma = \theta'(a_2)$, where $a_2 = a_1 + \delta^3/(1+\delta^4) =$ (upon substituting the expression for γ_1 in terms of γ, γ_0 and δ and simplifying)

$\delta(1+\delta)^{-1}\{(1+\sqrt{\delta})(1+\delta)^{-1} + \delta^2/(1+\delta^3)\} = a_3 + \delta(1+\sqrt{\delta})/(1+\delta)^2$,

where $a_3 = \delta^3/(1+\delta^2)^2$ which has the same image under θ' as its square root. Hence $\theta'(a_2) = \theta'(a_4)$, where

$a_4 = \delta\sqrt{\delta}/(1+\delta^2) + \delta(1+\sqrt{\delta})/(1+\delta^2) = \delta/(1+\delta^2) = ((\delta-1)+1)/(\delta-1)^2$

$= C + C^2$, where $C = (\delta-1)^{-1}$. As the image of C under θ' is the same as that of C^2, it follows that $\theta'(a_4) = 1$. This completes the proof of the lemma.

<u>Summary</u>

k a $\mathfrak{y}$-adic number field, absolute degree of $\mathfrak{y} = f$ absolute different of $k = \mathfrak{y}^d$. K is a cyclic extension of k of degree n, n prime. τ is a non trivial character of k^* which is trivial on the norm group. ψ is the standard additive character of k. If χ is a character of K^* of conductor $\mathfrak{P}^{1+m}$, which is trivial on K_N^* then

(1) For K/k unramified, $Q_{K/k}(\chi) = (-1)^{d(n-1)}$ (valid for n not prime)

(2) For K/k ramified, let π be a prime element of k which lies in the norm group. Then

(a) if $\mathcal{Y} \nmid n$

$$Q_{K/k}(\chi) = (\tau, \psi_{\pi^{-d-1}}) = (-1)^{f-1}\left(\sqrt{\left(\left(\frac{-1}{p}\right)\right)}\right)^{f}\left(\frac{PS_{k/T}(\pi^{-d-1})}{\mathcal{Y}}\right) \quad \text{if } n = 2$$

$$= 1 \quad \text{if } m = 0 \text{ or } -1 \quad \text{for } n \neq 2$$

$$= \left(\frac{N\mathfrak{p}}{n}\right)^{1+m} \quad \text{if } m > 0 \quad \text{for } n \neq 2$$

(b) if $\mathcal{Y} \mid n$

$$Q_{K/k}(\chi) = 1 \quad \text{if } n \neq 2$$

$$= (\tau, \psi_{\pi^{-d-1}}) \quad \text{if } n = 2$$

These results are now extended to the case in which K k is abelian.