

On the Root Number in the Functional Equation of the Artin-

Weil L-series.

38.318 C by Bernard H. Dwork.

780 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 $\sigma_1, \dots, \sigma_n$ 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 $\sigma_1, \dots, \sigma_n$ 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

JUL 19 1954 KM

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, $L(s, \chi, K/k)$, 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, G_k the group of idele classes, D_k the connected component of the unit element in G_k . The abelian L -series may be described as an Euler product over the primes of k involving a character of the factor group G_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 G_k/D_k to L -series with characters of G_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 G_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. "Über eine neue Art von Zetafunktionen 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 in the L-series of Weil (6), constructed with characters of the Weil group, the group extension of G_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. "Über 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 théorie du Corps de Classes" J. Math. Soc. of Japan, vol.3, (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 formulas 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 Zahlkörper", Journal für 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 subsequent theory.

I wish to express my gratitude 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 γ -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 procedure 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 γ . 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 $\mathcal{D}_{E/F}$, for $A_K \supset E \supset F \supset A_t$, E/A_t finite, may be defined in the usual way and in this connection the relative discriminant, $D_{E/F}$, is simply defined to be $N_{E/F} \mathcal{D}_{E/F}$. 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 $r_\circ(\chi, E/F) = \mathcal{O}^r$, \mathcal{O} being the prime of F and

$$r = [W_\circ]^{-1} \sum_{i=0} \sum_{x \in W_i} (\chi(1) - \chi(x))$$

where \mathcal{H}_0 is the inertial subgroup of $G(E/F)$ (i.e. the whole group) and \mathcal{H}_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 $F \subset A_t, E'/F'$ 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 $\text{ord}_{\mathcal{H}_i} f(\chi', E'/F') = \text{ord}_{\mathcal{H}_i} f_0(\chi, E/F)$, where \mathcal{H}_i 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 $f_0(\chi + \chi', E/F) =$

$$f_0(\chi, E/F) f_0(\chi', E/F).$$

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

$$f_0(\chi', L/F) = f_0(\chi, E/F).$$

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

$$f_0(\chi_\psi, E/F) = D_{L/F}^{\psi(1)} N_{L/F} f_0(\psi, E/L).$$

4. $f_0(\chi, E/F)$ is an integral power of \mathcal{O} .

These are the only properties of the conductors f_0 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 \mathcal{O}^r , where $r = \text{ord}_{P_t} f_0(\chi_L, L/A_t)$.

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 $\text{ord}_{\mathcal{O}} F(\chi, K/k) = \text{ord}_{P_t} f_0(\chi_{L'}, L'/A_t)$.

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_0 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, H , of k . Then $L = HA_t$ is the extension of A_t determined by the kernel of χ in H and by the arguments appearing in the construction, if χ_H is the character of $G(H/k)$ obtained by passage to quotients, then $f(\chi_H, H/k) = F(\chi, K/k)$. 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

Induced Character Theorem

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

Proof

Let: \mathfrak{p} be the prime of K , \mathfrak{p}' that of Ω , \mathfrak{p}'' 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

I, \bar{I}, I' be the inertial subgroups of $G(K/k)$, $G(K/\Omega)$ resp.

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

$\{\alpha_i\}$ be a set of representatives of right cosets of $\bar{7}$ in 7
 H be the inertial subgroup of $W_{K/k}$

Then $7 = \bigcup_{i=1}^{e'} \bar{7} \alpha_i$ whence $G(K/k) = \bigcup_{j=0}^{f'-1} 7 \tau^j = \bigcup_{n=0, s=0}^{\bar{f}-1, f'-1} 7 \tau^{f'n} \tau^s$
 As the Frobenius class of $G(K/\Omega)$ is $7 \tau^{f'} \cap G(K/\Omega)$, if we pick $\bar{\tau}$ in this class then there exists $\alpha \in 7$ such that $\tau^{f'} = \alpha \bar{\tau}$,
 whence $G(K/k) = \bigcup_{n=0, s=0}^{\bar{f}-1, f'-1} 7 (\alpha \bar{\tau})^n \tau^s$
 $= \bigcup_{n, s} 7 \tau^s$
 $= \bigcup_{n=0, s=0, l=1}^{\bar{f}-1, f'-1, e'}$ $\bar{\tau}^n \bar{7} \alpha_l \tau^s$
 $= \bigcup_{s=0, l=1}^{f'-1, e'}$ $G(K/\Omega) \alpha_l \tau^s$

Letting s_i be a representative in H of α_i ($1 \leq i \leq e'$)
 t be a representative of τ .

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

$\chi(x) = \sum_{j=0, l=1}^{f'-1, e'}$ $\psi(s_l t^j x t^{-j} s_l^{-1})$, where as usual $\psi(x)=0$ for x not in $W_{K/\Omega}$

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

7_j be the inertial subgroup of $G(K/\Omega_j)$

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

Then $\beta \mapsto \tau^{-j} \beta \tau^j$ is an isomorphism of $G(K/\Omega)$ onto $G(K/\Omega_j)$ and

$7_j = \tau^{-j} 7 \tau^j, H_j = t^{-j} H_0 t^j$

$7 = \bigcup_{i=1}^{e'} 7 \alpha_i = \bigcup_{i=1}^{e'} (\tau^{-j} 7 \tau^j) (\tau^{-j} \alpha_i \tau^j) = \bigcup_{i=1}^{e'} 7_j (\tau^{-j} \alpha_i \tau^j)$

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 $x \mapsto \psi_0(t^j x t^{-j})$

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

$$\begin{aligned} \chi_j(x) &= \sum_{i=1}^{e^f} \psi_j(t^{-j} s_i t^{jxt^{-j} s_i^{-1} t^j}) \\ &= \sum_{i=1}^{e^f} \psi_j(s_i t^{jxt^{-j} s_i^{-1}}), \text{ where } \psi_j \text{ is taken to be zero outside of } \bar{H}_0. \end{aligned}$$

Let χ' be the restriction of χ to H . For $x \in H$, we have: $s_i t^{jxt^{-j} s_i^{-1}} \in W_{K/\Omega} \iff s_i t^{jxt^{-j} s_i^{-1}} \in W_{K/\Omega} \cap H = \bar{H}_0$. It follows

that $\chi' = \sum_{j=0}^{f^i-1} \chi_j$.

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 ($0 \leq j \leq f^i-1$).

Let U^i be $G(A_K/L)$ (and its replica in H).

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

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

Proof Let $G = \bigcup_{j=1}^m \beta_j$, a disjoint union, then for $x \in G$

$$\chi(x) = \sum_{j=1}^m \psi(\beta_j x \beta_j^{-1})$$

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 $\chi(x) = n \psi(1) \Leftrightarrow x \in \bigcap_{j=1}^m \beta_j^{-1} H^* \beta_j$, 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 $\tilde{\beta}_j$ be the image of β_j in \tilde{G} , then $(G^*H) = (\tilde{G}^*\tilde{H})$, and therefore $\tilde{G} = \bigcup_{j=1}^m \tilde{H} \tilde{\beta}_j$, a disjoint union. For $\tilde{x} \in \tilde{G}$, let x be a representative in G , then $\tilde{\chi}(\tilde{x}) = \sum_{j=1}^m \psi(\beta_j x \beta_j^{-1}) = \sum \psi(\tilde{\beta}_j \tilde{x} \tilde{\beta}_j^{-1})$ whence $\tilde{\chi}$ is induced by $\tilde{\psi}$, which completes the proof of the lemma.

Continuing with the proof of the theorem,

$$\begin{aligned} \text{ord}_y F(\chi, K/k) &= \text{ord}_{P_t} f_0(\tilde{\chi}, L/A_t), \text{ while } f_0(\tilde{\chi}, L/A_t) = \\ &= \prod_{j=0}^{f-1} f_0(\tilde{\chi}_j, L/A_t) = \prod_{j=0}^{f-1} \left\{ D_{\Omega_j A_t / A_t}^{\psi_j(1)} \prod_{\Omega_j A_t / A_t} f_0(\tilde{\psi}_j, L/\Omega_j A_t) \right\} \\ &= \left(\prod_{j=0}^{f-1} D_{\Omega_j A_t / A_t} \right) \psi(1) \prod_{j=0}^{f-1} \prod_{\Omega_j A_t / A_t} f_0(\tilde{\psi}_j, L/\Omega_j A_t). \end{aligned}$$

To complete the proof we must show

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

Proof of (a) :

$\text{ord}_y \prod_{\Omega/k} F(\psi, K/\Omega) = f^i \text{ord}_y F(\psi, K/\Omega)$. As $\Omega_j A_t$ is inertial subfield of A_t/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 $\text{ord}_y F(\psi, K/\Omega) = \text{ord}_{P_{\Omega_0}} f_0(\psi_0, L/\Omega_0 A_t)$. Hence it is enough to show that

$\text{ord}_{\mathfrak{P}_j} f_0(\check{\psi}_j \circ L/A_t \Omega_j)$ is independent of j . But this is clear as \bar{H}_0 and \bar{H}_j are related by an inner isomorphism of Π 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 $\check{\psi}_0 \circ \check{\psi}_j$ (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):

$$D_{\Omega_j A_t / A_t} = N_{\Omega_j A_t / A_t} [\mathcal{G}_{KA_t / A_t} \mathcal{G}_{KA_t / \Omega_j A_t}] = \eta^j \cdot r \text{ independent}$$

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 $D_{\Omega/k} = N_{\Omega/k} \mathcal{G}_{\Omega/k} \Rightarrow \text{ord}_{\mathfrak{P}_j} D_{\Omega/k} = f^j \text{ord}_{\mathfrak{P}_j} \mathcal{G}_{\Omega/k}$. Hence it is enough to show that $\text{ord}_{\mathfrak{P}_0} \mathcal{G}_{\Omega A_t / A_t}$

$= \text{ord}_{\mathfrak{P}_j} \mathcal{G}_{\Omega/k}$. Letting T be the inertial subfield of K/k , and

η^j be the prime of ΩT , we have $\mathcal{G}_{\Omega T / \Omega} \mathcal{G}_{\Omega/k} = \mathcal{G}_{\Omega T/k} = \mathcal{G}_{\Omega T/T} \mathcal{G}_{T/k}$ whence $\text{ord}_{\mathfrak{P}_j} \mathcal{G}_{\Omega/k} = \text{ord}_{\mathfrak{P}_j} \mathcal{G}_{\Omega T/T}$

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

$$\mathcal{G}_{\Omega A_t / A_t} = \frac{\mathcal{G}_{KA_t / A_t}}{\mathcal{G}_{KA_t / \Omega A_t}}, \quad \mathcal{G}_{\Omega T/T} = \mathcal{G}_{K/T} / \mathcal{G}_{K/\Omega T}$$

This completes the proof of the theorem.

The treatment of the local theory is completed with:

Lemma

Let $K > L > k$, K and L normal over k , τ the topological homomorphism of $W_{K/k}$ onto $W_{L/k}$ with kernel $W_{K/L}^c$ which extends the transfer homomorphism $\tau: W_{K/L} \rightarrow W_{L/k}$. 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, $H \supseteq W_{K/L}^c$, the closure of the commutator subgroup of $W_{K/k}$. Hence $\tilde{\tau}(H) = H$. It follows that if \bar{H}^* is the kernel of ψ in \bar{H} then $\tilde{\tau}(\bar{H}^*) = H^*$, the kernel of $\psi \circ \tau$ in H . If as above, A_L is the inertial subfield of A_K/k , then A_L/k is certainly abelian, whence $A_L^c \subset A_K^c \subset A_L$. Therefore the inertial subfield of A_L/k is $A_L \cap A_K^c = A_L^c$. Identifying H with $G(A_K/A_L^c)$, \bar{H} with $G(A_L/A_L^c)$, the kernel of τ is $G(A_K/A_L)$. Hence if \bar{H}^* determines an extension, E , of A_L in A_K , then \bar{H}^* is identified with $G(A_L/E)$ and $H^* = \tilde{\tau}(\bar{H}^*)$ is identified with $G(A_K/E)$. Furthermore if $\sigma \in G(A_K/A_L^c)$ 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 $G(E/A_L^c)$ obtained from ψ and $\psi \circ \tau$ by passage to quotients are identical. Thus, $\text{ord}_y F(\psi, L/k) = \text{ord}_{P_L} f_0(\psi_{E^*} E/A_L^c) = \text{ord}_y F(\psi \circ \tau, K/k)$.

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 γ -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 γ^{1+s_j} ($1 \leq j \leq n$), f is the relative residue class degree and f_a is the absolute degree of γ . Let \mathfrak{p} be the prime of K and $g_{K/k}$ (or more simply, g) a mapping of integers into rationals defined by:

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

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, \dots, 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 $\Pi_{K/k}$ in K^* , and χ is the character of $W_{K/k}$ induced by λ then there exist characters μ of k^* such that $\lambda = \mu \circ \Pi_{K/k}$ and for any such μ , $\chi = \sum_{j=1}^n (\mu \tau_j) \circ \mathcal{N}_{W_{K/k} \rightarrow K^*}$. (The last symbol denotes the transfer homomorphism)

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

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

$$\chi(x) = \begin{cases} 0 & \text{for } x \notin K^* \\ = n\lambda(x) & \text{for } x \in K^* \end{cases} \text{ for if } (s_\alpha)_{\alpha \in G(K/k)} \text{ are a set}$$

of representatives of $G(K/k)$ in $W_{K/k}$ then for $x \in W_{K/k}$

$$\chi(x) = \sum_{\alpha \in G(K/k)} \lambda(s_\alpha x s_\alpha^{-1}), \text{ where } \lambda(x) = 0 \text{ for } x \notin K^*, \text{ whence}$$

$\chi(x) = n\lambda(x)$ for $x \in K^*$, while for $x \notin K$, $s_\alpha x s_\alpha^{-1} \notin K^*$ and there-

fore $\chi(x) = 0$. On the other hand $x \mapsto \mathcal{H}(x) \bmod N_{K/k} K^*$ is a

homomorphism of $W_{K/k}$ onto $K^*/N_{K/k} K^*$, whence the kernel is of in-

dex n . K^* lies in the kernel and is of index n and therefore is

the kernel. Hence $\mathcal{H}(x) \in N_{K/k} K^* \iff x \in K^*$. Now,

$$\sum_{j=1}^n (\mu \tau_j) \circ \mathcal{H}(x) = [(\mu \circ \mathcal{H})(x)] \sum_{j=1}^n (\tau_j \circ \mathcal{H})(x).$$

The sum is zero for $\mathcal{H}(x) \notin N_{K/k} K^*$, 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.

Definition 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 φ^{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.

Lemma 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 φ^{1+m} , then there exists a character μ of k^* of conductor γ^{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. $b = \min_{1 \leq j \leq n} \text{ord}_y F(\mu\tau_j, k/k)$, where $\mu \circ N_{K/k} = \lambda$.

Proof 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 preceding lemma, χ , the character of $N_{K/k}$ induced by λ is $\sum_{j=1}^n (\mu\tau_j) \circ \mathcal{N}$, whence by the properties of the conductor:

$$\begin{aligned} \prod_{j=1}^n F(\mu\tau_j, k/k) &= \prod_{j=1}^n F((\mu\tau_j) \circ \mathcal{N}, k/k) = F(\chi, k/k) \\ &= D_{K/k}^{\lambda(d)} N_{K/k} F(\lambda, K/K). \end{aligned}$$

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

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

We now compute this last expression. If μ_1, μ_2 are characters of k^* and have conductors y^{1+c}, y^{1+d} , respectively, then the conductor of $(\mu_1\mu_2)$ divides $y^{1+\max(c,d)}$ and if $c \neq d$ then the conductor of $\mu_1\mu_2$ is $y^{1+\max(c,d)}$. For suppose $c < d$ then μ_1 and μ_2 are both trivial on $1+y^{1+d}$, but μ_1 is trivial on $1+y^d$ while μ_2 is not, whence $\mu_1\mu_2$ not trivial on $1+y^d$, and therefore conductor $(\mu_1\mu_2) = y^{1+d}$. On the other hand if $c=d$ then $\mu_1\mu_2$ is certainly trivial on $1+y^{1+\max(c,d)}$, which proves

the assertion. Applying this simple result to the characters $\mu \chi_j$, we have, letting the conductor of μ be γ^{1+b} ,

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

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

$$\gamma^{f(1+m)} = \prod_{b < s_j} \frac{\gamma^{1+s_j}}{\gamma^{1+s_j}} \prod_{b > s_j} \frac{\gamma^{1+b}}{\gamma^{1+s_j}};$$

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 .

Corollary

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

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

Proof

1. The first part of this statement follows from the fact that if $\lambda = \mu \cdot \prod_{K/k}$ has conductor γ^{1+m} , then $m = g(b')$, where $b' = \min_{1 \leq j \leq n} \text{ord}_\gamma F(\mu \chi_j, k/k)$, whence $b' \leq b$. For the second part of the first statement, if $b' = b$ we are through. If $b' < b$, let μ' be a character of k^* of conductor $\gamma^{1+b'}$ such that $\lambda =$

$\mu \circ \mathbb{N}_{K/k}$. 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 $b = s_j > b^0$. If $b = -1$ or if b not one of the elements (s_1, \dots, 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, \dots, s_n) . From the above lemma $g(b)$ not admissible \Leftrightarrow given a character, μ , of K^* , trivial on $1+y^{1+b}$, there exists τ_j (depending on μ) such that $\mu \tau_j$ is trivial on $1+y^b$. Hence if $g(b)$ not admissible and $x \in (1+y^b) \cap \mathbb{N}_{K/k} K^*$, $x \notin 1+y^{1+b}$ then there exists θ , a character on K^* trivial on $1+y^{1+b}$ 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 admissible $\Rightarrow (1+y^b) \cap \mathbb{N}_{K/k} K^* \subset 1+y^{1+b}$. Conversely if

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

$$(1+y^t) \cap \mathbb{N}_{K/k} K^* \subset 1+y^{1+t} \Rightarrow t \text{ lies in the set } (s_1, \dots, s_n).$$

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

The main consequence of this theory is: (Let $1 + \mathcal{Y}^0 = U_K$, $1 + \mathcal{Z}^0 = U_{K^*}$, designate $N_{K/k}$ simply by N).

Theorem For $b \geq 0$,

$$1. N(1 + \mathcal{Z}^{1+g(b)}) = (1 + \mathcal{Y}^{1+b}) \cap N K^*$$

$$2. N(1 + \mathcal{Z}^{g(b+1)}) = (1 + \mathcal{Y}^{1+b}) \cap N K^*$$

$$3. g(b) \text{ admissible with respect to } K/k \Leftrightarrow N(1 + \mathcal{Z}^{g(b)}) \neq 1 + \mathcal{Y}^{1+b}.$$

Proof

We first note that if 2. is true then $N(1 + \mathcal{Z}^{g(b)}) = (1 + \mathcal{Y}^b) \cap N K^*$, 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

$$\chi(a) = 1. \text{ (In this lemma we do not insist that characters be continuous).}$$

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 (1). In either case the conditions are satisfied.

We now return to the proof of the theorem. $b \geq 0 \Rightarrow g(b) \geq 0$
 $\Rightarrow 1 + \varphi^{1+g(b)} \subset 1 + \varphi \Rightarrow N(1 + \varphi^{1+g(b)}) \subset 1 + \varphi$. Let $a \in 1 + \varphi$,
 $a \notin 1 + \varphi^{1+b}$, then by the above there exists a character μ of
 K^* such that $\mu(a) \neq 1$, conductor of $\mu = \varphi^{1+b}$. Then by the above
 corollary $\lambda = \mu \circ N$ has conductor $\varphi^{1+g(b')}$, $b' \leq b$, whence
 μ is trivial on $N(1 + \varphi^{1+g(b')}) \supset N(1 + \varphi^{1+g(b)})$. But $\mu(a)$
 not one, hence $a \notin N(1 + \varphi^{1+g(b)})$. Hence $N(1 + \varphi^{1+g(b)}) \subset$
 $1 + \varphi^{1+b}$. To prove inclusion in the other direction, let
 $a \in (1 + \varphi^{1+b}) \cap N K^*$. Then $a = Nz$, $z \in K^*$. We assert that

$z \in K_N^*(1 + \varphi^{1+g(b)})$. Let λ be any character of K^* which is triv-
 ial on $K_N^*(1 + \varphi^{1+g(b)})$ then $\lambda = \mu \circ N$ for some character, μ ,
 of K^* with the property that $F(\mu, k/k)$ divides $F(\mu \varphi^j, k/k)$ for
 all j between one and π . Let $\varphi^{1+b'}$ be the conductor of μ then
 the conductor of λ is $\varphi^{1+g(b')} \Rightarrow g(b) \geq g(b') \Rightarrow b \geq b'$
 $\Rightarrow \mu$ trivial on $1 + \varphi^{1+b'} \supset 1 + \varphi^{1+b} \ni a \Rightarrow \mu(a) = 1 \Rightarrow$
 $\lambda(z) = (\mu \circ N)(z) = 1$. This proves the assertion concerning z ,
 whence $a \in N(1 + \varphi^{1+g(b)})$. 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 φ^r . If a
 character, λ , of K^* is trivial on $K_N^*(1 + \varphi^r)$ then certainly the
 conductor of λ divides φ^r , whence from the description of ad-
 missible integers, the conductor of λ divides $\varphi^{1+g(b)}$, i.e.

every character trivial on $(1 + \mathfrak{p}^x)K_{\mathbb{N}}^*$ is trivial on $1 + \mathfrak{p}^{1+g(b)} \Rightarrow$
 $(1 + \mathfrak{p}^x)K_{\mathbb{N}}^* \supset (1 + \mathfrak{p}^{1+g(b)})K_{\mathbb{N}}^*$. Inverse conclusion is trivial and
 therefore $N(1 + \mathfrak{p}^x) = N(1 + \mathfrak{p}^{1+g(b)}) = \mathbb{N}K^* \cap (1 + \mathfrak{p}^{1+b})$, which
 proves 2. and in addition: $(1 + \mathfrak{p}^{g(b+1)})K_{\mathbb{N}}^* \supset 1 + \mathfrak{p}^{1+g(b)}$.

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

$$(Ny^n)^{-\frac{1}{2}} \sum_{x \in U/(1+y^n)} \chi(x) \psi(x),$$

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 y^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 χ_α be the character of k^* : $x \rightarrow \chi(\alpha x)$. If $\alpha \in U$ then trivially, χ_α is also a character of conductor y^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 $\bar{\psi} = \psi$, 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: $(-1)^{r-1} (\chi \cdot N_{K/k}, \psi \circ S_{K/k}) = (\chi, \psi)^r$.

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.

Theorem 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:

$$\bar{\psi}(\alpha z) = \chi(1+z) \text{ for all } z \in \mathfrak{y}^r. \text{ For } \alpha \text{ so chosen,}$$

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

Proof

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 $z \rightarrow \chi(1+z)$ is a character of the additive group \mathfrak{y}^r , and therefore is the restriction to \mathfrak{y}^r 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 $x \rightarrow \chi(1+x)$ on 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 y^r follows from the fact that if ψ_β is trivial on y^r then $\beta y^r \subset y^{2r}$, whence $\beta \in y^r$. 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 $1+y^r$ and w through a set of representatives of y^r modulo y^{2r} , $z+w$ runs through a set of representatives of the distinct residue classes of U modulo $1+y^{2r}$. Hence $\sum_{z,w} \chi(z+w) \psi(z+w) = \sum_z \psi(z) \chi(z) \sum_w \psi(w) \chi(1+wz^{-1})$. As $z \in U$, $w \in y^r$, $\chi(1+wz^{-1}) = \bar{\psi}(\alpha wz^{-1})$, whence

$$\sum_{z,w} \chi(z+w) \psi(z+w) = \sum_z \psi(z) \chi(z) \sum_w \psi((1-\alpha z^{-1})w).$$

The sum over w may be considered as the sum over y^r/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 y^r , i.e. unless $z \equiv \alpha \pmod{y^r}$. If $z \equiv \alpha \pmod{y^r}$, then the sum over w is $\sum y^r$. Taking α to be the representative of its class modulo 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 y^{2r+1} , $r > 0$. The above methods permit the following reduction:

Lemma

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

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

Proof

Precisely as before $z \mapsto \chi(1+z)$ is an additive character on y^{r+1} . Hence $\chi(1+z) = \bar{\psi}(\alpha z)$ for all $z \in y^{r+1}$, 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 y^r follows from the fact that ψ_β trivial on y^{r+1} implies $\beta y^{r+1} \subset y^{1+2r}$ which implies that $\beta \in y^r$. This proves the first part of the lemma.

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

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

$$= \sum_v \psi((1-\alpha u^{-1})v) = \begin{cases} Ny^r & \text{if } u \equiv \alpha \pmod{y^r} \\ 0 & \text{if } u \not\equiv \alpha \pmod{y^r} \end{cases}$$

Taking α to be the representative of the class of α modulo y^r ,

$$(Ny)^{-1/2} (\chi, \psi) = \sum_z \chi(\alpha+z) \psi(\alpha+z) = \chi(\alpha) \psi(\alpha) \sum_z \psi(z) \chi(1+(z/\alpha)) = \chi(\alpha) \psi(\alpha) \sum_{z \in y^r / y^{r+1}} \psi(\alpha z) \chi(1+z),$$

which proves the lemma.

To complete the computation of (χ, ψ) we must determine $\sum_{z \in \mathcal{O}/\mathcal{O}^\times} \psi(\alpha z) \chi(1+z) = \sum_{z \in \mathcal{O}/\mathcal{O}^\times} \psi(\alpha \pi^r z) \chi(1+\pi^r z)$, π being a prime element of k . For $x \in \mathcal{O}$, let $\phi(x) = \psi(\alpha \pi^r x) \chi(1+x \pi^r)$. ϕ satisfies a simple functional equation:

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

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

- (1) Δ maps \bar{k} into the unimodular complex numbers
- (2) $\Delta(0) = 1$
- (3) $\Delta(x+x^r) = \Delta(x) \Delta(x^r) \overline{\theta(xx^r)}$

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 $\sum_{x \in k} \Delta(x)$ as Δ -sums.

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

Lemma: If k is a finite field with q elements and characteristic p , θ is a non-trivial character of k^\times 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 $\Delta'(x) = \Delta(x) \bar{\theta}(cx)$ and $\sum_{x \in k} \Delta'(x) = \bar{\Delta}(c) \sum_{x \in k} \Delta(x)$.

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

Proof

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 $\Delta((r+1)x) = \Delta(rx)\Delta(x) \bar{\theta}(rx^2) = (\Delta(x))^{r+1} \bar{\theta}(x^2(r+\frac{r(r-1)}{2})) = (\Delta(x))^{r+1} \bar{\theta}(x^2 \frac{(r+1)r}{2})$ which proves the assertion in general.

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

For $p \neq 2$, therefore $\Delta(x)$ is a p^{th} root of 1, while for $p = 2$, $\bar{\theta}(x) = \pm 1$ 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 $x \rightarrow \bar{\theta}(cx)$ 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 $\hat{f}(x) = \frac{1}{\sqrt{q}} \sum_{z \in k} f(z) \bar{\theta}(xz)$. The inversion formula holds as is easily verified for the function $\theta(x) = \begin{cases} \sqrt{q} & \text{for } x = 0 \\ 0 & \text{for } x \neq 0 \end{cases}$ as $\hat{\theta}$ is the unit function

and the transform of the unit function is again θ . For the function Δ we have: $\hat{\Delta}(0) = \frac{1}{\sqrt{q}} \sum_z \Delta(x+z) = \Delta(x) \frac{1}{\sqrt{q}} \sum_z \Delta(z) \bar{\theta}(xz) = \Delta(x) \hat{\Delta}(x)$ whence $\hat{\Delta}(x) = \hat{\Delta}(0) \bar{\Delta}(x)$ (as $|\Delta(x)| = 1$). Assertion 4 follows directly.

5. By the inversion formula $1 = \Delta(0) = \hat{\Delta}(0) = \hat{\Delta}(0) \bar{\Delta}(0) = |\hat{\Delta}(0)|^2$ 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 analogous 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 $s_{K/k}^{(2)}$ where K is an extension of finite degree of a ground field, k .

Lemma

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

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

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

$$3. (s_{K/k}(a))^2 = s_{K/k}(a^2) + 2s_{K/k}^{(2)}(a).$$

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.

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

$$g^*(\Delta^*) = (-g(\Delta))^n.$$

Proof

Trivially, $\Delta^*(0) = \Delta(0)\theta(0) = 1$. For $x, y \in K$, from the previous lemma, $\Delta^*(x+y) = \Delta(S(x)+S(y))\theta(S^{(2)}(x)+S^{(2)}(y)+S(x)S(y)-S(xy)) = \Delta^*(x)\Delta^*(y)\bar{\theta}^*(xy)$ which proves the first assertion.

For the second assertion, consider the polynomials with coefficients in k and highest coefficient 1. To every such polynomial $F(X) = X^n + c_1 X^{n-1} + c_2 X^{n-2} + \dots + c_n$, 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. vol 55(1949)pp.497-508.

polynomial F , and by Z an indeterminate, this gives the formal identity: $1 + \sum_F \lambda(F) Z^{n(F)} = \prod_P (1 - \lambda(P) Z^{n(P)})^{-1}$ 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 these 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 $Z^n \sum_{x,y} \Delta(x)\theta(y) = Z^n g(\Delta) \sum_y \theta(y) = 0$. This gives

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

Similarly if $F^*(X) = X^n + d_1 X^{n-1} + \dots + d_n$ is a polynomial over K , we write $\lambda'(P^*) = \Delta^*(d_1)\theta^*(d_2)$ 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 $\deg K(t)/K = \deg k(t)/K/k(t) = n/d$, 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 $\deg K(t)/k(t) = n/d$.

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

$$\begin{aligned} & (\Delta \circ S_{K/K})(a')(\theta \circ S_{K/K}^{(2)})(a')(\theta \circ S_{K/K})(b') \\ &= (\Delta \circ S_{K(t)/k}(t)) \theta((S_{K/K}^{(2)} \circ S_{K(t)/K})(t) + (S_{K/K} \circ S_{K(t)/K}^{(2)})(t)) \\ &= \Delta(S_{K(t)/k}(t)) \theta(S_{K(t)/k}^{(2)}(t)). \end{aligned}$$

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

$$\begin{aligned} S_{K(t)/k}^{(2)}(t) &= S_{K(t)/k}^{(2)}(S_{K(t)/k}(t)) + S_{K(t)/k}(S_{K(t)/k}^{(2)}(t)) \\ &= S_{K(t)/k}^{(2)}(mt/d) + S_{K(t)/k}(\frac{m}{d}(\frac{m}{d}-1)\frac{1}{2}t^2) \\ &= (\frac{m}{d})^2 b + (\frac{m}{d})(\frac{m}{d}-1)\frac{1}{2} S_{K(t)/k}(t^2) \end{aligned}$$

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 η be the prime of a local number field of which k is the residue class field and let (for $a \in k$) $(\frac{a}{\eta}) = +1$ or -1 depending upon whether or not a is a square. We assert

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

$$\sum_{x \in k} \theta(x^2) = \left(\frac{a}{y}\right) \sum_{x \in k} \theta(ax^2).$$

Proof

If $\left(\frac{a}{y}\right) = 1$ then $a k^2 = k^2$ so that the assertion follows.

If $\left(\frac{a}{y}\right) = -1$ then $k^* = k^{*2} \cup ak^{*2}$ and as θ is ^{not} trivial we have

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

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

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

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

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 γ 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: $\Delta(x\gamma) = \Delta(x)\Delta(\gamma)\bar{\theta}(x\gamma)$. 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 $\Delta(x) = \bar{\theta}\left(\frac{x^2}{2} + \gamma x\right)$ for all $x \in k$, then

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

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 $\Delta(\beta x) = \Delta_0^*(x)\theta_0^*(\gamma x)$

where Δ_0^* is the function $(\Delta_0 \circ S_{k/R})(\theta_0 \circ S_{k/R}^{(2)})$ on k and

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

then

$$\frac{1}{\sqrt{2^f}} \sum_{x \in k} \Delta(x) = \frac{\Delta_0^*(\gamma)}{\sqrt{2}} \left(\frac{i}{\sqrt{2}}\right)^f (-1)^{f-1}$$

Proof

(1) $p \neq 2$: Let $\Delta_0(x) = \theta_0\left(\frac{x^2}{2}\right)$ for all $x \in R$. Then $\Delta_0(x+y) = \Delta_0(x)\Delta_0(y)\theta_0(xy)$. Let $\Delta_0^* = (\Delta_0 \circ S_{k/R})(\theta_0 \circ S_{k/R}^{(2)})$, a function

on k ; then by the previous theorem, $(-\sum_{x \in R} \Delta_0(x))^f = -\sum_{x \in k} \Delta_0^*(x)$.

But for $x \in k$, $\Delta_0^*(x) = \theta_0\left(-\frac{1}{2}(S(x))^2 + S^{(2)}(x)\right)$

$$= (\theta_0 \circ S)\left(\frac{x^2}{2}\right) = \theta_0\left(\frac{x^2}{2}\right) = \theta_0\left(\frac{1}{2\eta} x^2\right)$$

Hence by the previous lemma, $\sum_{x \in k} \Delta_0^*(x) = \left(\frac{\eta}{\gamma}\right) \sum_{x \in k} \theta_0(x^2/2)$.

From the previous lemma,

Let Δ^* be the function $x \mapsto \theta_0(x^2/2)$ on k . Then Δ^* satisfies the same functional equation as Δ and therefore there exists unique

$\gamma \in k$ such that $\Delta(x) = \Delta^*(x)\theta_0(\gamma x)$ and also

$$2\Delta(x) = \Delta^*(\gamma)2\Delta^*(x) = \Delta^*(\gamma)2\theta_0\left(\frac{x^2}{2}\right) = \theta(\gamma^2/2) \left(\frac{\eta}{\gamma}\right) 2\Delta_0^*(x)$$

$= \theta(\gamma^2/2) \left(\frac{\eta}{\gamma}\right) (-1)^{f-1} \left(\sum_{x \in R} \Delta_0(x)\right)^f$, all the sums except for the last

being over k . The condition on γ is $\Delta(x) = \Delta^*(x)\theta_0(\gamma x) =$

$\overline{\theta}(x/2 + \gamma x)$ and by a classical result, $\sum_{x \in R} \Delta_0(x) = \sum \overline{\theta}_0(x^2/2)$
 $= \left(\frac{2}{p}\right) \sum_{x \in R} \overline{\theta}_0(x^2) = \left(\frac{-2}{p}\right) \sqrt{p} \sqrt{\left(\frac{-1}{p}\right)}$. As $\left(\frac{-2}{p}\right)^2 = \left(\frac{-2}{p}\right)$, 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, $(-\sum_{x \in R} \Delta_0(x))^2 = -\sum_{x \in k} \Delta_0^*(x)$, whence

$$\sum_{x \in k} \Delta_0^*(x) = (-1)^{2-1} \left(\frac{1+i}{2}\right)^2 \sqrt{2}^2. \text{ Let } \Delta^* \text{ be the function}$$

$x \mapsto \Delta(\beta x)$ 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, $\sum_{x \in k} \Delta^*(x) =$

$\sum_{x \in k} \Delta(x)$ as $\gamma \neq 0$. As Δ^* and Δ_0^* satisfy the same functional equation, there exists a unique element $\gamma \in k$ such that

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

Also $\sum \Delta^*(x) = \overline{\Delta_0^*(\gamma)} \sum \Delta_0^*(x)$ (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.

Theorem 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 γ be the unit in T

uniquely determined modulo p by the condition that

$$\bar{\psi}(\alpha \pi^{2f} x) = (\theta_0 \circ S_{\mathbb{T}/R})(\gamma x) \text{ for all } x \in \mathcal{O}_T \text{ (= the ring of integers of } \mathbb{T})$$

Then

if $p \neq 2$, there exists an integer γ in \mathbb{T} uniquely determined modulo \mathfrak{p} by the condition

$$\psi(\alpha \pi^f x) \chi(1 + x \pi^f) = \psi(\alpha \pi^{2f} (\frac{x^2}{2} + \gamma x)) \text{ for all } x \in \mathcal{O}_T$$

and

$$(\chi, \psi) = \chi(\alpha) \psi(\alpha) \bar{\psi}(\alpha \pi^{2f} \gamma^{1/2}) (\frac{-2\gamma}{\mathfrak{p}}) (-1)^{f-1} (\sqrt{\frac{-1}{\mathfrak{p}}})^f$$

if $p = 2$, let $\beta \in U_{\mathbb{T}}$ be chosen such that $\gamma \equiv 1/\beta^2 \pmod{\mathfrak{p}}$

Δ_0 be the function on \mathcal{O}_R which is 1 on $2U_R$ and i on

U_R (where U_R is the group of units of R)

Δ_0^* be the function $(\Delta_0 \circ S_{\mathbb{T}/R})(\theta_0 \circ S_{\mathbb{T}/R}^{(2)})$ on \mathcal{O}_T

θ_0^* be the character $\theta_0 \circ S_{\mathbb{T}/R}$ on \mathbb{T}^*

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

$$\psi(\alpha \pi^n \beta x) \chi(1 + x \beta \pi^n) = \Delta_0^*(x) \theta_0^*(\gamma x) \text{ for all } x \in \mathcal{O}_T$$

and

$$(\chi, \psi) = \chi(\alpha) \psi(\alpha) \Delta_0^*(\gamma) (\frac{1+i}{\sqrt{2}})^f (-1)^{f-1}$$

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

Proof

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 $x \mapsto \chi(1 + \alpha \pi^n x) \psi(\alpha \pi^n x)$ and θ was obtained in the same way from the character $\chi_{\alpha \pi^n}$. The inertial subfield \mathbb{T} is used in defining γ and η because $\theta_0 \circ S_{\mathbb{T}/R}$ 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 y^n , $n > 1$, let s be the smallest integer such that $3s \geq n$; then there exists a unit α uniquely determined modulo y^{n-s} by the condition

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

and

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

where

$$t = 1$$

if n is even

$$t = \left(\frac{-27}{y} \right) \left(\sqrt{\frac{-1}{p}} \right)^f (-1)^{f-1}$$

if n is odd (η as defined in the last theorem).

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

Chapter III

The Abelian Norm Theorem

In the following k is a local number field, K is an abelian extension of degree n , (τ_1, \dots, τ_n) is the group of characters of k^* which are trivial on $N_{K/k} K^*$, K_H^* is the kernel in K^* of $N_{K/k}$ and \mathbb{C} is the field of complex numbers. Following Tate, a continuous homomorphism of k^* into \mathbb{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 \mathcal{O} be the group of all quasi-characters of K which are trivial on K_H^* . Let $\mathcal{O}_{K/k}$ be the complex valued function

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

on \mathcal{O} , the product being over all quasi-characters of k^* whose composition with the relative norm is X . This function is certainly well defined whenever the denominator is not zero. The definition is made precise by interpreting the function, \mathcal{O} , 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 $Q_{K/k}(\chi) = \chi(m, K/k)$, 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

$$\begin{aligned} \chi(m, K/k) &= 1 && \text{if } m = 0 \\ \chi(-1, K/k) &= \left(\frac{N_{K/k}}{e''}\right)^{1+m} && \text{if } m \neq 0 \end{aligned}$$

and if 2 does not divide e^* then

$$\chi(-1, K/k) = (-1)^{e^*(f^*-1)} \text{ord}_{\mathfrak{p}} \left(\frac{N_{K/k}}{e''}\right)$$

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

$K_{\mathbb{H}}^*$ = the unimodular complex numbers.

The generic quasi-character, χ , of K^* trivial on $K_{\mathbb{H}}^*$ is $x \mapsto |x|^{2s}$ 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

$$\mu_1: x \mapsto |x|^s$$

$$\mu_2: x \mapsto |x|^s (\text{sign } x). \quad \text{For these characters}$$

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

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

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{p} be the prime of k , $\mathfrak{o}_{\mathfrak{p}}$ the absolute different of $k_{\mathfrak{p}}$. Let R be the \mathfrak{p} -adic completion of the rational numbers $(\mathfrak{p} | p)$ and let λ be the mapping of R into the reals mod 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 \mathfrak{p} -adic integer.

Let θ be the additive character $x \rightarrow \exp(2\pi i \lambda(x))$ of R . The standard additive character 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

$$\rho_k(\mu) = N_{k/R}(\mathcal{N}_k F(\mu))^{-1/2} \mu(\pi^{-\text{ord } \mathcal{N}_k F(\mu)}) (\mu, \psi_{\pi^{-\text{ord } \mathcal{N}_k F(\mu)}})$$

where $F(\mu) =$ conductor of μ

$$\begin{aligned} (\mu, \psi_{\pi^{-\text{ord } \mathcal{N}_k F(\mu)}}) &= \text{root number as defined in Chapter II} \\ &\quad \text{if } y|F(\mu) \\ &= \frac{1 - N y^{-1} \mu(\pi^{-1})}{1 - \mu(\pi)} \quad \text{if } y \nmid F(\mu) \end{aligned}$$

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 y .

For K/k abelian and χ a character of K^* trivial on K_{Π}^*

$$\rho_{K/k}(\chi) = \frac{\prod_{\mu \circ N = \chi} \{ N_{k/R}(\mathcal{N}_k F(\mu))^{-1/2} \mu(\pi^{-\text{ord } \mathcal{N}_k F(\mu)}) (\mu, \psi_{\pi^{-\text{ord } \mathcal{N}_k F(\mu)}}) \}}{N_{K/R}(\mathcal{N}_k F(\chi))^{-1/2} \chi(\pi^{-\text{ord } \mathcal{N}_k F(\chi)}) (\chi, \psi_{\pi^{-\text{ord } \mathcal{N}_k F(\chi)}})}$$

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 ord_y in the numerator and ord_p in the denominator.

As shown in the proof of the lemma on admissible integers

$$\text{(Chapter I), } \prod_{\mu \circ N_{K/k} = \chi} F(\mu) = N_{K/k}(\mathcal{N}_{K/k} F(\chi))$$

whence

$$\begin{aligned} \mathbb{N}_{K/k}(\mathcal{G}_K P(X)) &= (\mathbb{N}_{K/R} \circ \mathbb{N}_{R/k})(\mathcal{G}_K \mathcal{G}_{K/k} P(X)) \\ &= \mathbb{N}_{K/R}(\mathcal{G}_K^n \prod_{\mu \circ N_{K/k} = X} P(\mu)) = \prod_{\mu \circ N_{K/k} = X} \mathbb{N}_{K/R}(\mathcal{G}_K P(\mu)) \end{aligned}$$

It follows that

$$\mathcal{G}_{K/k}(X) = \frac{\prod_{\mu \circ N_{K/k} = X} \left\{ \mu(\pi^{-\text{ord } \mathcal{G}_K F(\mu)})(\mu, \psi_{\pi^{-\text{ord } \mathcal{G}_K F(\mu)}}) \right\}}{X(\prod_{\mu \circ N_{K/k} = X} P(\mu)) (X, \bar{\psi}_{\prod_{\mu \circ N_{K/k} = X} P(\mu)})}$$

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 $P(X) = \mathcal{P}^{n+1}$, $\mathcal{G}_K = \mathcal{G}^d$ then $\mathcal{G}_{K/k}(X) = (-1)^{(n-1)(d+1-m)} \left[\prod_{\mu} (\mu, \psi_{\pi^{-d-1-m}}) \right] / (X, \bar{\psi}_{\prod_{\mu} P(\mu)})$.

(b) If K/k is purely ramified, set $\pi = \mathbb{N}_{K/k} \bar{\pi}$ and then

$$\mathcal{G}_{K/k}(X) = \left[\prod_{\mu} (\mu, \psi_{\pi^{-\text{ord } \mathcal{G}_K F(\mu)}}) \right] / (X, \bar{\psi}_{\prod_{\mu} P(\mu)})$$

in both cases the product being over all quasi-characters of k^+ whose composition with $\mathbb{N}_{K/k}$ is X .

Proof

(a) As K/k is unramified, we may set $\pi = \tau$. In the notation of Chapter I, $s_j = -1$ ($1 \leq j \leq n$) whence $\mu \circ \mathbb{N}_{K/k} = X \Rightarrow$

$P(\mu) = \mathcal{P}^{1+n}$. Also $d = \text{ord}_y \mathcal{G}_K = \text{ord}_p \mathcal{G}_K$. Hence it only remains to compute (μ_0 fixed, $\mu_0 \circ \mathbb{N}_{K/k} = X$)

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

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

where τ is an unramified quasi-character such that $\tau(\pi) = \xi$, 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

$$\frac{\prod_{j=1}^n (\mu_0 \tau_j)(\pi^{-\text{ord}_k \mathcal{I}_k} F(\mu_0 \tau_j))}{\chi(\Pi^{-\text{ord}_k \mathcal{I}_k} F(X))}$$

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

$$(\mu_0(\pi)^{-1})^{\sum_{\mu} \text{ord}_y \mathcal{I}_k} F(\mu)^{-\text{ord}_p \mathcal{I}_k} F(X) \quad \text{which is one as}$$

$$N_{K/k}(\mathcal{I}_{K/k} F(X)) = \prod_{\mu} F(\mu) \quad \Rightarrow \quad \sum_{\mu} \text{ord}_y F(\mu) = \text{ord}_p (\mathcal{I}_{K/k} F(X))$$

and as $\mathcal{I}_k = \mathcal{I}_{K/k} \mathcal{I}_k \Rightarrow \text{ord}_p \mathcal{I}_k = \text{ord}_p \mathcal{I}_{K/k} + n \text{ord}_y \mathcal{I}_k$ (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 Unramified

$\chi = \mu \circ N_{K/k}$, $\tau_j = \tau^j$, τ trivial on U_k , $\tau(\pi) = \xi$, a primitive n -th root of 1, $\mathcal{I}_k = y^d$, $F(X) = p^{1+mn}$, $F(\mu) = y^{1+mn}$

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

$$Q(X) (-1)^{(n-1)(d+1+m)} = \frac{\prod_{j=1}^m (\mu \tau_j, \psi_{\pi^{-d-1-m}})}{(X, \bar{\psi}_{\pi^{-d-1-m}})} \quad (5)$$

Case 1, $m = -1$:

$$(\mu \tau_j, \psi_{\pi^{-d}}) = \left[1 - \frac{1}{N_{\mathbb{Y}} \mu(\pi) s^j} \right] / \left[1 - \mu(\pi) s^j \right]$$

$$(X, \bar{\psi}_{\pi^{-d}}) = \left[1 - \frac{1}{(N_{\mathbb{Y}} \mu(\pi))^n} \right] / \left[1 - (\mu(\pi))^n \right]$$

whence the right side of (5) is 1. Hence for $m = -1$, $Q(X) = (-1)^{d(n-1)}$.

Case 2, $m \geq 0$:

As γ divides $P(\mu \tau_j)$, $(\mu \tau_j, \psi_{\pi^{-d-1-m}})$ 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

$$Q_{\mathbb{K}/\mathbb{K}}(X) (-1)^{(n-1)(d+1+m)} = \frac{(\mu, \psi_{\pi^{-d-1-m}})^m}{(X, \bar{\psi}_{\pi^{-d-1-m}})} \quad (55)$$

The notation may now be simplified. From the definition of standard additive characters, $\bar{\psi} = \psi \circ S_{\mathbb{K}/\mathbb{K}}$, hence setting

$$\varphi = \psi_{\pi^{-d-1-m}} \quad \psi = \bar{\psi}_{\pi^{-d-1-m}} \quad \text{we have } \psi = \varphi \circ S_{\mathbb{K}/\mathbb{K}}$$

and the right side of (55) is $(\mu, \varphi)^m / (X, \psi)$. 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 $\mu(1+\pi) = \bar{\varphi}(\alpha \pi)$ for all $\pi \in \mathfrak{y}^{\times}$, $r = (1+m)/2$. For $w \in \mathfrak{p}^{\times}$, $\chi(1+\pi) = \mu(1+\pi w + S(2)_w + \dots + \pi^r w)$

$= \mu(1 + S_{K/k} w) = (\bar{\varphi} \circ S_{K/k})(\alpha w) = \bar{\varphi}(\alpha w)$, as $S_{K/k}(\mathcal{P}^r) \subset \mathcal{Y}^r$
 and $S_{K/k}^{(j)}(\mathcal{P}^r) \subset \mathcal{Y}^{1+rn}$ 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 $(n+1)$ even.

$n+1$ odd

Let $r = n/2$. 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 $j \geq 2$, $S_{K/k}^{(j)}(\mathcal{P}^{r+1})$
 lies in \mathcal{Y}^{n+1} , while $S(\mathcal{P}^{r+1}) \subset \mathcal{Y}^{r+1}$, whence
 for $w \in \mathcal{P}^{r+1}$, $\chi(1+w) = (\mu \circ N)(1+w) = \mu(1+S(w))$
 $= (\bar{\varphi} \circ S)(\alpha w) = \varphi(\alpha w)$.

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
 $\bar{\varphi}(\alpha \pi^{2r} x) = (\theta_0 \circ S_{T^*/R})(\eta x)$ for $x \in \mathcal{U}_T$
 As $T = k \cap T^*$, $K = kT^*$, it follows that for $x \in \mathcal{U}_T$, $S_{K/k}(x)$
 $= S_{T^*/T}(x)$, whence

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

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

(a) $y \neq 2$ There exists $\gamma \in \mathcal{O}_K$ such that

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

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

$$\begin{aligned} \chi(1+z\pi^r) \varphi(\alpha z\pi^r) &= (\mu \circ N_{K/k})(1+z\pi^r) (\varphi \circ S_{K/k})(\alpha z\pi^r) \\ &= \mu(1 + \pi^r S(z) + \pi^{2r} S^{(2)}(z)) (\varphi \circ S)(\alpha z\pi^r) \\ &= \mu(1 + \pi^r S(z)) \varphi(\alpha \pi^r S(z)) \mu(1 + \pi^{2r} S^{(2)}(z)) \\ &= \varphi(\alpha \pi^{2r} [\frac{(S(z))^2}{2} + \gamma S(z)]) \bar{\varphi}(\alpha \pi^{2r} S^{(2)}(z)) \\ &= \Phi(\alpha \pi^{2r} (\frac{z^2}{2} + \gamma z)) \end{aligned}$$

Letting f be the absolute degree of γ , we obtain

$$\frac{(\mu, \varphi)^m}{(\chi, \Phi)} = \frac{\{\mu(\alpha) \varphi(\alpha) \bar{\varphi}(\alpha \pi^{2r} \gamma/2) (\frac{2\gamma}{\pi}) (-1)^{f-1} (\sqrt{\frac{-1}{p}})^f\}^m}{\Phi(\alpha) \chi(\alpha) \bar{\Phi}(\alpha \pi^{2r} \gamma/2) (\frac{2\gamma}{\pi}) (-1)^{mf-1} (\sqrt{\frac{-1}{p}})^{mf}} = (-1)^{m-1} = (-1)^{(m-1)(m+1)}$$

(b) $y \neq 2$ Let T, T^*, θ_0 be as above. Let

Δ_0 be the function on \mathcal{O}_R defined by $\Delta_0(x) = 1$ for $x \in 2\mathcal{O}_R$
 $= 1$ for $x \in \mathcal{O}_R$

Δ^* be the function $(\Delta_0 \circ S_{T/R})(\theta_0 \circ S_{T/R}^{(2)})$ on \mathcal{O}_T

Δ'' be the function $(\Delta_0 \circ S_{T^*/R})(\theta_0 \circ S_{T^*/R}^{(2)})$ 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^*} , $(\Delta^* \circ S_{T^*/T})(\theta^* \circ S_{T^*/T})$

$$= (\Delta_0 \circ S_{T^*/R})(\theta_0 \circ S_{T^*/R}^{(2)} \circ S_{T^*/T})(\theta_0 \circ S_{T^*/R} \circ S_{T^*/T}^{(2)})$$

$= (\Delta_0 \circ S_{T^*/R})(\theta_0 \circ S_{T^*/R}^{(2)}) = \Delta^n$, i.e., Δ^n may be obtained from Δ^* in much the same way that Δ^* is obtained from Δ_0 .

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

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

For $x \in \mathcal{U}_T$ (precisely as in paragraph (a)) $S_{K/k}(x) =$

$$S_{T^*/T}(x), S_{K/k}^{(2)}(x) = S_{T^*/T}^{(2)}(x) \text{ and also}$$

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

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

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

$$= \Delta^*(S_{K/k}(x)) \theta^*(\gamma S_{K/k}(x)) \overline{\varphi}(\pi^{2x} \alpha S_{K/k}^{(2)}(\beta x)) =$$

$$(\Delta^* \circ S_{T^*/T})(x) \theta^n(\gamma x) (\theta_0 \circ S_{T^*/R})(\eta S_{K/k}^{(2)}(\beta x)) \quad (\text{from definition of } \eta)$$

As $\eta S_{K/k}^{(2)}(\beta x) = \eta \beta^2 S_{T^*/T}^{(2)}(x) \equiv S_{T^*/T}^{(2)}(x) \pmod{\gamma}$ and as

$\theta_0 \circ S_{T^*/R}$ is trivial on $\gamma \cap T$, it follows that the above expression may be written

$(\Delta^* \circ S_{T^*/T})(x) \theta^n(\gamma x) (\theta_0 \circ S_{T^*/R}^{(2)})(x) = \Delta^n(x) \theta^n(\gamma x)$ (the last equality following from the previously derived relation between Δ^n and Δ^*).

By the theory of local root numbers we now have

$$\begin{aligned} \frac{(\mu, \varphi)^m}{(\chi, \Phi)} &= \frac{\left\{ \varphi(\alpha) \mu(\alpha) \bar{\Delta}'(\gamma) \left(\frac{1+i}{\sqrt{2}} \right)^f (-1)^{f-1} \right\}^m}{\Phi(\alpha) \chi(\alpha) \bar{\Delta}''(\gamma) \left(\frac{1+i}{\sqrt{2}} \right)^{mf} (-1)^{mf-1}} = (-1)^{m-1} \frac{(\bar{\Delta}'(\gamma))^m}{\bar{\Delta}''(\gamma)} \\ &= (-1)^{n-1} (\bar{\Delta}'(\gamma))^n / \bar{\Delta}''(\gamma) \text{ which is } (-1)^{n-1} \text{ as } \Delta^n(\gamma) \\ &= (\Delta^n \circ S_{\mathbb{T}^*/\mathbb{T}})(\gamma) (\theta^n \circ S_{\mathbb{T}^*/\mathbb{T}}^{(2)})(\gamma) = \Delta^n(n\gamma) \theta^n\left(\frac{n}{2}(m-1)\gamma\right) \\ &= (\Delta^n(\gamma))^n \text{ (using the fact that } \gamma \in \mathbb{T} \text{ and using one of the elementary properties of the function } \Delta^n) \end{aligned}$$

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 $s_{K/k}^{(j)}(\varphi^m)$ will be needed. The following will be adequate for our purposes.

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

$$1. \quad s_{K/k}(\varphi^m) < y^{m'} \Leftrightarrow m' \leq \left[\frac{m + \text{ord}_{\varphi} \rho_{K/k}}{e} \right]$$

(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

$$j \text{ then } s_{K/k}^{(j)}(\varphi^m) < y^{\left[\frac{j^m + \text{ord}_{\varphi} \rho_{K/k}}{e} \right]}$$

Proof

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

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 $(1+\gamma)$, i.e. if

$$n = (U_k : NU_k) = (U_k : 1+\gamma) = N\gamma^{-1}.$$

The previous estimates on traces reduces now to

$$S^{(j)}(\gamma^r) = \gamma^{\left[\frac{jr+n-1}{n}\right]} \quad \text{for } 1 \leq j \leq n-1.$$

The computations are greatly simplified by the existence 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 existence 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 $\langle \pi \rangle \cdot (1+\gamma)$ with the unique subgroup of index n of the $(N\gamma^{-1})$ 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_{Π}^* , let μ be a character of k^* such that $\mu \circ N_{K/k} = \chi$, and such that the conductor of μ has the smallest possible exponent. The set of all characters of k^* whose composition with the relative norm

$S_{K/k}(\mathcal{F}^{mj})$ 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 \mathcal{Y} , divides the degree.

Notation

T is the inertial subfield of k/R

θ is the standard additive character of R

θ_0 is the character $\theta_{p^{-1}}$ of R^*

θ^* is the character $\theta_0 \circ S_{T/R}$ of T^*

For $p = 2$:

Δ_0 is the function on \mathcal{U}_R which is 1 on the ideal (2) and is 1 on the group of units.

Δ^* is the function $(\Delta_0 \circ S_{T/R})(\theta_0 \circ S_{T/R}^{(2)})$ on \mathcal{U}_T

K/k Ramified Cyclic of Prime degree n , $p \neq n$.

Introduction

Conductor of $K/k = \mathcal{Y}$, $\mathcal{D}_{K/k} = \mathcal{F}^{n-1}$

Let $\mathcal{D}_k = \mathcal{Y}^d$, then $\mathcal{D}_K = \mathcal{F}^{n(d+1)-1}$

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 \mathcal{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{f}^{1+n} .

1. $n = -1$ (i.e. χ unramified)

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

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

Hence by a previous lemma,

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

$$\text{As } \pi = \mathbb{N}_{K/k}\pi \cdot \mathbb{N}\mathfrak{f} = \mathbb{N}\mathfrak{y}.$$

$$\frac{(\mu, \psi_{\pi^{-d}})}{(\chi, \bar{\psi}_{\pi^{-nd-n+1}})} = \frac{1 - \mathbb{N}\mathfrak{y}^{-1}\mu(\pi^{-1})}{1 - \mu(\pi)} \cdot \frac{1 - \chi(\pi)}{1 - \mathbb{N}\mathfrak{f}^{-1}\chi(\pi^{-1})} = 1$$

whence $Q_{K/k}(\chi) = \prod_{j=1}^{n-1} (\tau_j, \psi_{\pi^{-d-1}})$ as the symbols appear-

ing 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 character, 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 $\tau^{n-j} = \tau^{-j} = \bar{\tau}^j$, 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

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

2. $n \geq 0$

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

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

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

but $\prod_{j=0}^{n-1} \gamma^{j(d+1+t)} = (-1)^{(n+1)(d+1+t)} \pi^{d+1+t}$

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

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

2.1. $m=0$

Conductor of $\chi = \varphi$, $N\varphi = N\gamma$, hence

$$\sqrt{N\gamma}(\chi, \Phi) = \sum_{x \in U_K/(1+\varphi)} \chi(x) \Phi(x). \text{ Taking as representatives}$$

of the residue classes of U_K modulo $(1+\varphi)$ the $(N\gamma+1)$ roots of 1 in K , all of which lie in k , the sum on the right becomes

$$\sum_{x \in U_K/(1+\gamma)} \mu^n(x) \varphi^n(x) = \sqrt{N\gamma}(\mu^n, \varphi^n), \text{ whence}$$

$$Q_{K/k}(\chi) = \left[\prod_{j=0}^{n-1} (\mu \gamma^j, \varphi) \right] / (\mu^n, \varphi^n) \text{ , which, by a previ-}$$

ously quoted result of Hasse and Davenport, is just $\prod_{j=1}^{n-1} (\gamma^j, \varphi)$

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

2.2. $t > 0$

2.2.1.1 $1+t$ even, $n \neq 2$

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

$\mu(1+z) = \bar{\varphi}(\alpha z)$ for all $z \in \mathfrak{y}^{(1+nt)/2}$. From the estimates on traces it is readily verified that for $\text{ord}_{\mathfrak{p}} w \geq (1+nt)/2$, we have $S(w) \in \mathfrak{y}^{(1+t)/2}$, $s^{(j)}(w) \in \mathfrak{y}^{1+t}$ for $2 \leq j \leq n-1$, $H(w) \in \mathfrak{y}^{1+t}$, whence $\chi(1+w) = \mu(1+S(w)) = \bar{\varphi}(\alpha S(w)) = \bar{\varphi}(\alpha w)$.

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

Applying the formula for the root numbers,

$$\mathfrak{Q}_{K/k}(\chi) = \frac{\prod_{j=0}^{n-1} [(\mu\tau^j)(\alpha)\varphi(\alpha)]}{\chi(\alpha)\bar{\varphi}(\alpha)} = \prod_{j=0}^{n-1} \tau^j(\alpha) = \tau(\alpha)^{n(n-1)/2} = 1$$

2.2.1.2. 1+t even, n=2

Here the conductor of χ is \mathfrak{p}^{1+2t} , $(1+2t)$ of course odd.

Also $\pi = N(\Pi) = -\Pi^2$. Certainly $\mathfrak{y} \nmid 2$.

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

$$\mu(1+z) = \bar{\varphi}(\alpha z) = (\mu\tau^j)(1+z) \text{ for all } z \in \mathfrak{y}^{(1+t)/2}$$

For $w \in \mathfrak{p}^{1+t}$, $\text{ord}_{\mathfrak{y}} S(w) \geq (1+t)/2$, $\text{ord}_{\mathfrak{y}} H(w) \geq 1+t$, whence

$$\chi(1+w) = \mu(1+S(w)+H(w)) = \mu(1+S(w)) = \bar{\varphi}(\alpha S(w)) = \bar{\varphi}(\alpha w).$$

There exists an element γ of \mathbb{T} such that $\bar{\varphi}(\alpha \pi^{2t} x) =$

$$(0_0 \circ S_{\mathbb{T}/R})(\gamma x) \text{ for all } x \in \mathcal{O}_{\mathbb{T}}. \text{ Hence,}$$

$$(0_0 \circ S_{\mathbb{T}/R})(\gamma x) = \bar{\varphi}(\alpha (-1)^t \pi^t x) = \varphi(2\alpha \pi^t x) \text{ for } x \in \mathcal{O}_{\mathbb{T}}, \text{ a relation which we hold for future use.}$$

Finally there exists $\gamma \in \mathcal{O}_{\mathbb{T}}$ such that for all integers x

in \mathbb{T}_p $\theta(\alpha \pi^{2t} (\frac{x^2}{2} + \gamma x)) = \chi(1 + x \pi^t) \theta(\alpha x \pi^t)$. Using the relations between χ and μ and between θ and θ_p , the right side becomes $\theta(\alpha S(x \pi^t)) \mu(1+S(x \pi^t)+N(x \pi^t))$
 $= \theta(\alpha S(x \pi^t)) \mu(1+S(x \pi^t)) \mu(1+x^2 \pi^t) = \bar{\theta}(\alpha x^2 \pi^t)$
 $= \bar{\theta}(\frac{1}{2} \alpha x^2 \pi^t) = \bar{\Phi}((-1)^t \frac{1}{2} \alpha x^2 \pi^{2t})$
 $= \bar{\theta}(\alpha \pi^{2t} \frac{x^2}{2})$ comparing this with the left side of the condition on γ , clearly $\gamma = 0$.

Applying the root number formulae,

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

where f is the absolute degree of γ . As τ is of order 2 and

$$\alpha \in U_K, \quad \tau(\alpha) = \left(\frac{\alpha}{\gamma}\right), \text{ whence}$$

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

. 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 \mathbb{T} , $\delta \equiv 2\alpha/\gamma \pmod{\gamma}$. then $(\theta(X))^{-1} = \left(\frac{-\delta}{\gamma}\right) (-1)^{f-1} \left(\sqrt{\frac{-1}{p}}\right)^f$, and also by the relation between θ_0 and θ_p $(\theta_0 \circ S_{\mathbb{T}/\mathbb{R}})(x) = \theta(\delta \pi^t x) = \psi_{\pi^{-d-1}}(\delta x)$ for all $x \in \mathcal{O}_{\mathbb{T}}$. Let τ' be the restriction of τ to $\mathcal{O}_{\mathbb{T}}$. As $(\tau, \psi_{\pi^{-d-1}})$ depends only upon the behavior of the additive and multiplicative characters on the $(N\gamma - 1)$ roots of 1 in k , all of which lie in \mathbb{T} , and as $\psi_{\pi^{-d-1}}$ coincides with $(\theta^*)_{\delta^{-1}}$ on $\mathcal{O}_{\mathbb{T}}$, it is clear that

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

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

Hence $(\tau, \psi_{\pi^{-d-1}}) = \left(\frac{\delta}{\gamma}\right) (-1)^{f-1} \left(\sqrt{\left(\frac{-1}{p}\right)}\right)^f \left(\frac{-1}{\gamma}\right) = \epsilon_{K/k}(\chi)$ as $\left(\sqrt{\left(\frac{-1}{p}\right)}\right)^{2f} = \left(\frac{-1}{\gamma}\right)$. This proves the assertion which shows that $\epsilon_{K/k}(\chi)$ 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, $(\theta \circ S_{T/R})(\chi/p) = \theta'(x) = \psi_{\pi^{-d-1}}(\delta x) = (\theta \circ S_{K/R})(\delta x / \pi^{d+1}) = (\theta \circ S_{T/R})(\delta x (S_{K/T}(\pi^{-1}/\pi^d)))$,

whence $\sigma^{-1} \equiv p S_{K/T}(\pi^{-1}/\pi^d) \pmod{\gamma}$ and so

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

2.2.2.1. 1+t odd, $p \neq 2$.

conductor of $\mu = \gamma^{1+t}$
 conductor of $\chi = \frac{\gamma}{p}^{1+nt}$, 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

$$\begin{aligned} \mu(1+x) &= \overline{\varphi}(\alpha x) \quad \text{for all } x \in \gamma^{1+(t/2)} \\ \theta^t(\eta x) &= \overline{\varphi}(\alpha \pi^t x) \quad \text{for all } x \in \mathcal{O}_T \\ \varphi(\alpha \pi^{t/2} (\frac{x^2}{2} + \gamma x)) &= \varphi(\alpha \pi^{t/2} x) \mu(1+x \pi^{t/2}) \quad \text{for all } x \in \mathcal{O}_T \end{aligned}$$

We assert that

$$\begin{aligned} \chi(1+w) &= \overline{\varphi}(\alpha' w) \quad \text{for all } w \in \gamma^{1+(nt/2)} \\ \theta^t(\eta' x) &= \overline{\varphi}(\alpha' \pi^{nt} x) \quad \text{for } x \in \mathcal{O}_T \\ \varphi(\alpha' \pi^{nt} (\frac{x^2}{2} + \gamma' x)) &= \varphi(\alpha' \pi^{nt} x) \chi(1+x \pi^{nt/2}) \quad \text{for } x \in \mathcal{O}_T \end{aligned}$$

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

For the first assertion the estimates on traces give

$$\begin{aligned} \text{ord}_\gamma S(w) &\geq 1 + (t/2) \\ \text{ord}_\gamma S^{(j)}(w) &\geq 1 + t \\ \text{ord}_\gamma \Pi(w) &\geq 1 + (nt/2) \geq 1 + t, \quad \text{where the symmetric functions} \\ &\quad \text{are with respect to } K/k. \end{aligned}$$

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

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

$$\overline{\varphi}(\alpha \pi^{nt} x) = \overline{\varphi}(\alpha (-1)^{(n+1)t} \pi^t x) = \overline{\varphi}(\alpha \pi^t x) = \overline{\varphi}(n \alpha \pi^t x) = \theta^t(n \eta x),$$

which is the second assertion.

For the third assertion the estimates on traces are

$$\begin{aligned} S(\gamma^{nt/2}) &\subset \gamma^{t/2} \\ S^{(j)}(\gamma^{nt/2}) &\subset \gamma^t \quad \text{for } 2 \leq j \leq n-1 \\ \Pi(\gamma^{nt/2}) &= \gamma^{nt/2} \subset \begin{cases} \gamma^{1+t} & \text{for } n > 2 \\ \gamma^t & \text{for } n = 2 \end{cases} \end{aligned}$$

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

$$\begin{aligned}
 & \phi(\alpha \pi^{nt/2}) \chi(1+z \pi^{nt/2}) \\
 &= \phi(\alpha S(z \pi^{nt/2})) \mu(1+S(z \pi^{nt/2})+S^{(2)}(z \pi^{nt/2})) = \\
 & \phi(\alpha \pi^{t/2} \left[\frac{1}{2} \left(\frac{S(x \pi^{nt/a})}{\pi^{t/a}} \right)^2 + \gamma \left(\frac{S(x \pi^{nt/a})}{\pi^{t/a}} \right) \right]) \bar{\phi}(\alpha S^{(2)}(x \pi^{nt/a})) \\
 &= \phi(\alpha \left(\frac{1}{2} (S(z \pi^{nt/2}))^2 - S^{(2)}(z \pi^{nt/2}) \right)) \bar{\phi}(\alpha \gamma \pi^{t/2} S(z \pi^{nt/2})) \\
 &= \phi(\alpha \frac{1}{2} S(z^2 \pi^{nt})) \bar{\phi}(\alpha \gamma \pi^{t/2} z \pi^{nt/2}) \\
 &= \phi \left\{ \alpha \pi^{nt} \left(\frac{x^2}{2} - \gamma x \left(\frac{\pi}{\pi^n} \right)^{t/a} \right) \right\} = \phi \left(\alpha \pi^{nt} \left(\frac{x^2}{2} + \gamma x \right) \right)
 \end{aligned}$$

which is the third assertion.

Finally we note that $(\tau^j \mu)(1+z) = \bar{\phi}(\alpha z)$ for $z \in \gamma^{1+(t/2)}$

Hence by the theory of local root numbers

$$\begin{aligned}
 Q_{\mathbb{Z}/\mathbb{Z}}(X) &= \frac{\prod_{j=0}^{n-1} \left\{ (\tau^j \mu)(\alpha) \phi(\alpha) \bar{\phi}(\alpha \pi^t \gamma^2/2) \left(\frac{-2\gamma}{\gamma} \right) (-1)^{f-1} \left(\sqrt{\left(\frac{-1}{p} \right)} \right)^f \right\}}{\chi(\alpha) \bar{\phi}(\alpha) \bar{\phi}(\alpha \pi^{nt} \gamma^2/2) \left(\frac{-2n\gamma}{\gamma} \right) (-1)^{f-1} \left(\sqrt{\left(\frac{-1}{p} \right)} \right)^f} \\
 &= \frac{\tau(\alpha)^{n(n-1)/2} \left(\frac{n}{\gamma} \right) \left(\frac{-2\gamma}{\gamma} \right)^{n-1} \left\{ (-1)^{f-1} \left(\sqrt{\left(\frac{-1}{p} \right)} \right)^f \right\}^{n-1}}{\bar{\phi} \left(\frac{\alpha \gamma^2}{2} \{ S(\pi^{nt}) - n \pi^t \} \right)}
 \end{aligned}$$

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) $n \neq 2$

Here $n-1$ is even and therefore $(\tau(\alpha))^{n(n-1)/2} = 1$ and $\left(\frac{-2\gamma}{\gamma} \right)^{n-1} = 1$, so that

$$Q(X) = \left(\frac{n}{\gamma} \right) \left((-1)^{f-1} \left(\sqrt{\left(\frac{-1}{p} \right)} \right)^f \right)^{n-1} = \left(\left(\frac{n}{p} \right) \left(\sqrt{\left(\frac{-1}{p} \right)} \right)^{n-1} \right)^f$$

whence by the quadratic law of reciprocity, $Q_{K/k}(X) = \left(\frac{p}{n}\right)^f$.

(b) $n = 2$

Here $\tau(\alpha) = \left(\frac{\alpha}{y}\right)$, hence $Q(X) = \left(\frac{-\alpha^2}{y}\right)(-1)^{f-1} \left(\sqrt{\left(\frac{-1}{p}\right)}\right)^f$.

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

$$\theta^*(\eta x) = \bar{\varphi}(\alpha \pi^t x) = \psi_{\pi^{d-1}}(-\alpha x)$$

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

It follows from the analysis of case 2.2.1.2. that

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

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

2.2.2.2. $1+t$ odd, $n = 2$

Here $n \neq 2$, exponent of the conductor of X 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

$$\mu(1+x) = \bar{\varphi}(\alpha x) \text{ for } x \in y^{1+(t/2)}$$

$$\theta^*(\eta x) = \bar{\varphi}(\alpha \pi^t x) \text{ for } x \in \mathcal{O}_T$$

$$\Delta^j(x)\theta^*(\gamma x) = \varphi(\alpha \pi^{t/2} \beta x) \mu(1 + \beta x \pi^{t/2}) \text{ for } x \in \mathcal{O}_T$$

$$\eta \equiv 1/\beta^2 \pmod{y}$$

$$(\mu^j)(1+x) = \bar{\varphi}(\alpha x) \text{ for all integers } j, x \in y^{1+(t/2)}$$

The proofs in 2.2.2.1 show that

$$X(1+w) = \bar{\varphi}(\alpha w) \text{ for } w \in y^{1+(nt/2)}$$

and also

$$\theta^*(n\gamma x) = \theta^*(\alpha \pi^{nt} x) \text{ for } x \in \mathcal{O}_T$$

Let β' be a unit in \mathbb{Z} such that $\beta'^2 \equiv (n\gamma)^{-1}$, i.e. $(\frac{\beta}{\beta'})^2 \equiv n^{-1}$.

We assert that

$$\Delta^*(x)\theta^*(\gamma x) = \theta^*(\alpha \pi^{nt/2} \beta' x) \chi(1 + \beta' x \pi^{nt/2}) \text{ for } x \in \mathcal{O}_T \quad (\S)$$

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

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

$$\rho(\alpha \beta \pi^{t/2} w) \mu(1 + \alpha \beta \pi^{t/2} w) \mu(1 + s(2)(x \beta' \pi^{nt/2})),$$

where $w = (\beta \pi^{t/2})^{-1} s(x \beta' \pi^{nt/2}) = nx \beta' / \beta$

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

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

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

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

(modulo γ). Also for $x \in \mathcal{O}_T$, $\theta^*(x^2) = \theta^*(x)$ as $S_{\mathbb{Z}/R}(x^2) \equiv$

$S_{\mathbb{Z}/R}(x) \pmod{\gamma}$. 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

$$\begin{aligned} \mathcal{O}_{\mathbb{Z}/R}(\chi) &= \frac{\prod_{\gamma=0}^{n-1} \{(\mu \tau^{\frac{1}{2}})(\alpha) \varphi(\alpha) \bar{\Delta}^*(\gamma) (\frac{1+i}{\sqrt{2}})^{\frac{1}{2}} (-1)^{\frac{1}{2}}\}}{\chi(\alpha) \bar{\Phi}(\alpha) \bar{\Delta}^*(\gamma + \frac{n-1}{2}) (\frac{1+i}{\sqrt{2}})^{\frac{1}{2}} (-1)^{\frac{1}{2}}} \\ &= \frac{[\bar{\Delta}^*(\gamma)]^n \{(\frac{1+i}{\sqrt{2}})^{\frac{1}{2}} (-1)^{\frac{1}{2}}\}^{n-1}}{\bar{\Delta}^*(\gamma + \frac{n-1}{2})} \end{aligned}$$

By the functional equation of Δ^*

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

As shown in Chapter II, $(\Delta^*(\chi))^2 = \Delta^*(n\chi) \theta^*(\chi \frac{n(n-1)}{2})$,

also $\theta^* = \bar{\theta}^*$ on \mathcal{U}_T , 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 $\left(\frac{a}{n} \right)$ given by the quadratic reciprocity law, the right side of the above relation reduces to $\left(\frac{a}{n} \right)^2$.

Thus we have shown:

Lemma If k is a γ -adic number field, K a cyclic ramified extension of prime degree n , γ/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

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

2. If $n \neq 2$,

$$Q(\chi) = 1 \quad \text{if the conductor of } \chi \text{ is } \mathfrak{f}^0 \text{ or } \mathfrak{f}$$

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

where

f is the absolute degree of γ

d is the exponent of the absolute different of k

p is the rational prime which γ 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 $\mathfrak{g}_{K/k} = \mathfrak{f}^{(p-1)(1+v)}$. Hence

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

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 is trivial on the norm group has 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 $K_{\mathfrak{p}^*}$ conductor of $\chi = \mathfrak{f}^{1+m}$, τ is a fixed non-trivial character of k^* trivial on the norm group, μ is a character of k^* such that $\mu \circ \mathfrak{N}_{K/k} = \chi$ and whose conductor is \mathfrak{y}^{1+b} , where $m = \mathfrak{S}_{K/k}(b)$ 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

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

v is admissible \Leftrightarrow absolute degree of η is ^{not} 1. To prove this we first note that the index $((1 + \eta^v)_{HK^*} : HK^*)$ is not 1 (as $1 + \eta^v \notin HK^*$) and divides $(k^* : NK^*) = p$, whence the index is p .

But v admissible $\Leftrightarrow (1 + \eta^v) \cap HK^* \neq (1 + \eta^{1+v}) \cap HK^* = (1 + \eta^{1+v})$

$$\Leftrightarrow ((1 + \eta^v) : (1 + \eta^{1+v})) > ((1 + \eta^v) : (1 + \eta^v) \cap HK^*)$$

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

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

$$s_{K/k}^{(j)}(\varphi^x) \subset \eta^{\left[\frac{jn + (p-j)(v+1)}{p} \right]} \quad \text{for } 1 \leq j \leq p-1$$

For the ramified extension studied previously, it was possible to choose a prime element, π , of K such that

$\pi^n + (-1)^n N(\pi) = 0$. For the extension 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

$$\pi^p / \pi^{(-1)^{p-1}} \equiv 1 \pmod{\varphi^{(p-1)v}} \quad \text{and furthermore}$$

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

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

Proof

Let $h(x) = x^p + a_1 x^{p-1} + \dots + a_p$ be the irreducible polynomial in k of which π is a root. Then $a_p = (-1)^p \pi$ and $a_j \in \varphi$ ($1 \leq j < p$). Clearly

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

$$\text{Also } h^p(\pi) = p\pi^{p-1} + (p-1)a_1\pi^{p-2} + \dots + a_{p-1}$$

As is well known, each of the terms in the expression for $h^*(\Pi)$ has a different valuation, the smallest $\text{ord}_{\mathcal{P}}$ 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 separately.

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

$$\text{ord}_{\mathcal{P}}\left(\frac{a_j}{\pi} \Pi^{p-j}\right) > pe + p - 1 + (1-p) = pe = (p-1)v \quad (\text{where } e \text{ is the absolute ramification of } \mathcal{P})$$

whence

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

(b) $(1+v)(p-1) = \text{ord}_{\mathcal{P}}(a_1 \Pi^{p-1-1})$ ($p \nmid 1$), then

$$\text{ord}_{\mathcal{P}} a_1 - 1 = v(p-1) \Rightarrow p(v - \text{ord}_{\mathcal{P}} a_1) = v - 1 \quad (\text{i.e. } v \equiv 1 \pmod{p})$$

For $j \neq 1$, $1 \leq j \leq p-1$,

$$\text{ord}_{\mathcal{P}}(a_1 \Pi^{p-1-1}) < \text{ord}_{\mathcal{P}}(a_j \Pi^{p-j-1}) \Rightarrow$$

$$\text{ord}_{\mathcal{P}}\left(\frac{a_1}{\pi} \Pi^{p-1}\right) < \text{ord}_{\mathcal{P}}\left(\frac{a_j}{\pi} \Pi^{p-j}\right) \Rightarrow$$

$$\text{ord}_{\mathcal{P}}\left[\frac{\Pi^p}{(\pi(-1)^{p-1})}\right] = \text{ord}_{\mathcal{P}}\left(\frac{a_1}{\pi} \Pi^{p-1}\right) = \text{ord}_{\mathcal{P}} a_1 - 1 = v(p-1).$$

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 , and let $\tilde{\psi}$ 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

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

$$z \in \mathfrak{y}^{1+(v/2)} \quad \text{if } v \text{ is even}$$

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

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

- 1) $N(1+\mathfrak{z}^a) = (1+\mathfrak{y}^a) \cap KK^*$ for $1 \leq a \leq v$
 $N(z) \equiv 1 \pmod{\mathfrak{y}^a} \Rightarrow z \equiv 1 \pmod{\mathfrak{z}^a}$
- 2) For $r \geq 0$, $1+\mathfrak{y}^{1+v+pr} = N(1+\mathfrak{z}^{p+v+pr}) = N(1+\mathfrak{z}^{1+v+pr})$
 $N(z) \equiv 1 \pmod{\mathfrak{y}^{1+v+pr}} \Rightarrow$ there exists $A \in K^*$ such that
 $z \equiv A^{\sigma^{-1}} \pmod{\mathfrak{z}^{p+v+pr}}$ where σ generates $G(K/k)$
- 3) $N(1+\mathfrak{z}^v) = 1+\mathfrak{y}^{v+1} \Leftrightarrow$ absolute degree of \mathfrak{y} is 1.
- 4) $(1+\mathfrak{z}^{1+v}) \cap (K^*)^{\sigma^{-1}} = (1+\mathfrak{z}^{1+v})^{\sigma^{-1}}$ for $r \geq 0$
- 5) $s(j)(\mathfrak{z}^a) \subset \mathfrak{y}^{\lfloor \frac{aj + (p-1)(1+v)}{p} \rfloor}$ for $1 \leq j \leq p-1$
- 6) Let $v' = v - \lfloor \frac{v}{p} \rfloor$, then $\text{ord}_{\mathfrak{y}} p \geq v'$ and

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

7) If $1 \leq a \leq v$ then $x \mapsto N(x) \pmod{\mathfrak{y}^a}$ is an additive homomorphism of \mathcal{O}_K onto $\mathcal{O}_K/\mathfrak{y}^a$ with kernel \mathfrak{f}^a .

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

$Z \in \mathcal{O}_K$, $N(Z)/Z^p \equiv 1 \pmod{\mathfrak{f}^{pv}}$

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

10) If $u \in \mathcal{O}_K$ then $S(u\pi^v)/N(u\pi^v)$ is a unit in k and is congruent modulo \mathfrak{f} 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 $Z^* \in 1 + \mathfrak{f}^a$ such that $N(Z/Z^*) = 1$, whence $Z \in Z^*(K)^{\sigma-1} \subset Z^*(1 + \mathfrak{f}^v) \subset (1 + \mathfrak{f}^a)$. 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 $Z \in \mathfrak{f}^{1+v}$, $(1+Z)^{\sigma-1} = 1 + Z(Z^{\sigma-1}-1)/(1+Z) \in 1 + \mathfrak{f}^{1+v}$. For inclusion in the opposite direction, induction is used. The statement is first proven for $v=0$. It is first noted that

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

If $x \in (1 + \mathfrak{f}^{1+v}) \cap (K^+)^{\sigma-1}$ 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 $w = u\pi^{ap+b}$, 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}^n , whence by index considerations the mapping is onto.

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

a) $|x| > |y|$, then $z = y/x \in \mathcal{P}$, and by (5), $N(1+z) \equiv 1+Nz \bmod y^{v^t}$, whence $N(x+y) = Nx N(1+z) \equiv Nx (1+Nz) \equiv Nx+Ny \bmod y^{v^t}$.

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

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

8) It has already been shown that $\pi^p / N(\pi) \equiv (-1)^{p-1} \bmod \mathcal{P}^{v(p-1)}$. As $pv^t \geq (p-1)v$, 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 \mathcal{O}_K . As a direct consequence of (6), $x \mapsto x^p \bmod \mathcal{P}^{pv^t}$ is an additive homomorphism of \mathcal{O}_K . For $z \in \mathcal{O}_K$, we may write $z = a_0 + a_1 \pi + \dots + a_{p-1} \pi^{p-1}$, $a_0 \in \mathcal{O}_K$, $a_j \in \mathcal{O}_K$.

whence $N(z)/z^p \equiv \frac{a_0^p + a_1^p \pi + \dots + \pi^{p-1} a_{p-1}^p}{a_0^p + a_1^p \pi^p + \dots + a_{p-1}^p \pi^{p(p-1)}} \bmod \mathcal{P}^{pv^t}$. The right

is congruent to 1 mod $\mathcal{P}^p \left(\frac{\pi^p}{\pi} - 1 \right) = \mathcal{P}^{pv}$, 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 $z \in \mathcal{P}^a$, $N(1+z) \equiv 1+S(z)+N(z) \bmod y^{1+v}$ as is verified with the aid of (5). Furthermore $S(z), N(z) \in y^a$ and therefore $1 = \tau(1+S(z)+N(z)) = \bar{\tau}(\alpha_0 S(z) + \alpha_0 N(z))$

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

$$1 = \overline{\varphi} \left\{ \alpha_0 (xS(u\pi^V) + x^D N(u\pi^V)) \right\} = \overline{\varphi} (\alpha_0 \pi^V N_{\mathbb{H}}(xE + x^D)).$$

By (5) E is an algebraic integer. Let E' be an element of T congruent mod \mathfrak{p} to E and u' an element of T congruent mod \mathfrak{p} to u , then

$$1 = \overline{\varphi} (\alpha_0 \pi^V u'^D (xE' + x^D)) \text{ and therefore by the definition of } \beta_0,$$

$$1 = \theta^* \left(\left(\frac{\alpha'}{\beta_0} \right)^D (xE' + x^D) \right). \text{ As } S_{T/R}(x) \equiv S_{T/R}(x^D) \pmod{\mathfrak{p}},$$

$\theta^* \left(\left(\frac{\alpha'}{\beta_0} \right)^D E' x \right) = \theta^* \left(\left(\frac{\alpha'}{\beta_0} \right) x \right)$. The assertion follows using the fact that θ^* has conductor \mathfrak{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 $K_{\mathbb{H}}^*$

$l+m$ = 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{p}^{l+b} , such that $\chi = \mu \circ N_{K/k}$

$\psi, \overline{\psi}$ are the standard additive characters of k and K respectively

$$\varphi = \psi_{\pi^{-d-l-v}}$$

$$\varphi^* = \psi_{\pi^{-d-l-b}}$$

} additive characters of k

$\phi = \prod_{\pi} \pi^{-d-1-m}$, an additive character of K

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

$$= (\pi / \prod p_j^{d+1+b}) \quad \text{otherwise}$$

S is a fixed primitive $(p-1)^{\text{st}}$ root of unity
 a_j is an integer such that $a_j \equiv S^j \pmod{p}$ ($1 \leq j \leq p-1$)
 $\tau_j = \tau^{a_j}$.

The relations between the characters ϕ, ϕ^t, ϕ may be easily established.

Lemma

$$\phi^t = \phi_{\pi^{v-b}} \quad \text{if } t \equiv 1 \pmod{p^{v(p-1)}}$$

On \mathcal{O}_K $\phi = (\phi \circ S)_{\pi^{v-b}}$ if either $b = v$ or if $b < v$.
 $p \neq 2$

On K , $\phi = (\phi^t \circ S)_B$ 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 u, b, v and from E.F.(5).

Finally $Q(X)$ may be expressed in terms of the characters ϕ, ϕ^t, ϕ . It follows from the determination of the various conductors that:

Lemma

$$Q(X) = \frac{(\mu, \varphi') \prod_{i=1}^{p-1} (\mu \tau^i, \varphi)}{(X, \Phi)} \quad \text{for } b \leq v$$

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

Detailed Computations1. $b = -1, m = -1$

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

$$(\mu, \varphi^2) / (\chi, \varphi) = \frac{1 - N\mu^{-1}(\pi^{-1})}{1 - \mu(\pi)} \cdot \frac{1 - \chi(\pi)}{1 - N\chi^{-1}(\pi^{-1})} = 1.$$

Hence $Q(\chi) = \prod_{j=1}^{p-1} (\tau^j, \varphi) = \begin{cases} 1 & \text{for } p \neq 2 \\ (\tau, \varphi) & \text{for } p = 2, \text{ the result} \end{cases}$

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. $b = 0 = n$

$$Q(\chi) = \frac{(\mu, \varphi^2)}{(\chi, \varphi)} \prod_{j=1}^{p-1} (\mu \tau^j, \varphi). \text{ The quotient}$$

and the product are computed separately.

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

Proof:

$p \neq 2, 1+v$ even

$$\text{If } \text{ord}_y z \geq (1+v)/2, \tau(1+z) = \overline{\varphi}(\alpha_0 z) \Rightarrow \tau^{2j}(1+z) =$$

$$\overline{\varphi}(a_j \alpha_0 z) \Rightarrow \tau_j(1+z) = \overline{\varphi}(s^j \alpha_0 z) \Rightarrow (\mu \tau_j)(1+z) = \overline{\varphi}(s^j \alpha_0 z)$$

as μ is trivial on $1+y$. Hence $(\mu \tau_j, \varphi) = (\mu \tau_j)(\alpha_0 s^j) \varphi(\alpha_0 s^j)$,

whence the contention is easily verified using the fact that

s lies in the norm group.

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

$$\text{As above, if } \text{ord}_y z \geq 1+(v/2), (\mu \tau_j)(1+z) = \overline{\varphi}(\alpha_0 s^j z)$$

There exists $\gamma_0 \in \mathcal{U}_\Gamma$ such that $\theta^*(\gamma_0 x) = \bar{\varphi}(\alpha_0 \pi^v x)$ for $x \in \mathcal{O}_\Gamma$

Hence $\theta^*(S^{\frac{1}{2}} \gamma_0 x) = \bar{\varphi}(\alpha_0 S^{\frac{1}{2}} \pi^v x)$. There exists $\gamma \in \mathcal{O}_\Gamma$ such that

$$\tau(1+x \pi^{v/2}) \varphi(\alpha_0 x \pi^{v/2}) = \varphi(\alpha_0 \pi^v (\frac{x^2}{2} + \gamma x)), \text{ whence}$$

$$\tau_y(1+x \pi^{v/2}) \varphi(\alpha_0 S^{\frac{1}{2}} x \pi^{v/2}) = \varphi(\alpha_0 S^{\frac{1}{2}} \pi^v (\frac{x^2}{2} + \gamma x)).$$

$$\text{Hence } \prod_{j=1}^{p-1} (\mu \tau^j, \varphi) = \prod_{j=1}^{p-1} \{ (\mu \tau_j)(\alpha_0 S^{\frac{1}{2}}) \varphi(\alpha_0 S^{\frac{1}{2}}) (\frac{-2S^{\frac{1}{2}} \gamma_0}{y}) \bar{\varphi}(\alpha_0 S^{\frac{1}{2}} \pi^v \frac{\gamma_0^2}{2}) (-1)^f (\frac{-1}{p})^f \}$$

$$= \mu(-\alpha_0^{p-1}) (\frac{-1}{y}) (\frac{-1}{p})^f \frac{1}{2} = \mu(-\alpha_0^{p-1}), \text{ as } (\frac{-1}{y}) = (\frac{-1}{p})^f, \text{ which}$$

proves the contention for $p \neq 2$.

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

If $1+v$ is even, $\tau(1+z) = \bar{\varphi}(\alpha_0 z)$ for $\text{ord}_y z \geq (1+v)/2$, whence $(\mu \tau)(1+z) = \bar{\varphi}(\alpha_0 z)$. 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, $(\mu \tau)(1+z) = \bar{\varphi}(\alpha_0 z)$ for $\text{ord}_y z \geq 1+(v/2)$,

$$\bar{\varphi}(\alpha_0 \pi^v x) = \theta^*(x/\beta_0^2) \text{ for } x \in \mathcal{O}_\Gamma$$

$$\tau(1+\pi^{v/2} x) \varphi(\alpha_0 \pi^{v/2} x) = \Delta^*(x/\beta_0) \theta^*(\gamma_0 x/\beta_0) \text{ for } x \in \mathcal{O}_\Gamma$$

$$\text{whence } (\mu \tau)(1+\pi^{v/2} x) \varphi(\alpha_0 \pi^{v/2} x) = \Delta^*(x/\beta_0) \theta^*(\gamma_0 x/\beta_0).$$

Hence precisely as before $(\mu \tau, \varphi) = \mu(\alpha_0) (\tau, \varphi)$, which completes the proof of the contention.

To compute $(\mu, \varphi^*) / (\chi, \varphi)$, let μ_0 be the restriction of μ to Γ^* . As μ and χ have conductors y and z respectively, the corresponding root numbers depend upon the behavior of $\mu, \chi, \varphi^*, \vartheta$ at the $(Ny-1)$ roots of 1 and therefore can be expressed in terms of the root number (μ_0, ϑ^*) .

$$\varphi^* = \psi_{\Gamma-d-1} = (\vartheta \circ S_{\mathbb{Z}/R})_{\Gamma-d-1}, \quad \vartheta^* = \vartheta_{p-1} \circ S_{\mathbb{Z}/R}, \text{ whence}$$

$(\theta^* \circ S_{K/T}) = (\theta \circ S_{K/H})_{p-1} = \varphi^*_{\pi^{d+1/p}}$; 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

$x \rightarrow x^p$ 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 $\phi = (\varphi \circ S_{K/k})_{\pi^v} = (\varphi^*_{\pi^{-v}} \circ S_{K/k})_{\pi^v} =$

$(\theta^* \circ S_{K/T})_{p\pi^{d+1-v}} \circ S_{K/k})_{\pi^v}$, whence the restriction of ϕ to \mathcal{O}_T is:

$$(\theta^*)_{p S_{K/T}(\pi^{-d-1} S_{K/k}(\pi^v) / \mathbb{N}_{K/k}(\pi^v))}, \text{ while the}$$

restriction of χ to \mathcal{O}_T is μ_0^p . From E.P.(10),

$$S_{K/k}(\pi^v) / \mathbb{N}_{K/k}(\pi^v) \equiv -\beta_0^{p-1} \pmod{\gamma}, \text{ whence by E.P.(5)}$$

$$\text{ord}_p \left[p S_{K/T} \{ \pi^{-d-1} (-\beta_0^{p-1}) \} - p S_{K/T} \{ \pi^{-d-1} S_{K/k}(\pi^v) / \mathbb{N}_{K/k}(\pi^v) \} \right] \geq 1.$$

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 $\mathcal{O}_{K/k}(\chi)/A = \mu(\delta)$,

where $\delta = \{ \alpha_0 \beta_0^p p S_{K/T}(\pi^{-d-1}) \}_{p-1}$.

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

To prove this last assertion we recall that on \mathcal{O}_T , $\theta^1 = (\vartheta) \alpha_0 \beta_0^p \pi^v$, whence on the same ring, $\bar{\theta}^1 = \vartheta^1 \alpha_0 \beta_0^p = (\theta^1 \circ S_{K/T}) \alpha_0 \beta_0^p \pi^{-d-1} = \theta^1 S_{K/T} (\alpha_0 \beta_0^p \pi^{-d-1})$, whence $-1 \equiv \beta_0^p \pi^v S_{K/T} (\alpha_0 \pi^{-d-1}) \pmod{\mathfrak{y}}$. Letting α'_0 be an element of U_T congruent to α_0 modulo \mathfrak{y} and using E.P.(5), $-1 \equiv \beta_0^p \alpha'_0 \pi^v S_{K/T} (\pi^{-d-1}) \pmod{\mathfrak{y}}$ and the assertion then follows. Hence $\mu(\theta) = 1$ and therefore $Q(X) = A$ if $b = 0$.

For $b > 0$, $Q(X)$ 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.

Determination of Parameters ($b > 0$)

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 $\mu(1+z) = \bar{\theta}(\alpha z)$ for $z \in \mathfrak{y}^{(1+b)/2}$ (resp: $\mathfrak{y}^{1+(b/2)}$).

Lemma 1. Given X , it is possible to choose α_0 and α in such

a manner that there exists $\delta \in U_K$ for which $\alpha = \alpha_0 N_{K/k}(\delta)$.

Proof

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_L in terms of additive characters. These conditions remain satisfied if α_0 is replaced by an element congruent modulo γ^a , where $a = (1+v)/2$ or $1+(v/2)$. In any case by H.P.(7) there exists $\delta \in U_K$ such that $N(\delta) \equiv \alpha/\alpha_0 \pmod{\gamma^a}$. 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.

Lemma 2:

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

$$(\mu\tau_j)(1+z) = \begin{cases} \overline{\varphi}(\alpha_j z) & \text{if } b \leq v \text{ for } \text{ord } \gamma z \geq \begin{cases} (1+v)/2, & \text{if } v \text{ odd} \\ 1+(v/2), & \text{if } v \text{ even} \end{cases} \\ \overline{\varphi}^*(\alpha_j z) & \text{if } b \geq v \text{ for } \text{ord } \gamma z \geq \begin{cases} (1+b)/2, & \text{if } b \text{ odd} \\ 1+(b/2), & \text{if } b \text{ even} \end{cases} \end{cases}$$

(b) $\chi(1+w) = \overline{\varphi}(\alpha'w)$ for $\text{ord } \gamma w \geq \begin{cases} (1+m)/2 & \text{if } m \text{ odd} \\ 1+(m/2) & \text{if } m \text{ even} \end{cases}$

where

$$\begin{aligned} \alpha_j &= \int \alpha_0 + \alpha \pi^{v-b} & \text{if } b \leq v \\ \alpha_j &= \alpha + \alpha_0 \int \pi^{b-v} & \text{if } b \geq v \\ \alpha' &= \alpha \left(\frac{\pi}{\pi}\right)^{v-b} - \int \alpha_0 & \text{if } b < v \\ \alpha' &= \left[\alpha - \alpha_0 \delta \left(\frac{\pi}{\pi}\right)^{b-v} \right] / \delta & \text{if } b \geq v \end{aligned}$$

Proof

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

$$\mu(1+z) = \overline{\varphi}(\alpha z) \text{ for } \text{ord } \gamma z \geq b^n \quad (b^n \text{ is the integer in the set: } (1+b)/2, 1+(b/2))$$

Let v^n be the integer in the set: $(1+v)/2, 1+(v/2)$. It is easily verified that $b \leq v \Rightarrow b^n \leq v^n$. Hence for $\text{ord}_y z \geq v^n$, $\mu(1+z) = \bar{\varphi}^1(\alpha z)$, whence $(\mu \tau_j)(1+z) = (\mu \tau_j^a)(1+z) = \bar{\varphi}^1(\alpha z) \bar{\varphi}(a_j \alpha z) = \bar{\varphi}^1(\alpha_j z)$ as $a_j \equiv 5^j \pmod{p}$, $\text{ord}_y z + \text{ord}_y p \geq v^n + v \geq 1+v$.

For $b \geq v$, conductor of $\mu \tau_j =$ conductor of $\mu = y^{1+b}$. For $\text{ord}_y z \geq v^n$, $\tau(1+z) = \bar{\varphi}^1(\alpha z)$. But now $b^n \geq v^n$ and therefore for $\text{ord}_y z \geq b^n$ $\mu(1+z) = \bar{\varphi}^1(\alpha z)$, $\tau(1+z) = \bar{\varphi}^1(\alpha z)$, whence $(\mu \tau_j)(1+z) = \bar{\varphi}^1(\alpha z) \bar{\varphi}(a_j \alpha z)$. The assertion then follows using: $a_j \equiv 5^j \pmod{p}$, $b-v+\text{ord}_y(pz) \geq b-v+v^1+b^n \geq 1+b$.

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

For $b \geq v$, conductor of χ is z^{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^n be the integer in the set: $(1+m)/2, 1+(m/2)$. For $\text{ord}_z z \geq m^n$ it again follows from E.P.(5) that $\chi(1+z) = \mu(1+S(z)+N(z)) = \bar{\varphi}^1(\alpha S(z) + \alpha N(z))$ as $S(z), N(z) \in y^{b^n}$. As $v-b+m^n \geq v^n$ it again follows from E.P.(9) that $\varphi^1(\alpha N(z)) = \varphi(\alpha N(5z \pi^{v-b})) = (\bar{\varphi} \circ S)(\alpha S z \pi^{v-b})$

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^i and the restrictions to \mathcal{U}_T of the characters $\phi_{\pi^v} = \phi^i_{\pi^b} = \hat{\phi}_{\pi^m}$. There has already been occasion to introduce η_0, β_0 , units of T such that $(\bar{\phi})_{\alpha_0 \pi^v / \eta_0}$ coincides with θ^i on \mathcal{U}_T and $\beta_0^p \eta_0 \equiv 1 \pmod{\eta}$.

Lemma 3.

On \mathcal{U}_T $\bar{\theta}^i = \phi^i_{\alpha \pi^b / \eta} = \phi_{\alpha_j \pi^v / \eta_j} = \phi^i_{\alpha_j \pi^b / \eta_j} = \bar{\phi}_{\alpha' \pi^m / \eta'}$

where:

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

Proof

As $\phi^i_{\pi^b} = \phi_{\pi^v}$ and the conductor of ϕ is η^{1+v} , the conditions to be imposed on η, η_j are: $\alpha_0 / \eta_0 \equiv \alpha / \eta \equiv \alpha_j / \eta_j \pmod{\eta}$.

As $\alpha / \alpha_0 = N(\delta) \equiv \delta^p$, the assertions concerning η, η_j follow without difficulty. For $b < v$, $\bar{\phi}_{\alpha' \pi^m / \eta'} = (\phi \circ S_{K/k})_{\alpha' \pi^v / \eta'}$

The restriction of this last character to \mathcal{U}_T is readily found

to be $(\bar{\theta}^i)_h$, where $h \equiv \frac{\eta_0}{\eta'} \frac{S_{K/k}(\alpha' \pi^v)}{\alpha_0 \pi^v}$. η' is therefore de-

terminated by the condition $h \equiv 1$ and the assertion involving γ' follows easily with the help of E.P.(10). The proof for $b \geq v$ of the congruence involving γ' , 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:

$$\gamma_0 \in \mathcal{O}_{\mathbb{T}}, \quad \tau(1+x\pi^{v/2})\varphi(\alpha_0 x \pi^{v/2}) = \varphi(\alpha_0 \pi^v (\frac{x^2}{2} + \gamma_0 x)) \quad \text{if } p \neq 2$$

$$\Delta^*(x/\beta_0) \theta^*(\gamma_0 x/\beta_0) \quad \text{if } p = 2$$

for all $x \in \mathcal{O}_{\mathbb{T}}$. Likewise if $2 \mid b$, $\gamma \in \mathcal{O}_{\mathbb{T}}$ may be chosen so that

$$\mu(1+x\pi^{b/2})\varphi(\alpha x \pi^{b/2}) = \varphi(\alpha \pi^b (\frac{x^2}{2} + \gamma x)) \quad \text{if } p \neq 2$$

$$\Delta^*(x/\beta) \theta^*(\gamma x/\beta) \quad \text{if } p = 2, \text{ where}$$

in the latter case $\beta \in U_{\mathbb{T}}, \beta^2 \gamma \equiv 1$

The corresponding parameter for χ may now be specified.

Lemma 4

Let β' be an element of $U_{\mathbb{T}}$ such that $\beta'^p \gamma' \equiv 1$, then if $2 \mid m$, $x \in \mathcal{O}_{\mathbb{T}}$

$$\chi(1+x\pi^{m/2})\varphi(\alpha' x \pi^{m/2}) = \varphi(\alpha' \pi^m (\frac{x^2}{2} + \gamma' x)) \quad \text{if } p \neq 2$$

$$\Delta^*(x/\beta') \theta^*(\gamma' x/\beta') \quad \text{if } p = 2$$

where γ' is an integer of \mathbb{T} such that

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

$$\text{if } b > v: \gamma' = 0 \quad \text{if } p \neq 2$$

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

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

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

Proof

Let H be the function $x \mapsto \chi(1+x\pi^{m/2})\psi(\alpha'x\pi^{m/2})$ on \mathcal{U}_T .

If $\text{ord}_p m \geq \frac{m}{2}$ then by E.P.(5),

$\text{ord}_\gamma \psi(s) \geq b^{m/2}$

$\text{ord}_\gamma \psi(2)(z) \geq 1+b$ if $v > b$
 $\geq b$ if $v \leq b$ } for $p \neq 2$

$\text{ord}_\gamma \psi(j)(z) \geq 1+b$ 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 $x \in \mathcal{U}_T$, $H(x) = \mu(1+\psi(x\pi^{b/2})+\psi(x\pi^{b/2}))\psi(\alpha'x\pi^{b/2})$

$= \mu(1+\psi(x\pi^{b/2}))\psi(\alpha(\frac{\pi}{\pi})^{v-b}x\pi^{b/2})\mu(1+\psi(x\pi^{b/2}))\psi(\alpha_0x\pi^{b/2})$.

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

Furthermore by the relation between ψ and φ and E.P.(9), $(v-(b/2) \geq v^2)$
 $\psi(\alpha_0x\pi^{b/2}) = \varphi^*(\alpha\psi(x)\tau^{b/2})$. Hence

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

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

(using the fact that $\beta'^p = \beta$ and $\gamma'^p = \gamma$). 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 $b > v$:

$p \neq 2$ $2|b$ and for $x \in \mathcal{O}_{\mathbb{T}}$

$$\mathbb{H}(x) = \mu(1+S(x\pi^{m/2}))S(2)(x\pi^{m/2})N(x\pi^{m/2}) \cdot (\theta' \circ S)((\alpha - \alpha_0(\frac{\pi}{\pi})^{b-v})x\pi^{m/2})$$

For $\text{ord}_x z \geq m/2$, $2S(2)(z) \equiv -S(z^2) \pmod{y^{1+b}}$.

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

$$\mathbb{H}(x) = \mu(1+N(x\pi^{m/2}))(\theta' \circ S)(\alpha_0(\pi/\pi)^{b-v}x\pi^{m/2})\mu(1-S(x^2\pi^m)/2).$$

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

For $b > v$: $2|v$ and for $x \in \mathcal{O}_{\mathbb{T}}$
 $p = 2$

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

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

$\theta(\alpha x\pi^{m/2}/\beta) = \theta'(\alpha S(x\pi^{m/2}))$, it follows that

$$\mathbb{H}(x) = \theta'(\alpha_0 N(\alpha x\pi^{v/2}) + \alpha_0 S(\alpha x\pi^{v/2})) = \theta'(\alpha_0 W), \text{ where } 1+W \in$$

$\mathbb{H}(1+\alpha_0\pi^{v/2})$. Clearly $\text{ord}_y W = v/2$. As $\tau(1+W) = 1$,

$$\mathbb{H}(x) = \theta(\alpha_0 W)\tau(1+W) = \Delta^*(Z)\theta'(\alpha_0 W/2), \text{ where } Z \text{ is an integer of } \mathbb{T}$$

which is congruent modulo y to $W/\beta_0\pi^{v/2}$, which is readily found

to be congruent to x^2/β'^2 . Hence $\mathbb{H}(x) = \Delta^*(x^2/\beta'^2)\theta'(\gamma_0 x^2/\beta'^2)$

$= \Delta^*(x/\beta')\theta'(\gamma_0^{1/2}x/\beta')$. But $\bar{\Delta}^*(x) = \Delta^*(x)\theta^*(x)$, whence the

assertion follows for $b > v$, $p = 2$.

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

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

$$\begin{aligned} H(x) &= \mu(1+S(y)+S^{(2)}(y)+N(y)) (\varphi \circ S)((\alpha - \alpha_0 \delta)y) \\ &= \mu(1+S(y)) \varphi(\alpha S(y)) \mu(1+N(y)) \frac{(\varphi \circ S)(\alpha y^2/2)}{(\varphi \circ S)(\alpha_0 \delta y)} \\ &= \mu(1+N(y)) \frac{(\varphi \circ S)(\alpha y^2/2)}{(\varphi \circ S)(\alpha_0 \delta y)} \end{aligned}$$

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

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

whence,

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

$$\begin{aligned} \frac{\mu(1+N(y)) \varphi(\alpha N(y))}{\tau(1+N(\delta y)) \varphi(\alpha_0 N(\delta y))} &= \frac{\varphi(\alpha \pi^v (\frac{1}{2} N(x)^2 + \gamma N(x)))}{\varphi(\alpha_0 \pi^v (\frac{1}{2} N(x_0)^2 + \gamma_0 N(x_0)))} \\ &= \bar{\theta}^v (\frac{1}{2} x^2 (\gamma^{1/p} - \delta^2 \gamma_0^{1/p}) + x ((\gamma \gamma)^{1/p} - (\gamma_0 \gamma_0)^{1/p} \delta)) \quad (\text{using the} \\ &\text{relation between } \theta^v \text{ and } \varphi). \text{ Furthermore,} \end{aligned}$$

$$\frac{(\varphi \circ S)(\frac{1}{2} \alpha x^2 \pi^v)}{(\varphi \circ S)(\frac{1}{2} \alpha_0 \delta^2 x^2 \pi^v)} = \frac{\bar{\theta}^v (\frac{1}{2} \gamma' x^2 \alpha / \alpha')}{\bar{\theta}^v (\frac{1}{2} \gamma' \delta^2 x^2 \alpha_0 / \alpha')} \quad \text{These statements}$$

together with Lemma 3 yield: $H(x) = \bar{\theta}^v (\gamma' (\frac{1}{2} x^2 + \gamma' x))$. The assertion then follows from the relation between θ^v and $\bar{\theta}$.

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

as for $b > v$, $p \neq 2$ that

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

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

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

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

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 γ .

Lemma 5

Let β_j be a unit of T such that $\beta_j^p \eta_j \equiv 1$. Then for $x \in U_T$, $1 \leq j \leq p-1$,

$$\left. \begin{aligned} (\mu\tau_j)(1+x\pi^{v/2})\varphi(\alpha_j x\pi^{v/2}) &= \varphi(\alpha_j \pi^v (\frac{1}{2}x^2 + \gamma_j x))_{p \neq 2} \\ &\Delta^*(x/\beta_j)\theta^*(\gamma_j x/\beta_j)_{p=2} \end{aligned} \right\} \text{if } \frac{b \leq v}{2|v}$$

$$\left. \begin{aligned} (\mu\tau_j)(1+x\pi^{b/2})\varphi(\alpha_j x\pi^{b/2}) &= \varphi(\alpha_j \pi^b (\frac{1}{2}x^2 + \gamma x))_{p \neq 2} \\ &\Delta^*(x/\beta_j)\theta^*(\gamma x/\beta_j)_{p=2} \end{aligned} \right\} \text{if } \frac{b > v}{2|b}$$

where

$$\begin{aligned} \gamma_j &= \gamma_0 \quad \text{if } b < v \\ &\equiv (\delta^j \gamma_0 + \delta^p \gamma) / (\delta^j + \delta^p) \quad \text{if } b = v, 2|v, p \neq 2 \\ &\equiv (\gamma_0 + \gamma \delta + \sqrt{\delta}) / (\delta + 1). \quad \text{if } b = v, 2|v, p = 2. \end{aligned}$$

Proof The proof follows almost directly from the definitions.

For $p = 2$, $b = v$, use is made of the functional equation of Δ^* .

Computation of $Q(X)$, $b > 0$.

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

$p \neq 2$

It is our purpose to show that for p odd, $Q(X) = 1$.

An important step in this direction is taken by showing that $Q(X)$ may be computed as though all the conductors have even exponents.

Lemma 6

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

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

Proof

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

$$(1) \left. \begin{array}{l} 1+v \text{ even} \\ 1+b \text{ odd} \\ b < v \end{array} \right\} \frac{(\mu, \phi^*)}{\mu(\alpha)\phi^*(\alpha)} = \left(\frac{-27}{y}\right)\phi^*(\alpha \pi^b \gamma^2/2) \left(\sqrt{\left(\frac{-1}{p}\right)}\right)^f (-1)^{f-1}$$

$\mu\tau_j$ has conductor with even exponent

$$\frac{(\chi, \phi)}{\chi(\alpha')\phi(\alpha')} = \left(\frac{-27'}{y}\right)\phi(\alpha' \pi^b \gamma'^2/2) \left(\sqrt{\left(\frac{-1}{p}\right)}\right)^f (-1)^{f-1}$$

Hence it is enough to show that $\left(\frac{27'}{y}\right) \frac{\phi^*(\alpha \pi^b \gamma^2/2)}{\phi(\alpha' \pi^b \gamma'^2/2)} = 1$

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^{\pm} and using the relations between $\gamma\theta^{\pm}$ and $\gamma\theta^{\pm}$

$$(2) \left. \begin{array}{l} 1+v \text{ odd} \\ 1+b \text{ even} \\ b < v \end{array} \right\} \mu, \chi \text{ have conductors with even exponents.}$$

$$\frac{(\mu\tau_{j,0})}{(\mu\tau_j)(\alpha_j)\phi(\alpha_j)} = \left(\frac{-2\gamma}{y}\right)\phi(\alpha_j \pi^v \gamma^2/2) \left(\sqrt{\left(\frac{-1}{p}\right)}\right)^f (-1)^{f-1}$$

Hence it is enough to show that

$$1 = \prod_{j=1}^{p-1} \left\{ \left(\frac{\gamma}{y}\right)\phi(\alpha_j \pi^v \gamma^2/2) \left(\sqrt{\left(\frac{-1}{p}\right)}\right)^f \right\}$$

But $\prod_{j=1}^{p-1} \gamma_j \equiv \gamma_0^{p-1} \int p(p-1)/2 = -\gamma_0^{p-1}$, whence the product of

the Legendre symbols involving the prime y , is $\left(\frac{-1}{p}\right)^f$. Furthermore $\left(\frac{-1}{y}\right)\left(\sqrt{\left(\frac{-1}{p}\right)}\right)^{p-1f} = \left\{\left(\frac{-1}{p}\right)^{1+(p-1)/2}\right\}^f = 1$ as is easily verified.

The product of the terms involving the character ϕ is 1 as

$$\sum_{j=1}^{p-1} \alpha_j \equiv 0 \pmod{y}.$$

(3) $\left. \begin{array}{l} 1+v \text{ odd} \\ 1+b \text{ odd} \\ b < v \end{array} \right\}$ 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) $\left. \begin{array}{l} 1+b \text{ odd} \\ b > v \end{array} \right\}$ Here all conductors have odd exponents.

$$\frac{(\mu, \theta^{\pm})}{\mu(\alpha)\phi^{\pm}(\alpha)} = \left(\frac{-2\gamma}{y}\right)\phi^{\pm}(\alpha \pi^b \gamma^2/2) \left(\sqrt{\left(\frac{-1}{p}\right)}\right)^f (-1)^{f-1}$$

$$\frac{(\mu \gamma_j \phi^*)}{(\mu \gamma_j) (\alpha_j) \phi^*(\alpha_j)} = \left(\frac{-2\gamma_j}{\gamma} \right) \overline{\phi}^*(\alpha_j \pi^b \gamma_j^2/2) \left(\sqrt{\left(\frac{-1}{p} \right)} \right)^f (-1)^f$$

$$\frac{(\chi \phi)}{\chi(\alpha') \phi(\alpha')} = \left(\frac{-2\gamma'}{\gamma} \right) \overline{\phi}(\alpha' \pi^b \gamma'^2/2) \left(\sqrt{\left(\frac{-1}{p} \right)} \right)^f (-1)^{f-1}$$

The product of all these expressions is again shown to be 1 by using the relations between the γ parameters to show that the product of all the Legendre symbols (both in p and in γ) 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) $b = v$ Here all the conductors have odd exponents. It is easily verified that "error" factor is the product, XZ , where

$$Z = \left(\frac{\gamma \gamma'}{\gamma} \right) \left(\sqrt{\left(\frac{-1}{p} \right)} \right)^{f(p-1)} \prod_{j=1}^{p-1} \left(\frac{-2\gamma_j}{\gamma} \right)$$

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

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

It has already been noted that $\left(\sqrt{\left(\frac{-1}{p} \right)} \right)^{p-1} = \left(\frac{-1}{p} \right)$. Certainly $(-2)^{p-1}$ is a square. The relations between the γ parameters for $b = v$ give:

$$\prod_{j=1}^{p-1} \gamma_j \equiv \gamma_0^{p-1} (s^{p-1} - 1) / \beta_0,$$

$$\prod_{j=1}^{p-1} \gamma_j^p \equiv \gamma_0^{p-1} (s^{p(p-1)} - 1) \equiv \gamma_0^{p-1} (s^{p-1} - 1)^p,$$

and discarding squares the product of the two lines is $-\gamma_0^p / \beta_0$. The assertion for Z now follows from $\gamma_0 \beta_0^p \equiv 1$. Expressing ϕ and ϕ in terms of θ^* , it is readily seen that $Y = \theta^*(W)$, where

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

The proof of the lemma is completed by showing that $2W = 0$.

It is first noted that $\eta_j/\eta_0 = \zeta^j + \theta^p \neq 0$, whence it follows

that θ is not a $(p-1)^{\text{st}}$ root of 1. Let $x_j = \eta_j \gamma_j^2/\eta_0$, also let

$$W^1 = \sum_{j=1}^{p-1} x_j. \quad \text{Then } x_j = (\zeta^j \gamma_0 + \theta^p \gamma)^2 / (\zeta^j + \theta^p) \text{ and it must be}$$

noted that x_j may be obtained from x_1 by replacing ζ with ζ^j .

$$\text{Furthermore } (\zeta^j + \theta^p)^{-1} = \theta^{-p} (1 + (\zeta^j/\theta^p))^{-1} = \theta^{-p} \frac{\sum_{i=0}^{p-2} (-\zeta/\theta^p)^i}{1 - \theta^p (p-1)(-1)}$$

It follows that $x_1 = \sum_{r=0}^{p-2} c_r \zeta^r$, 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 $W^1 = \sum_{j=1}^{p-1} \sum_{r=0}^{p-2} c_r \zeta^{rj} = \sum_{r=0}^{p-2} c_r \sum_{j=1}^{p-1} \zeta^{rj}$. The

inner sum is zero unless $\zeta^r = 1$, whence $W^1 = -c_0$. The remainder

of the computation of W is completely straightforward, 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 $t = \theta/\pi^{b-v}$, $z = -N(t)/t$, then $Q(X) = \varphi(\alpha, X)$,

where

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

Proof

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

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

$$\begin{aligned} A &= \varphi^{\dagger}(\alpha) \overline{\varphi}(\alpha') \varphi \left(\sum_{j=1}^{p-1} \alpha_j \right) && \text{if } b \leq v \\ &= \varphi^{\dagger}(\alpha) \overline{\varphi}(\alpha') \varphi^{\dagger} \left(\sum_{j=1}^{p-1} \alpha_j \right) && \text{if } b \geq v. \end{aligned}$$

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

Using the relation between φ and φ^{\dagger} , it follows that in any case

$$A = \overline{\varphi}(\alpha') \varphi(p \alpha \pi^{v-b}). \text{ Furthermore}$$

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

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

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 \mathbb{H} is somewhat

more lengthy. Direct computation shows that $\alpha \left[\prod_{j=1}^{p-1} \alpha_j \right] / \mathbb{H}(\alpha') = (1+\mathbb{H}\mathbb{H}) / \mathbb{H}(1+\mathbb{H})$, both for $b \leq v$ and for $b \geq v$. Furthermore $\prod_{j=1}^{p-1} \tau_j(\alpha_j) = \prod_{j=1}^{p-1} \tau_j(\alpha_j / \alpha_0)$, as $\prod_{j=1}^{p-1} \tau_j(\alpha_0) = \prod_{j=1}^{p-1} \tau^j(\alpha_0) = \tau(\alpha_0^{(p-1)/2}) = 1$.

$$\begin{aligned} \text{Also } \alpha_j / \alpha_0 &= s^j + \mathbb{H}t && \text{if } b \leq v \\ &= \pi^{b-v} (s^j + \mathbb{H}t) && \text{if } b \geq v. \end{aligned} \text{ As } \tau \text{ is trivial on the}$$

norm group, it follows that

$$\begin{aligned} \mathbb{H} &= \mu(Z^{\dagger}) \prod_{j=1}^{p-1} \tau_j(z_j), \text{ where } Z^{\dagger} = \mathbb{H}(1+Z) / (1+\mathbb{H}Z) \\ & \quad z_j = \mathbb{H}(t + s^j) / (s^j + \mathbb{H}t). \end{aligned}$$

With the aid of E.P.(7) it is readily shown that $\text{ord}_y(Z^{\dagger}-1) \geq b''$, whence $\mu(Z^{\dagger}) = \overline{\varphi}^{\dagger}(\alpha(Z^{\dagger}-1)) = \overline{\varphi}(\alpha_0 \mathbb{H}t(Z^{\dagger}-1))$. Likewise $\text{ord}_y(z_j-1) \geq v''$ (Note: v'', b'' are defined in the proof of Lemma 2), whence

$\zeta_j(x_j) = \overline{\varphi}(\alpha_0 a_j(x_j-1)) = \overline{\varphi}(\alpha_0 s^j(x_j-1))$ as $a_j \equiv s^j \pmod{p}$.
Collecting these results, M 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:

Lemma 8 $x \in \mathcal{O}_y^{1+v}$, and therefore $Q(X) = 1$ if $p \neq 2$.

Proof If $\text{ord}_y X \geq 1+v$, then the assertion concerning Q follows directly from the previous lemma. In the notation of the previous lemma, $X = S(t) + Nt(Z^t-1) + \sum_{j=1}^{p-1} s^j(x_j-1)$. 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 s^j for s , and therefore if the first term, $s(x_1-1)$, is written as a polynomial of degree $(p-2)$ in s , 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 $x_1-1 = \sum_{r=0}^{p-2} C_r s^r$, then $\sum_{j=1}^{p-1} s^j(x_j-1) = C_{p-2}(p-1)$ (where the coefficients, C_r , do not explicitly involve s). To determine C_{p-2} we write $x_1 = N(1+(t/s))/(1+N(t/s)) = (1+N(-t/s))^{p-1} \sum_{i=0}^{p-2} N(-t/s)^i \sum_{j=0}^p s^{(j)}(t/s)$ (where $s^{(p)}$ denotes N) $= (1-Nt^{p-1})^{-1} \sum_{i=0}^{p-2} \sum_{j=0}^p N(-t)^i s^{(j)}(t) s^{-(1+j)}$. The terms involving the $(p-2)^{\text{nd}}$ power of s are those terms for which either $1+j = 1$ or $1+j = p$. It follows that $C_{p-2} =$

$(1-Nt^{p-1})^{-1} \{ s(t) - N(t) + \sum_{i=0}^{p-2} N(-t)^i s^{(p-1)}(t) \}$. We now compute

$$\begin{aligned} Z^t N(t) &= Nt N(1-Z)/(1+NZ) = Nt N(1-(Nt/t))/(1-N(Nt/t)) \\ &= N(t - Nt)/(1-Nt^{p-1}) = -Nt^p(1-Nt^{p-1})^{-1} N(1-(t/Nt)) \\ &= -Nt^p(1-Nt^{p-1})^{-1} \sum_{i=0}^{p-1} s^{(i)}(-t/Nt) = -(1-Nt^{p-1})^{-1} \sum_{i=0}^{p-1} (-1)^i s^{(i)}(t) Nt^{p-1} \end{aligned}$$

Combining these results it is found that

$$X = p(1-Nt^{p-1})^{-1} \{ s(t) + \sum_{j=1}^{p-2} (-1)^j Nt^j s^{(p-j)}(t) \}$$
. Using E.P.(5), (6)

the lemma is immediately verified for $b \leq v$, as for $b < v$, $t \in \mathcal{F}$ while for $b = v$, $t = 0$ and it has already ^{been shown} that Nt 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 $p s(t) Nt^{1-p}$ and $p Nt^{1-j} s^{(j)}(t)$ ($2 \leq j \leq p-1$) lie in \mathcal{Y}^{1+v} .

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

$p = 2$

It is first shown that a result analogous to Lemma 6 holds.

Lemma 6': $\frac{Q(X)}{(\tau, \phi)} = FE$,

where

$$\begin{aligned} F &= \frac{\mu(\alpha)\phi'(\alpha)(\mu\tau)(\alpha_1)\phi(\alpha_1)}{\chi(\alpha')\phi(\alpha')\tau(\alpha_0)\phi(\alpha_0)} & \text{if } b < v \\ &= \frac{\mu(\alpha)\phi'(\alpha)(\mu\tau)(\alpha_1)\phi'(\alpha_1)}{\chi(\alpha')\phi(\alpha')\tau(\alpha_0)\phi(\alpha_0)} & \text{if } b \geq v. \end{aligned}$$

$$E = 1 \quad \text{if either } b < v, \text{ or } (1+b) \text{ even}$$

$$= \theta^1(\gamma) i^2 \quad \text{if } b > v, (1+b) \text{ odd}$$

$$= \theta^1(\gamma, \delta/(1+\delta)) \Delta^1(\delta/(1+\delta)) \quad \text{if } b=v, 1+b \text{ odd.}$$

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

a) For $b < v$, E^s is trivially 1 if both $1+b$ and $1+v$ are even, $\Delta^s(\gamma) \Delta^s(\gamma')$ if $1+v$ even, $\Delta^s(\gamma_1) \Delta^s(\gamma_0)$ if $1+v$ odd, and is $1+b$ odd $1+b$ even

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 $\Delta^s(x^2) = \Delta^s(x)$ if x lies in the residue class field. Hence $E^s = 1$ if $b < v$.

b) For $b > v$, $\gamma_1 \equiv \gamma$, $\gamma'^2 \equiv 1 + \gamma_0$, $1+v$ even $\Leftrightarrow 1+b$ even,

$1+b$ even \Rightarrow conductor of $\mu\tau$ has even exponent. Hence

$$\begin{aligned} E^s &= 1 \dots \dots \dots \text{if } 1+v \text{ and } 1+b \text{ are even} \\ &= \Delta^s(\gamma) \Delta^s(\gamma_1) \left(\frac{1+i}{\sqrt{2}}\right)^{2f} \quad \text{if } 1+v \text{ is even and } 1+b \text{ is odd.} \\ &= \overline{\Delta^s(\gamma')} \overline{\Delta^s(\gamma_0)} \left(\frac{1+i}{\sqrt{2}}\right)^{2f} \quad \text{if } 1+v \text{ is odd and } 1+b \text{ is even.} \\ &= \text{product of the two previous lines if both } 1+v \text{ and } 1+b \text{ are odd} \end{aligned}$$

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

c) For $b = v$, we may assume that v is even. Using equality in the sense of residue class fields, $\gamma'^2 = (1+\theta)^{-1}(\gamma + \gamma_0\theta + \theta + \sqrt{\theta})$,

$\gamma_1 = (1+\theta)^{-1}(\gamma_0 + \gamma\theta + \sqrt{\theta})$, whence $\gamma_1 + \gamma'^2 = \gamma + \gamma_0 + \theta(1+\theta)^{-1}$, which may be written: $\theta(1+\theta)^{-1} + \gamma + \gamma_1 = \gamma_0 + \gamma'^2$. Using the functional equation it follows that

$$\begin{aligned} E^s \Delta^s(\theta/(1+\theta)) &= \Delta^s(\gamma) \Delta^s(\gamma_1) \Delta^s(\theta/(1+\theta)) / [\Delta^s(\gamma_0) \Delta^s(\gamma')] \\ &= \theta^s (W + \theta(1+\theta)^{-1} \gamma_1), \text{ where } W = \gamma_0 \gamma'^2 + \gamma \gamma_1 + \gamma \theta(1+\theta)^{-1}. \text{ Straight-} \\ &\text{forward manipulation shows that } W = \pi + \pi^2, \text{ where } \pi = \frac{(\gamma_0 + \gamma)(\theta + \sqrt{\theta})}{1+\theta} \end{aligned}$$

and therefore $\theta^s(W) = 1$. The assertion follows directly.

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

Lemma 7'

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

where

$$X = S(t) + xH(t) + y$$

$$t = \delta \pi^{v-b}$$

$$\rightarrow Z = Ht/t$$

$$1+x = H(1+S)/(1+Ht)$$

$$1+y = H(1+t)/(1+Ht)$$

$$x^* = x/(\beta \pi^{b/2})$$

$$y^* = y/(\beta \pi^{v/2})$$

$$\sigma = 1 \quad \text{if either } b < v \text{ or } 1+b \text{ even}$$

$$= i^{\frac{b}{2}} \theta^*(\gamma) \Delta^*(x^*) \theta^*(\gamma x^*) \quad \text{if } b > v \text{ and } 1+b \text{ odd}$$

$$= \theta^*(\gamma, \delta/(1+\delta)) \Delta^*(\delta/(1+\delta)) \Delta^*(x^*) \theta^*(\gamma x^*) \Delta^*(y^*) \theta^*(\gamma y^*) \quad \text{if } b = v \text{ and } 1+b \text{ odd.}$$

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' $F = \varphi(\alpha, S(t)) \mu(1+x) \tau(1+y)$. It follows from our usual methods of estimation that

$$\text{ord } \frac{x}{\pi} \geq \begin{cases} b'' & \text{if either } b < v \text{ or } 1+b \text{ even} \\ b/2 & \text{if both } b \geq v \text{ and } 1+b \text{ odd} \end{cases}$$

$$\text{ord } \frac{y}{\pi} \geq \begin{cases} v'' & \text{if either } b \neq v \text{ or } 1+v \text{ even} \\ v/2 & \text{if both } b = v \text{ and } 1+v \text{ odd.} \end{cases}$$

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 $\tau(1+y)\varphi^*(\alpha, y) = \Delta^*(y^*)\theta^*(\gamma y^*)$, 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 6¹.

The computation is finally completed with:

Lemma 8¹ $\varphi(\alpha, X) \sigma = 1$, and therefore $Q(X) = (\tau, \varphi)$.

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

ord $X \geq 1+v$ if either $b \neq v$ or $(1+v)$ even
 $\geq v$ if $b = v$. As the conductor of φ has exponent $1+v$,
 it follows that (as $X = -2x$)

$$\varphi(\alpha, X) \sigma = 1 \quad \text{if } b < v \text{ or } 1+b \text{ even}$$

$$= i^f \theta^s(\gamma) \Delta^s(x^s) \theta^s(\gamma x^s) \quad \text{if } b > v \text{ and } 1+b \text{ odd.}$$

$$= \sigma \theta^s(\gamma 2x/\pi^v) \quad \text{if } b = v \text{ and } 1+v \text{ odd.}$$

For $b > v$ } We know that in any case $x = -S(t)/(1+Nt)$,
 $1+b \text{ odd}$ }

$t = \delta \pi^{v-b}$, 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) $x^s = 1$ and the proof is immediate.

For $b = v$ } Here $t = \delta$. Let $w = (\pi/\pi^2)^{v/2} \pi^v$, then
 $1+v \text{ odd.}$ }

$$2/\pi^{v/2} = S(w)/N(w), \quad S(t)\pi^{-v/2}(1+N\delta)^{-1} = (N\delta^{-1}+1)^{-1}S(\delta w)/N(\delta w).$$

Using E.P.(10) and the relations between the γ parameters, it follows that (again using equality in the sense of elements of

the residue class field) $x^t = \delta^2/(1+\delta^2)$, $\eta_0 28(t) \tau^{-v} (1+\delta t)^{-1} = \delta/(1+\delta^2) = y^t$. Consequently,

$$\varphi(\alpha, X) \sigma = \Delta^t(\delta/(1+\delta)) \overline{\Delta}^t(\delta^2/(1+\delta^2)) \overline{\Delta}^t(\delta/(1+\delta^2)) \theta^t(a_1), \text{ where}$$

$$a_1 = \gamma_0 \delta/(1+\delta) + \gamma_0 \delta^2/(1+\delta^2) + \gamma_0 \delta/(1+\delta^2) + \delta/(1+\delta^2).$$

But $\Delta^t(\delta^2/(1+\delta^2)) \overline{\Delta}^t(\delta/(1+\delta^2)) = \Delta^t((\delta+\delta^2)/(1+\delta^2)) \theta^t(\delta^3/(1+\delta^4))$, and $(\delta+\delta^2)/(1+\delta^2) = \delta/(1+\delta)$, whence

$$\varphi(\alpha, X) \sigma = \theta^t(a_2), \text{ where } a_2 = a_1 + \delta^3/(1+\delta^4) = (\text{upon substituting the expression for } \gamma_0 \text{ in terms of } \gamma, \gamma_0 \text{ and } \delta \text{ and simplifying})$$

$$\delta(1+\delta)^{-1} \{ (1+\sqrt{\delta})(1+\delta)^{-1} + \delta^2/(1+\delta^3) \} = a_3 + \delta(1+\sqrt{\delta})/(1+\delta)^2,$$

where $a_3 = \delta^3/(1+\delta^2)^2$ which has the same image under θ^t as its square root. Hence $\theta^t(a_2) = \theta^t(a_4)$, 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^t is the same as that of C^2 , it follows that $\theta^t(a_4) = 1$. This completes the proof of the lemma.

Summary

k a γ -adic number field, absolute degree of $\gamma = f$ absolute different of $k = \gamma^d$. 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 $\neq 1+m$, which is trivial on K_{II}^* then

$$(1) \text{ For } K/k \text{ unramified, } \theta_{K/k}(\chi) = (-1)^{d(n-1)} \quad (\text{valid for } n \text{ not prime})$$

(2) For K/k ramified, let π be a prime element of k which lies in the norm group. Then

(a) if $\eta \nmid n$

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

if $n = 2$

$$\left. \begin{aligned} &= 1 && \text{if } n = 0 \text{ or } -1 \\ &= \left(\frac{Np}{\pi}\right)^{1+n} && \text{if } n > 0 \end{aligned} \right\} \text{for } n \neq 2$$

(b) if $\eta \mid n$

$$\epsilon_{K/k}(\chi) = 1 \quad \text{if } n \neq 2$$

$$= (\tau, \psi_{\pi^{-d-1}}) \quad \text{if } n = 2$$

These results are now extended to the case in which K/k is abelian.

K/k Abelian

As the results for archimedean primes have already been determined, it may be assumed that the valuation is discrete. The notation is that introduced at the beginning of the chapter; specifically, χ is a quasi-character of K^* , of conductor \mathfrak{f}^{1+n} , which is trivial on K_H^* .

Theorem 1

- a) $Q_{K/k}(\chi) = \chi(n, K/k)$, a fourth root of unity depending only on the conductor (and the fields k, K)
 b) $(Q_{K/k}(\chi))^2 = \prod_{j=1}^n \gamma_j(-1)$.

Proof

We first show that the second assertion is a consequence of the first. Indeed, all that is needed is that $Q(\bar{\chi}) = Q(\chi)$ which is certainly true if the first statement is true.

(b) It follows from the explicit formula for $\rho_K(c)$ (where c is any quasi-character of k^*) that $\rho_K(\bar{c}) = c(-1) \overline{\rho_K(c)}$. Hence if μ is a quasi-character of k^* whose decomposition with $\mathbb{H}_{K/k}$ is χ , then $Q(\bar{\chi}) = \left[\prod_{j=1}^n \overline{\rho_K(\mu \gamma_j)} \right] / \overline{\rho_K(\chi)}$

$= \frac{Q(\bar{\chi})}{\chi(-1)} \prod_{j=1}^n (\mu \gamma_j)(-1)$. As $\chi(-1) = \mu(-1)^n$, it is clear that

(b) follows from (a).

(a) It has already been shown that the assertion is true if n is prime. We prove it in general by induction on the number of (not necessarily distinct) prime factors of n . For given n take as the induction hypothesis the statement that (a) is valid when-

over the

ever the number of prime factors is less than the number of prime factors of n . We may assume that n is not prime. Hence there exists an intermediate field, K^* , such that the degree of K/K^* is q , a non trivial divisor of n . (The proof does not require that q be prime.) Let μ be as defined in the proof of part (b) and let χ' be the quasi-character, $\mu \circ \mathbb{N}_{K^*/K}$, of K^* . Let $n^* = n/q$ be the degree of K^*/k , and let $(\sigma_j)_{j=1}^q$ be the group of characters of K^* which are trivial on $\mathbb{N}_{K/K^*} K^*$ and also let $(\delta_j)_{j=1}^{n^*}$ be the group of characters of k^* which are trivial on $\mathbb{N}_{K^*/k} K^*$. As this last group of characters is a subgroup of $(\tau_j)_{j=1}^n$ of index q , there exists q characters say, τ_1, \dots, τ_q such that

$$(\tau_j)_{j=1}^n = \bigcup_{s=1}^q \tau_s (\delta_j)_{j=1}^{n^*} \quad (\text{a disjoint union}).$$

In terms of the local norm rest symbol, for $x \in K^*$, $(x, K/K^*) = 1 \Leftrightarrow (\mathbb{N}_{K^*/K} x, K/k) = 1 \Leftrightarrow (\tau_j \circ \mathbb{N}_{K^*/K})(x) = 1$ for all j , $1 \leq j \leq n$. Hence as j runs through the integers $1, 2, \dots, n$, $\tau_j \circ \mathbb{N}_{K^*/K}$ runs through the group of characters of K^* which are trivial on $\mathbb{N}_{K/K^*} K^*$. As $\delta_j \circ \mathbb{N}_{K^*/K}$ is trivial on K^* , it follows that $(\tau_j \circ \mathbb{N}_{K^*/K})_{j=1}^q$ is the group of characters of K^* which are trivial on $\mathbb{N}_{K/K^*} K^*$ and therefore with a suitable choice of indices, $\sigma_s = \tau_s \circ \mathbb{N}_{K^*/K}$ for $1 \leq s \leq q$. Hence, $\rho_{K/k}(\chi) = (\rho_K(\chi))^{-1} \prod_{j=1}^n \rho_K(\mu \tau_j)$

$$= \frac{\prod_{j=1}^{n^*} \prod_{s=1}^q \rho_K(\mu \tau_s \delta_j)}{\rho_K(\chi)} =$$

$$\left[\frac{\prod_{s=1}^q \rho_{K'}(\sigma_s \chi')}{\rho_K(\chi)} \right] \prod_{s=1}^q \left[\frac{\prod_{j=1}^{n_s} \rho_{K'}((\mu_j) \sigma_j)}{\rho_{K'}(\chi' \sigma_s)} \right]$$

$= \rho_{K'/K}(\chi) \prod_{s=1}^q \rho_{K'/K}(\chi' \sigma_s)$. The set $(\chi' \sigma_s)_{s=1}^q$ of characters of K'^* is uniquely determined by the condition that the composition of each element of the set with $N_{K'/K}$ is χ . Let η be the prime of K' and $(\eta^{1+m_s})_{s=1}^q$ be the set of conductors of these characters. The set (m_1, \dots, m_q) is determined by m , for there exists unique integer b such that $m = g_{K'/K}(b)$ and (cf. Chapter I) $m_s = \text{Max}(b, t_s)$ for $1 \leq s \leq q$, where η^{1+t_s} is the conductor of σ_s . Applying the induction hypothesis we now have $\rho_{K'/K}(\chi) = \chi(m, K'/K) \prod_{s=1}^q \chi(\text{Max}(b, t_s), K'/K)$ whence the assertion follows. We have also proven:

Corollary

If K/k is abelian, m an integer admissible with respect to K/k , K' an intermediate field, $(1+s_j)_{j=1}^r$ the exponents of the group of characters of K'^* trivial on $N_{K'/K} K'^*$, where $r = \text{deg}(K'/K)$, then $\chi(m, K'/K) = \chi(m, K/K') \prod_{j=1}^r \chi(\text{Max}(b, s_j), K'/K)$ where $m = g_{K'/K}(b)$.

This permits the computation of $\chi(m, K/k)$ by reduction to cyclic fields of prime degree.

The next theorem will specify $(\chi(m, K/k))^2$ in terms of the norm group, $N_{K/k} K^*$. To simplify the proof we introduce the following notation: $x \rightarrow (x, K/k)^{n/2}$ is a homomorphism of k^* into $G(K/k)$ and the image is the trivial automorphism of K/k unless the 2-sylow subgroup of G is cyclic and non-trivial, in which case the image is the unique subgroup of order 2.

We identify $(x, K/k)^{n/(n,2)}$ with +1 if it is the neutral element of the Galois group, and with -1 if it is a non-trivial element. This being said, we assert:

Theorem 2

If K/k is abelian of degree n , $\alpha \in k^*$, then

$$\prod_{j=1}^n \tau_j(\alpha) = (\alpha, K/k)^{n/(n,2)} \quad \text{and therefore}$$

$$(\chi(n, K/k))^2 = (-1, K/k)^{n/(n,2)}.$$

Proof

If the group is cyclic then we may set $\tau_j = \tau^j$, whence the product is $\tau(\alpha^{n/2})$ if n is even and otherwise is 1. As $\tau(x) = 1 \Leftrightarrow (x, K/k) = 1$, the assertion follows for K/k cyclic and in particular for n prime. To prove the theorem in general, induction is used. Using the same notation and the same induction hypothesis as in the proof of the first part of Theorem I,

$$\begin{aligned} \prod_{j=1}^n \tau_j(\alpha) &= \prod_{s=1}^q \prod_{j=1}^{n^s} (\tau_s \delta_j)(\alpha) = \prod_{s=1}^q (\tau_s(\alpha)^{n^s} \prod_{j=1}^{n^s} \delta_j(\alpha)) \\ &= \left(\prod_{s=1}^q \sigma_s(\alpha) \right) \left(\prod_{j=1}^{n^s} \delta_j(\alpha) \right)^q \quad (\text{as } \sigma_s(\alpha) = (\tau_s \circ \Pi_{K^s/k})(\alpha)) \\ &= \tau_s(\alpha^{n^s}). \end{aligned}$$

Applying the induction hypothesis, it is found that the product under consideration is $(\alpha, K/K^s)^{q/(q,2)} (\alpha, K^s/k)^{qn^s/(2, n^s)}$. In completing the proof, the question of whether or not q is even must be considered.

(a) q even. Then $qn^s/(2, n^s)$ is a multiple of n^s , whence the second factor is 1. Also, $(\alpha, K/K^s)^{q/(q,2)} = (\Pi_{K^s/k} \alpha, K/k)^{q/2} = (\alpha, K/k)^{qn^s/2}$, which completes the proof if q is even.

(b) q odd. Certainly $(e, K/K^f)^{q/(q,2)} = 1$. Also $(n, 2) = (n^f, 2)$. Hence it is enough to show that $(e, K^f/k)^{n/(n,2)} = (e, K/k)^{n/(n,2)}$. If the right side is 1 then the left side is also 1 as if the two sides are considered as elements of galois groups the left side is the restriction to K^f of the right side. If the left side is one then there exists $x \in K^f$ such that $N_{K^f/k} x = e^{n/(n,2)}$, whence $N_{K/k} x = e^{qn/(n,2)}$, whence the q^{th} power of the right side is 1. But q is odd and the right side is $+1$ or -1 and therefore the right side is one. Hence the two sides are equal.

The final theorem of this chapter gives an almost complete specification of $\chi(m, K/k)$.

Theorem 3

If K is an abelian extension of k of degree n , relative ramification e , relative residue class degree f , let d be the exponent of the absolute different of k and let e' be the largest integral divisor of e which is relatively prime to $2p$ (y/p),

then

$$(a) \quad \frac{\chi(m, K/k)}{\chi(-1, K/k)} = \begin{cases} 1 & \text{if } m = 0 \\ \left(\frac{N_{K/k}}{e'}\right)^{1+m} & \text{if } m \neq 0 \end{cases}$$

(b) If $2 \nmid e$ then

$$\chi(-1, K/k) = (-1)^{e(f-1)d} \left(\frac{N_{K/k}}{e'}\right)$$

Proof

Let K_0 be the inertial subfield of K/k

K_1 be the first ramification subfield of K/k

K_0^f the largest field between K_1 and K_0 such that degree (

degree (K'_0/K_0) is a power of 2.

From the results for unramified extensions and the corollary to Theorem 1, it is clear that

$$\chi(m, K/k) = \chi(m, K/K_0) (-1)^{e(f-1)d}$$

therefore we may assume $k = K_0$. Furthermore from the results for cyclic extensions of degree 2 and the same corollary it follows that

$$\chi(m, K/K_0) = \chi(m, K/K'_0) (\chi(-1, K'_0/K_0))^{(K/K'_0)}$$

Hence the problem has been reduced to proving the theorem for:

K/k abelian, purely ramified, K_1 the first ramification subfield of K/k , $e' = K_1/k$, $2 \nmid e'$. We first assert

Contention:

The theorem is valid if $K = K_1$.

Proof

We are now considering the case K/k abelian, purely ramified of conductor γ . The proof is by induction. $e' = \deg K/k$.

If e' is prime then $\chi(m, K/k) = 1$ if $m = 0$ or -1

$$\left(\frac{N\gamma}{e'}\right)^{1+m} \text{ for } m > 0$$

while, $\mathcal{G}_{K/k} = \gamma^{e'-1} \Rightarrow \left(\frac{N\gamma_{K/k}}{e'}\right) = 1$ as $e'-1$ is even, whence the contention is correct if e' is prime.

If then e' is not prime, use induction on the number of prime divisors of e' , and let K' be an intermediate field such that $K/K' = q$, a prime. Then in the notation of the corollary (Theorem 1)

$s_1 = -1$, $s_j = 0$ for $j > 1$. Let $m = \mathcal{G}_{K/K'}(b)$ then

$$\chi(m, K/k) = \chi(m, K/K') \chi(\text{Max}(-1, b), K'/k) [\chi(\text{Max}(0, b), K'/k)]^{q-1}$$

$$= \chi(m, K/K') \chi(\text{Max}(-1, b), K'/k)$$

as $q-1$ is even.

If $m = 0$, $b = 0$

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

$$m > 0, b = \frac{m}{q}$$

$$\text{Hence } \chi(-1, K/k) = \chi(-1, K/K^*) \chi(-1, K^*/k)$$

$$\chi(0, K/k) = \chi(0, K/K^*) \chi(0, K^*/k)$$

$$\chi(m, K/k) = \chi(m, K/K^*) \chi\left(\frac{m}{q}, K^*/k\right) \text{ for } m \neq 0.$$

By induction hypothesis, $\chi(-1, K^*/k) = \left(\frac{N_{K^*/k}}{e'/q}\right) = 1$

We know that $\chi(-1, K/K^*) = 1$

Hence $\chi(-1, K/k) = 1 = \left(\frac{N_{K/k}}{e'/q}\right)$, which proves (b) for $K = K_1$.

As $\chi(0, K/K^*) = 1$, while by induction hypothesis $\chi(0, K^*/k) = 1$, it follows that $\chi(0, K/k) = 1$.

For $m > 0$, let η be the prime of K^* , then $N_{K^*/k} = N_{\eta}^2$ and $2/m$

$\Leftrightarrow 2/(m/q)$. Hence by the induction hypothesis, $\chi(m/q, K^*/k) =$

$$\left(\frac{N_{\eta}}{e'/q}\right)^{1+(m/q)} = \left(\frac{N_{\eta}^2}{e'/q}\right)^{1+m}, \text{ while we know that } \chi(m, K/K^*) = \left(\frac{N_{K^*/k}}{e'/q}\right)^{1+m}.$$

It follows that

$$\chi(m, K/k) = \left(\frac{N_{K/k}}{e'/q}\right)^{1+m} \text{ which completes the proof of}$$

the contention.

Returning to the more general case ($K \neq K_1$) (but K/k purely ramified, $2/\sigma^2$), let K_1 be the intermediate field in the corollary to Theorem 1. Then in the notation used there, $s_1 = -1, s_j > 0$ for $j > 1$. Letting $\mathcal{E}_{K/K_1}(b) = m$, we have

$$\chi(m, K/k) = \chi(m, K/K_1) \prod_{j=1}^{s/\sigma^2} \chi(\text{Max}(s_j, b), K_1/k).$$

From the computations for the cyclic case of prime degree, it is

clear that $\chi(m, K/K_1) = \chi(-1, K/k)$ and is actually 1 if K/K_1 is of odd degree (i.e. if either $p \neq 2$ or $K = K_1$).

Hence $\chi(m, K/k) = \chi(-1, K/K_1) \prod_{j=1}^{e/e'} \chi(\text{Max}(s_j, K_1/k))$.

If $m = 0$ then $b = 0$, whence

$$\chi(0, K/k) = \chi(-1, K/K_1) \chi(0, K_1/k) \prod_{j=2}^{e/e'} \chi(s_j, K_1/k)$$

while if $m = -1$ then $b = -1$, whence

$$\chi(-1, K/k) = \chi(-1, K/K_1) \chi(-1, K_1/k) \prod_{j=2}^{e/e'} \chi(s_j, K_1/k),$$

so that $\chi(0, K/k) = \chi(-1, K/k)$, as $\chi(0, K_1/k) = \chi(-1, K_1/k)$.

For any $m \neq 0$ we now have (for $g_{K/K_1}(b) = m$)

$$\begin{aligned} \frac{\chi(m, K/k)}{\chi(-1, K/k)} &= \prod_{j=1}^{e/e'} \left[\frac{\chi(\text{Max}(b, s_j), K_1/k)}{\chi(\text{Max}(-1, s_j), K_1/k)} \right] \\ &= \prod_{j=1}^{e/e'} \left[\frac{\chi(\text{Max}(b, s_j), K_1/k)}{\chi(s_j, K_1/k)} \right] = \prod_{j=1}^{e/e'} \left(\frac{N\mathbb{F}}{e'} \right)^{\text{Max}(b, s_j) - s_j} \\ &= \left(\frac{N\mathbb{F}}{e'} \right)^{1+m} \text{ which completes the proof of (a).} \end{aligned}$$

For (b), we may assume that $p \neq 2$ (as for $p = 2$, $2 \nmid e \Rightarrow K = K_1$ and this case has already been taken care of). We then have

$\chi(-1, K/K_1) = 1$, whence

$$\chi(-1, K/k) = \prod_{j=2}^{e/e'} \chi(s_j, K_1/k) = \left(\frac{N\mathbb{F}}{e'} \right)^{\sum_{j=1}^{e/e'} (1+s_j)} = \left(\frac{N\mathbb{F}_{K/K_1}}{e'} \right).$$

But $g_{K/k} = g_{K/K_1} g_{K_1/k}$ and $g_{K_1/k} = \frac{e-1}{2}$. As e' is odd it follows that $\left(\frac{N\mathbb{F}_{K/k}}{e'} \right) = 1$, which completes the proof of the theorem.

Chapter IV

The Weil L-Series

§1. Some Group-theoretical Results

Note: Many of the results of this section appear in the writings of Mackey, (10), Shoda, (11), Taketa, (12). In particular, Taketa has given a slightly weaker form of lemma 7. (below). The analogue of the Frobenius Reciprocity Law for characters of an infinite group which are induced by characters of a subgroup of finite index, which is used several times in the following, is proven in Mackey's article.

- (10) Mackey, G., "On induced representations of groups", Amer. Jour. of Math, 1951 (73).
- (11) Shoda, K., "Über die monomialen Darstellungen Endlichen Gruppe", Proceedings of the Physico-Mathematical Society of Japan, 1933 (15).
- (12) Taketa, K., "Über die Gruppen deren Darstellungen sämtlich auf monomiale gestalt transformieren lassen", Proceedings of the Imperial Academy of Japan, 1930 (6).

In the following let G be a group, H an invariant subgroup, the index not necessarily finite, χ a character of G (as usual we restrict character to refer to a bounded matrix representation). If δ is a character of H and $x \in G$ then $h \rightarrow \delta(xhx^{-1})$ is also a character of H , which we shall call the x conjugate of δ and denote by δ^x . The set of all $(\delta^x)_{x \in G}$ may be referred to as the set of G conjugates of δ .

Lemma 1 If δ is an irreducible character of H occurring in X_H , the restriction of X to H , then every conjugate of δ occurs in X_H the same number of times as δ . The set G_δ of all $x \in G$ such that $\delta^x = \delta$ is a subgroup of G containing H and of index in G equal to the number of distinct conjugates of δ . The conjugates of δ correspond to the right cosets of G_δ . Finally $G_{\delta^x} = x^{-1}(G_\delta)x$.

Proof For $x, y \in G$, $(\delta^x)^y(h) = \delta^x(yhy^{-1}) = \delta(xyhy^{-1}x^{-1}) = \delta^{xy}(h)$ for all $h \in H$, i.e. $(\delta^x)^y = \delta^{xy}$. It follows immediately that G_δ is a subgroup of G containing H . If δ occurs in X_H , n times then for $x \in G$, δ^x occurs in X_H^x at least n times (as δ^x is also irreducible). But $X_H^x = X_H$, hence δ^x occurs in X_H at least n times. As δ is a conjugate of δ^x , δ occurs at least as often as δ^x whence δ^x occurs exactly n times. It follows that δ has only a finite set of distinct conjugates. For $x, y \in G$, $\delta^x = \delta^y \Leftrightarrow \delta^{xy^{-1}} = \delta \Leftrightarrow xy^{-1} \in G_\delta \Leftrightarrow x \in G_\delta y$, which shows that there exists a one to one correspondence between the right cosets of G_δ in G and the distinct conjugates of δ . Finally $(\delta^x)^y = \delta^x = \delta^{xyx^{-1}} \in G_\delta$, whence $G_{\delta^x} = x^{-1}(G_\delta)x$.

Lemma 2 If X is irreducible and δ is an irreducible character of H which occurs in the restriction, X_H , of X to H and if either

1) $(G:H)$ is finite

or 2) δ is of degree 1

then X_H is the sum of conjugates of δ .

Proof

1) If $(G:H)$ finite, let t_1, \dots, t_s be a set of representatives

of distinct right cosets of H in G . Let X_G be the character of G induced by δ . Then X_G contains X , but the restriction of X_G to H is simply $\sum_{i=1}^s \delta^{h_i}$ which proves the assertion.

2) If δ is of degree 1, let $\delta_1, \dots, \delta_s$ be the distinct G conjugates of δ ; by lemma 1 they all occur the same number of times. Let V be the representation space of a representation ρ of G whose character is X . Let $V_i (i=1, 2, \dots, s)$ be the set of all $v \in V$ such that $\rho(h)v = \delta_i(h)v$ for all $h \in H$. Let the direct sum of the V_i be W . Let $v \in V_1$, $x \in G$ then for all $h \in H$, $\rho(h)(\rho(x)v) = \rho(hx)v = \rho(x)(\rho(x^{-1}hx)v) = \rho(x)(\delta(x^{-1}hx)v) = \delta^{x^{-1}}(h)(\rho(x)v)$. As $\delta^{x^{-1}}$ is a conjugate of δ , there exists $i (1 \leq i \leq s)$ such that $\delta^{x^{-1}} = \delta_i$, whence $\rho(x)V_1 \subset V_i$, i.e. $\rho(x)V_1 \subset W$. It follows that $\rho(x)W \subset W$, i.e. W is a subspace of V invariant under ρ . As ρ is irreducible, W must be V .

Corollary For X irreducible, if the restriction of X to H contains the principal representation of H then it contains only the principal representation.

Lemma 3 Under the conditions of lemma 2, X is induced by an irreducible character σ of G_δ . The restriction of σ to H contains only δ .

Proof

The restriction of X to G_δ must contain an irreducible character σ of G_δ with the property that the restriction of σ to H contains δ . By lemma 2, the restriction of σ to H contains only G_δ conjugates of δ , i.e. just δ , say m times. We assert that X is induced by σ . Let X_G be the character of G induced by σ . Certainly

χ occurs in X_G and therefore it is enough to show that the degrees are equal. Let $r = (G:G_\theta)$, then $X_G(1) = r\theta(1) = r\theta(1)$. But by Lemma 1, r is the number of distinct G conjugates of θ . As θ occurs in the restriction of X to G_θ , and θ occurs n times in the restriction of σ to H , we may conclude that θ occurs at least n times in the restriction of X to H . Each G conjugate of θ must therefore also occur at least n times, whence $X(1) \geq r\theta(1) = X_G(1)$ which proves that X and X_G are of the same degree.

Lemma 4 If $(G:H)$ is finite, and θ an irreducible character of H and X_θ the character of G induced by θ then X_θ is irreducible if and only if $H = G_\theta$. If in addition H is abelian then all irreducible characters of G of degree $(G:H)$ are induced by irreducible characters θ of H for which $H = G_\theta$.

Proof

If X_θ is irreducible then by the induced character theorem, θ occurs just once in the restriction of X_θ to H . Hence each conjugate of θ occurs just once. By Lemma 2, only conjugates of θ occur. If r is the number of conjugates then $X_\theta(1) = r\theta(1)$. But $X_\theta(1) = (G:H)\theta(1)$. Hence $(G:H) = (G:G_\theta)$, whence $G_\theta = H$.

Conversely if $G_\theta = H$, then θ has $(G:H)$ distinct G conjugates. Among the irreducible characters of G occurring in X_θ , there must be one, X , whose restriction to H contains θ . X irreducible implies each conjugate of θ occurs in this restriction. Hence $X(1) \geq (G:H)\theta(1) = X_\theta(1) \geq X(1)$, whence $X_\theta = X$.

If H is abelian and X irreducible character of G of degree $(G:H)$, let θ be an irreducible character of H appearing in the

restriction of χ to H . Then δ is of degree 1, whence the character of G induced by δ is of degree $(G:H)$ and contains χ and therefore is χ . It follows from the above that δ must have $(G:H)$ distinct conjugates, whence $H = G_\delta$.

Lemma 5 If H is abelian and G/H cyclic, χ irreducible character of G and δ an irreducible character of H contained in the restriction of χ to H , then χ is induced by a character φ of G_δ of degree one.

Proof

By Lemma 3, χ is induced by an irreducible character φ of G_δ whose restriction to H is just $\varphi(1)\delta$ (as δ is of degree 1). Let n be the degree of φ , then there exists a unitary matrix representation, ρ , of G_δ and character φ such that for all $h \in H$, $\rho(h) = \delta(h)I_n$, I_n being the unit matrix of rank n . It follows that $\rho(H)$ lies in the center of $\rho(G_\delta)$. G/H cyclic $\Rightarrow G_\delta/H$ cyclic $\Rightarrow \rho(G_\delta)/\rho(H)$ cyclic; whence $\rho(G_\delta)$ is a cyclic group extension of its center and therefore must be an abelian group of unitary matrices, but it is also irreducible and therefore the degree must be one.

Lemma 6 Under the conditions of Lemma 5, if G' is any subgroup of G which contains H and φ' is a character of degree 1 of G' which induces χ then $G' = G_\delta$ and there exists an inner automorphism σ of G such that $\varphi' = \varphi \circ \sigma$.

Proof

As G/H is cyclic every subgroup of G containing H is an invariant subgroup of G . In particular then G' and G_δ are invariant

subgroups of G . The restriction of X to G' contains φ' and therefore the restriction of φ' to H is a character of H of degree one which occurs in the restriction of X to H , whence the restriction of φ' to H is δ' , a conjugate of δ . It follows that there exists an inner automorphism σ of G such that X is induced by the character, $\varphi' \circ \sigma^{-1}$, of $\sigma(G') = G'$; this character is of degree one and its restriction to H is δ . Hence we may assume that the restriction of φ' to H is δ . For $x \in G'$, $h \in H$, $\delta^x(h) = \delta(xhx^{-1}) = \varphi'(xhx^{-1}) = \varphi'(h) = \delta(h)$, whence $G' \subset G_\delta$. But by Lemma 5, $(G:G_\delta) = X(1) = (G:G')$, whence $G' = G_\delta$. By Lemma 2, the restriction of X to G_δ contains only conjugates of φ and therefore the assertion follows.

Lemma 7 If X is irreducible and H is abelian and there exists a sequence of intermediate groups, invariant in G , $G = G_0 \supset G_1 \supset G_2 \supset \dots \supset G_n = H$ such that G_j/G_{j+1} is cyclic ($j=0, 1, \dots, n-1$) and δ is an irreducible character of H appearing in the restriction of X to H then there exist a character φ of degree 1 of a group lying between G_δ and H such that φ induces X .

Note: 1) If $(G:H)$ is finite then the condition may be stated: the prime factor groups of the principal series of G/H are cyclic. This condition is stronger than the condition that G/H is solvable. If G/H is solvable then we may only conclude that the prime factor groups are direct products of isomorphic cyclic groups of prime order (of Sperser, Gruppentheorie, 3rd edition Satz 32, 33). Taketa has given an example of a solvable group of order 24 (a group with the quaternion group as invariant subgroup of index 3)

for which the conclusions of this lemma do not hold.

Proof

As the assertion is known to be true for $n = 1$, i.e. for G/H cyclic, we may apply induction on n and assume that the assertion is valid if the chain is of length $n-1$. By lemma 3, X is induced by an irreducible character σ of G_0 whose restriction to H contains only δ . Let $G_j^! = G_j \cap G_0$ ($0 \leq j \leq n$), then $G_0 = G_0^! > G_1^! > \dots > G_n^! = H$ and the sequence has the property: $G_j^!$ invariant in $G_0^!$, $G_j^!/G_{j+1}^!$ cyclic. There exists a matrix representation ρ of $G_0^! = G_0$, corresponding to the character σ such that for $h \in H$, $\rho(h) = \delta(h) I_m$, where $m = \deg \sigma$ and I_m is the unit matrix of rank m . Let $C_j = \rho(G_j^!)$ ($0 \leq j \leq n$), then $\rho(H) = C_n$ abelian, C_j invariant subgroup of C_0 and C_j/C_{j+1} cyclic. Clearly C_n lies in the center of C_0 , while C_{n-1}/C_n is cyclic, whence C_{n-1} is abelian. Let $\bar{\sigma}$ be the character $x \rightarrow \text{Tr } x$ of C_0 , then $\sigma = \bar{\sigma} \circ \rho$ and $\bar{\sigma}$ is irreducible. Then $C_0 > C_1 > \dots > C_{n-1}$ is a chain of length $n-1$ to which the induction hypothesis applies, hence $\bar{\sigma}$ is induced by a character $\bar{\varphi}$ of degree 1 of a subgroup \bar{g} of C_0 which contains C_{n-1} . Let $g = \bar{\rho}^{-1}(\bar{g})$, φ the character $\bar{\varphi} \circ \rho$ of g . We assert that X is induced by the character φ of g . We note that φ is of degree 1, that g contains the kernel of ρ and also g contains H . Clearly $(C_0 : \bar{g}) = \deg \bar{\sigma}$. Hence $C_0 = \bigcup_{j=1}^m \bar{g}c_j$ (where $m = \deg \bar{\sigma}$), a disjoint union. There exists $d_j \in G_0^!$ such that $\rho(d_j) = c_j$ ($1 \leq j \leq m$) and therefore $G_0^! = \bar{\rho}^{-1}(C_0) = \bigcup_{j=1}^m gd_j$, also a disjoint union as $gd_j \cap gd_{j'} = \emptyset$ implies $c_{j'} = \bar{g}^{-1}c_j$. For $z \in C_0$

$$\bar{\sigma}(x) = \sum_{j=1}^m \bar{\varphi}(c_j x c_j^{-1}), \text{ whence for } x \in G_0, \sigma(x) = \bar{\sigma}(\rho(x))$$

$$= \sum_{j=1}^m \bar{\varphi}(c_j \rho(x) c_j^{-1}) = \sum_{j=1}^m (\bar{\varphi} \circ \rho)(d_j x d_j^{-1}) = \sum_{j=1}^m \varphi(d_j x d_j^{-1}).$$

It follows that σ is induced by the character φ of g . But the character σ of G_0 induces X and by the transitivity law for such relations, X is induced by φ which completes the proof.

§2. Let K be a finite normal extension of an algebraic number field k . Let C_K be the group of idele classes of K . $W_{K/k}$, the group extension of C_K by the galois group, $G(K/k)$, corresponding to the canonical cohomology class has been extensively studied by Weil, (6), and for that reason the group has been referred to as the Weil group. If \mathfrak{y} is a prime of k , $k_{\mathfrak{y}}$, the corresponding completion of k , then we define, $W_{K_{\mathfrak{y}}/k_{\mathfrak{y}}}$, (local Weil group), to be the group extension of $(K_{\mathfrak{y}})^*$ by $G(K_{\mathfrak{y}}/k_{\mathfrak{y}})$ corresponding to the local canonical cohomology class. It is known that this group may be identified with a decomposition subgroup of $W_{K/k}$ at \mathfrak{y} , a subgroup which is unique to within inner automorphisms of $W_{K/k}$. This decomposition subgroup is a group extension of V by $G_{\mathfrak{y}}$, V being one of the natural images in C_K of $(K_{\mathfrak{y}})^*$ and $G_{\mathfrak{y}}$ being the corresponding decomposition subgroup of $G(K/k)$.

If $W_{K/k}$ is a local Weil group at a discrete prime, \mathfrak{y} , χ a character, H the inertial subgroup and t an element in the Frobenius class then we define a local zeta function, $Z(s, \chi, K/k)$, by setting: $\log Z(s, \chi, K/k) = \sum_{n > 0} (n \ N \ \gamma^{ns})^{-1} \int_H \chi(xt^n) dx$, for $\text{Re } s > 0$, where dx is the Haar measure of H normalized so that the measure of H is 1. As the Frobenius class is a coset of H , the definition is independent of the choice of t . Trivially, $Z(s, \chi + \chi', K/k) = Z(s, \chi, K/k) Z(s, \chi', K/k)$. Let χ be irreducible and ρ a unitary matrix representation of $W_{K/k}$ whose character is

(6) Weil, A., "Sur la Theorie du Corps de Classes", J. Math. Soc. of Japan, vol 3 (1951)

X then as H is compact, by suitable choice of ρ , $\int_H \rho(x) dx$ is a matrix, all of whose elements are zero except for r diagonal elements which are unity, where r is the number of times the trivial representation of H occurs in the restriction of ρ to H . Lemma 2. (§1) shows that r is either 0 or $\deg X$. If the latter, then ρ is trivial on H and therefore $\rho(W_{K/k})$ is an irreducible cyclic group of unitary matrices, whence $r = 1$. As $\int_H X(xt^n) dx$ is the trace of $\rho(t^n) / \int_H \rho(x) dx$, it follows that for X irreducible, the zeta function is 1 unless X is of degree 1 and trivial on H , in which case it is $(1 - X(t) N \eta^{-s})^{-1}$ for $\text{Re } s > 0$.

If $W_{K/k}$ is a local Weil group at an archimedean prime the local zeta function $Z(s, X, K/k)$ is defined to be 1. In any case the local zeta function has an obvious analytic continuation.

If $W_{K/k}$ is a global Weil group and X is a character then the Weil L -series is defined to be:

$$L(s, X, K/k) = \prod_{\mathfrak{y}} Z(s, X_{\mathfrak{y}}, K_{\mathfrak{y}}/k_{\mathfrak{y}}) \quad \text{for } \text{Re } s > 1,$$

the product being taken over all primes of k , and $X_{\mathfrak{y}}$ being the restriction of X to the local Weil group, $W_{K_{\mathfrak{y}}/k_{\mathfrak{y}}}$. As X is invariant under inner automorphisms, the local zeta functions which appear are well defined. It is readily shown that for fixed s the mapping, $F: X \rightarrow L(s, X, K/k)$, of characters of $W_{K/k}$ into the complex plane has the properties:

(I) If X, X^{\dagger} are characters of $W_{K/k}$ then $F(X+X^{\dagger}, K/k) = F(X, K/k) F(X^{\dagger}, K/k)$.

(II) If L is an intermediate field, ϕ a character of $W_{K/L}$, X_{ϕ}

the induced character of $W_{K/k}$ then

$$F(\varphi, K/L) = F(X_{\varphi}, K/k) \quad (\text{Induced character property})$$

(III) If θ is a character of G_K , X the character of $W_{K/k}$ obtained by composing θ with the transfer homomorphism of $W_{K/k}$ into G_K (a mapping onto G_K) then $F(\theta, K/k) = F(X, K/k)$.

(IV) If L is an intermediate field, normal over k , X a character of $W_{L/k}$, $t_{K/k} \rightarrow L/k$ the homomorphism of $W_{K/k}$ onto $W_{L/k}$ described by Weil then

$$F(X, L/k) = F(X \circ t_{K/k} \rightarrow L/k, K/k).$$

By means of the first three properties and an extension of Brauer's theorem to characters of the Weil group, Weil proved that his L-series is a product of Hecke L-series and therefore is a meromorphic function in s . By extending the Artin conductor to characters of the Weil group it will be easy to extend the functional equation of the Artin L-series to a functional equation of the Weil L-series. A more difficult problem is that of decomposing the root number appearing in this functional equation into root numbers depending upon the local behavior of the global character. It will be shown that this problem may be reduced to the problem of extending in a specified manner ρ_K , Tate's function on local quasi-characters (which may be interpreted with s fixed as a function on local characters) to a function defined on the characters of local Weil groups.

§3.

For simplicity we shall refer to the properties I - IV of the previous section as the Artin conditions. We are interested in mappings $F_\gamma : X_\gamma \rightarrow F_\gamma (X_\gamma, W_{K_\gamma/k_\gamma})$ of local characters (i.e. of characters of local Weil groups) into the complex plane which have the property that if γ_0 is some fixed prime of some lower field k_0 then the function on global characters:

$$F(X, K/k) = \prod_{\gamma/\gamma_0} F_\gamma (X_\gamma, W_{K_\gamma/k_\gamma}) \quad (A)$$

satisfies the Artin conditions (X_γ being related to X as defined in the previous section).

This product is not well defined unless $F_\gamma (X_\gamma, W_{K_\gamma/k_\gamma})$ has the property of being independent of the choice of replica of W_{K_γ/k_γ} as decomposition subgroup of γ in $W_{K/k}$. Interpreting the Artin conditions as conditions on a mapping F of local characters into the complex plane, (with G_K replaced by K^*) we are thus led to the following (local) condition which is certainly satisfied if $F(X, K/k)$ is defined by intrinsic properties.

(V) K, K' isomorphic normal extensions of a local number field k , σ an isomorphism of K onto K' leaving each element of k fixed, then certainly σ may be considered as an isomorphism of $W_{K/k}$ with $W_{K'/k}$. If X' is a character of $W_{K'/k}$ then the condition is that

$$F(X', K'/k) = F(X' \circ \sigma, K/k).$$

We assert that the local Artin conditions I-V for the local functions F_γ imply that the global function F , defined by formula (A)

satisfies the global Artin conditions I - IV. Except for the induced character property the proof is immediate. The proof of the assertion then follows from the following lemma.

Lemma k an algebraic number field, K a normal extension of finite degree, L an intermediate field, φ a character of $W_{K/L}$, χ the induced character of $W_{K/k}$, γ a prime of k , $\gamma_1, \dots, \gamma_r$ the extensions of γ to L and \mathcal{P}_1 an extension of γ_1 to K . Let $W_{K/L}^{(1)}$ be a decomposition subgroup of $W_{K/k}$ at \mathcal{P}_1 and then $W_{K/L}^{(1)} = W_{K/L} \cap W_{K/k}^{(1)}$

is a decomposition subgroup of \mathcal{P}_1 in $W_{K/L}$. Let t_1, \dots, t_r be representatives in $W_{K/k}$ of elements of $G(K/k)$ which permute the primes $\mathcal{P}_1, \dots, \mathcal{P}_r$ transitively. Let φ_1 be the restriction of φ to $W_{K/L}^{(1)}$ and χ_1 the character of $W_{K/k}^{(1)}$ induced by φ_1 . Then

$t_i W_{K/k}^{(1)} t_i^{-1} = W_{K/k}^{(1)}$ ($1 \leq i \leq r$), and for $w \in W_{K/k}^{(1)}$ we have $\chi(w) =$

$$\sum_{i=1}^r \chi_1(t_i w t_i^{-1}).$$

Proof

Let U be the galois group of K/L , then $G = G(K/k) = \bigcup_{i=1}^r \bigcup_{j=1}^{n_i} U z_{ij} b_j$ where $b_j \mathcal{P}_1 = \mathcal{P}_j$, $n_i = \deg(L \mathcal{P}_i / k \gamma)$, and $(z_{ij})_{j=1, \dots, n_i}$ are representatives of the right cosets of the decomposition subgroup of \mathcal{P}_1 in U in the decomposition subgroup of \mathcal{P}_1 in G . The t_i are chosen so as to lie in the class modulo G_K corresponding to b_i . Pick $(s_{ij})_{j=1, \dots, n_i}$ such that $s_{ij} \in W_{K/k}^{(1)}$ and such that z_{ij} corresponds to the class of s_{ij} modulo G_K . Then $W_{K/k} = \bigcup_{i=1}^r \bigcup_{j=1}^{n_i} W_{K/L} s_{ij} t_i$, whence for $w \in W_{K/k}$

$$X(w) = \sum_{i=1}^n \sum_{j=1}^{n_i} X(s_{ij} t_i w t_i^{-1} s_{ij}^{-1}). \text{ But for } w_1 \in \mathbb{N}_{k/k}^{(1)}$$

$$X_1(w_1) = \sum_{j=1}^{n_1} \varphi_1(s_{1j} w_1 s_{1j}^{-1}) \text{ while for } w \in \mathbb{N}_{k/k}^{(1)}$$

$$t_1 w t_1^{-1} \in \mathbb{N}_{k/k}^{(1)} \text{ whence } X_1(t_1 w t_1^{-1}) = \sum_{j=1}^{n_1} \varphi_1(s_{1j} t_1 w t_1^{-1} s_{1j}^{-1})$$

which proves the lemma.

§4. The Functional Equation

If θ is an irreducible character of G_k then the Weil L-series, $L(s, \theta, k/k)$, coincides with Hecke's and its functional equation may be expressed as:

$$L(s, \theta, k/k) C(s, \theta, k/k) A(s, \theta, k/k) W(\theta, k/k) =$$

$$L(1-s, \bar{\theta}, k/k) C(1-s, \bar{\theta}, k/k) A(1-s, \bar{\theta}, k/k),$$

where $f(\theta, k/k) =$ conductor of θ

$W(\theta, k/k)$ is a unimodular complex number

$$A(s, \theta, k/k) = (d_k \prod_{\mathfrak{p} \in \mathbb{Q}} f(\theta, k/k)^{s/2}), \quad \mathbb{Q} = \text{field of rational numbers}$$

$n =$ absolute degree of k

$d_k =$ absolute discriminant of k

$$C(s, \theta, k/k) = \prod_{\mathfrak{p} \in \mathbb{P}_n} \gamma(s, \theta_{\mathfrak{p}}, k_{\mathfrak{p}}/k_{\mathfrak{p}})$$

$\theta_{\mathfrak{p}} =$ restriction of θ to the natural image of $k_{\mathfrak{p}}^*$ in G_k

and

$$\gamma(s, \theta_{\mathfrak{p}}, k_{\mathfrak{p}}/k_{\mathfrak{p}}) = \Gamma((s+it_{\mathfrak{p}})/2) \pi^{-s/2} \text{ if } \mathfrak{p} \text{ real, and } \theta_{\mathfrak{p}}(x) = |x|^{it_{\mathfrak{p}}}$$

$$= \Gamma((1+s+it_{\mathfrak{p}})/2) \pi^{-s/2} \text{ if } \mathfrak{p} \text{ real, and } \theta_{\mathfrak{p}}(x) = |x|^{it_{\mathfrak{p}}} (\text{sign } x)$$

$$= \pi^{-s} \Gamma((s+it_{\mathfrak{p}} + |a_{\mathfrak{p}}|)/2) \Gamma((1+s+it_{\mathfrak{p}} + |a_{\mathfrak{p}}|)/2),$$

if \mathfrak{p} complex and $\theta_{\mathfrak{p}}(\text{re } \theta) = x^{2it_{\mathfrak{p}}} e^{i2a_{\mathfrak{p}}}$
($t_{\mathfrak{p}}$ real, $2a_{\mathfrak{p}}$ an integer).

From Weil's extension of Brauer's theorem to characters of Weil groups it follows that the functional equation of the Weil L series, $L(s, X, K/k)$, X a character of the global Weil group $W_{K/k}$ is

$$L(s, X, K/k) C(s, X, K/k) A(s, X, K/k) W(X, K/k) =$$

$$L(1-s, \bar{X}, K/k) C(1-s, \bar{X}, K/k) A(1-s, \bar{X}, K/k)$$

where $W(X, K/k)$ is a unimodular complex number, provided that we may define $C(s, X, K/k)$, and $A(s, X, K/k)$ as functions on characters of Weil groups which satisfy the Artin conditions and in addition assume the form indicated above in the special case when $\begin{cases} X \text{ of degree } 1 \\ K = k. \end{cases}$ (It is already known that $L(s, X, K/k)$ has this property). We consider the gamma function factors and the term involving the conductor separately.

a) Conductor Factor

The conductor of a character of a local Weil group has already been defined. The γ inertial subgroup of $W_{K/k}$ is a group extension of the units of $(K/k_\gamma)^*$ by the inertial subgroup of $G(K_\gamma/k_\gamma)$. As almost all primes of k are unramified in K it follows that for almost all γ the inertial subgroup is just the group of units of $(K/k_\gamma)^*$. The restriction of X to G_X is a finite sum of characters of degree 1 and at almost all primes these characters are unramified. It follows that X is just $X(1)$ on almost all inertial subgroups of $W_{K/k}$. We now define the conductor of X to be

$f(X, K/k) = \prod_\gamma f(X_\gamma, K_\gamma/k_\gamma)$, the product being taken over all discrete primes of k , X_γ being the restriction of X to the local Weil group W_{K_γ/k_γ} and $f(X_\gamma, K_\gamma/k_\gamma)$ being the con-

ductor of X_γ as defined in Chapter I. The global conductor is well defined as by the above argument the local contribution is just 1 for almost all primes and because the local conductor is defined by intrinsic properties. Deviating slightly from Artin, we now set:

$$A(s, X, K/k) = (d_K^{X(1)} \prod_{K/Q} f(X, K/k))^{s/2}$$

Certainly this assumes the desired form when $K = k$, $\deg X = 1$. To verify conditions I-IV, it is enough to consider the expression within the brackets, i.e. $A(X, K/k) = \prod_\gamma A(X_\gamma, K_\gamma/k_\gamma)$,

where $A(X_\gamma, K_\gamma/k_\gamma) = d_{k_\gamma}^{X_\gamma(1)} \prod_{K_\gamma/Q_p} f(X_\gamma, K_\gamma/k_\gamma)$, d_{k_γ} being

the discriminant of k_γ . As this function on local characters has been shown to satisfy the local Artin conditions, it follows that $A(s, X, K/k)$ has the desired global properties.

b) Gamma Function Factors

For these terms it is enough to extend the functions, γ , defined above for characters of R^* and C^* to characters of the local Weil group, $W_{C/R}$. (R the field of real numbers and C the field of complex numbers). If X is an irreducible character of $W_{C/R}$ then it is contained in the character of $W_{C/R}$ induced by any of the irreducible characters of C^* appearing in the restriction of X to C^* . Hence X is at most of degree 2. If X is linear then it is trivial on the commutator subgroup and therefore may be obtained by transfer from a linear character of R^* . If X is of degree 2 then (Lemma #, §1) it is induced by a linear char-

acter, δ , of G^* which is not invariant under the galois group, $(1, \sigma)$, of G/R and therefore the restriction of X to G^* is $\delta + \delta^\sigma$. Hence δ^σ also induces X but no other character of G^* has this property. It follows that if X is linear then we may define $\gamma(s, X, G/R) = \gamma(s, \delta, R/R)$, where δ is the character of R^* from which X is obtained by transfer, while if X is irreducible of degree 2 we define $\gamma(s, X, G/R) = \gamma(s, \delta, G/C)$, where δ is a character of G^* which induces X . In this second case,

$\gamma(s, \delta, G/C) = \gamma(s, \delta^\sigma, G/C)$ and therefore in any case $\gamma(s, X, G/R)$ is well defined if X is irreducible and this definition may be extended to reducible characters in the manner suggested by condition I. It is immediate that only condition II, the induced character relation, requires verification. For this it is enough to let δ be a linear character of G^* which is invariant under σ . We may set $\delta(x e^{i\theta}) = x^{2iv}$, v real. Then X , the character induced by δ is reducible and is readily seen to be $X_1 + X_2$, X_j is obtained by transfer from the character, e_j , of R^* ($j = 1, 2$), e_1 being the character $x \mapsto |x|^{iv}$, e_2 being the character $x \mapsto |x|^{iv}(\text{sign } x)$, whence by definition

$\gamma(s, X, G/R) = \gamma(s, X_1, G/R) \gamma(s, X_2, G/R) = \pi^{-s} \Gamma((s+iv)/2) \Gamma((1+s+iv)/2)$ which is $\gamma(s, \delta, G/C)$. It follows that the function γ on characters of the archimedean local Weil groups satisfy the desired conditions and therefore the function $X \mapsto \mathcal{O}(s, X, K/k) =$

$\prod_{y/p} \gamma(s, X_y, \mathbb{R}_y/k_y)$ satisfies the global Artin conditions.

This completes the demonstration of the functional equation of the Weil L series. For the problem of giving a local decomposition of the root number appearing in this equation, we consider the Weil L-series as a function defined on the characters of $\mathbb{W}_{K/k}$ and rewrite the functional equation of the Hecke L-series in terms of the coefficients appearing in the functional equations of the local zeta functions studied by Tate.

§5

If χ is a character of a local Weil group, $\mathbb{W}_{E/F}$, let $Z'(s, \chi, E/F) = Z(1-s, \bar{\chi}, E/F) / Z(s, \chi, E/F)$, a ratio between local zeta functions of the type discussed in §2. If

If k is a global number field and θ is a character of G_k , then Tate's formulation of the functional equation of the Hecke L-series, $L(s, \theta, k/k)$ may be written

$$L(1-s, \bar{\theta}, k/k) = L(s, \theta, k/k) \prod_{\mathfrak{y}} [\rho(s, \theta_{\mathfrak{y}}, k_{\mathfrak{y}}/k_{\mathfrak{y}}) Z'(s, \theta_{\mathfrak{y}}, k_{\mathfrak{y}}/k_{\mathfrak{y}})]$$

where the product is over all primes of k and $\rho(s, \theta_{\mathfrak{y}}, k_{\mathfrak{y}}/k_{\mathfrak{y}})$ is used to denote $\rho_{k_{\mathfrak{y}}}(\theta_{\mathfrak{y}} | |_{\mathfrak{y}}^{\#})$, i.e. the factor associated by Tate with the quasi character $x \mapsto |x|_{\mathfrak{y}}^{\#} \theta_{\mathfrak{y}}(x)$ of $k_{\mathfrak{y}}^*$ (the valuation, $| \cdot |_{\mathfrak{y}}$ being the normalized valuation). It should be noted that the infinite product appearing in this functional equation causes no difficulty as for almost all \mathfrak{y} the term in the brackets is 1.

Suppose that it were possible to extend the function $\rho(s, \theta_{\mathfrak{y}}, k_{\mathfrak{y}}/k_{\mathfrak{y}})$ on characters of the multiplicative groups of local fields to a function $\rho(s, \chi_{\mathfrak{y}}, Kk_{\mathfrak{y}}/k_{\mathfrak{y}})$ on characters of local Weil groups such that conditions I-V hold. As the local

Weil zeta functions have these properties, it would follow that the functional equation of the Weil L-series could be written $L(1-s, \bar{X}, K/k) = L(s, X, K/k) \prod_y [\rho(s, X_y, K_y/k_y) \epsilon^1(s, X_y, K_y/k_y)]$ a decomposition into local factors of the global factor which appears in the functional equation. (From the similar observation for the Hecke L-series, it would follow that almost all the brackets appearing in the last equation are 1). From this decomposition and the fact that the expression,

$$\frac{G(s, X, K/k)}{G(1-s, \bar{X}, K/k)} = \frac{A(s, X, K/k)}{A(1-s, \bar{X}, K/k)}, \text{ Also has a natural decomposition}$$

into local factors, it would follow that the root number may be decomposed into purely local factors.

Thus it is possible to state conditions of a local nature which insure the existence of a decomposition of the root number. Nothing has been said concerning the necessity of these conditions. Certainly condition IV is not necessary.

Actually, it is ^{not} possible to extend the Tate factors in such a manner that conditions I, II, III hold as the following simple counter example shows :

Let K be an abelian extension of a local number field k , δ an arbitrary character of k^* , let $\varphi = \delta \circ N_{K/k}$ a character of K^* and let X be the character of $N_{K/k}$ induced by φ . If the extension exists, then by condition II we must have

$$\rho(s, X, K/k) = \rho(s, \varphi, K/K) = \rho_K(\varphi | |_{K^*}), \quad ||_K \text{ being normalized valuation of } K. \text{ But as shown in chapter I, } X \text{ is obtained by transfer}$$

from the character, $\sum_{j=1}^n \tau_j$, of k^* ; τ_1, \dots, τ_n being the group of characters of k^* trivial on the norm group. It follows by conditions I and III that

$$\rho(s, X, K/k) = \prod_{j=1}^n \rho(s, \delta \tau_j, k/k) = \prod_{j=1}^n \rho_k(s \| \delta_{k^*} k/k).$$

We thus have a contradiction as the ratio between these two expressions for $\rho(s, X, K/k)$ is $\chi(m, K/k)$, where $m+1$ is the exponent of the conductor of φ .

However we do know that $(\chi(m, K/k))^{1/4} = 1$ and thus we are led to the conjecture:

It is possible to extend the fourth power of the Tate function to a complex valued function defined on the characters of local Weil groups which satisfies the local Artin conditions.

This conjecture concerning the characters of local Weil groups has been verified only in the cyclic case, i.e. only for characters of local groups $W_{K/k}$, where K is a cyclic extension of k . This will be proven subsequently. From this it follows that if $W_{K/k}$ is a global Weil group and every decomposition subgroup of $G(K/k)$ is cyclic and if X is a character of $W_{K/k}$ then the fourth power of the root number $W(X, K/k)$ has a canonical local decomposition. We may also conclude that if k is an algebraic number field, L a normal extension of k such that every decomposition subgroup of the Galois group $G(L/k)$ is cyclic and if K is an abelian extension of L normal over k and X a character of $G(K/k)$ then the fourth power of the root number appearing in the functional equation of the Artin L -series, $L_A(s, X, K/k)$, has a

canonical decomposition into local factors.

In the abelian local example cited above we note that for the character χ appearing there, we could have used property III to define $\rho(s, \chi, K/k)$. It then follows that $\chi(m, K/k)$ is a "measure" of the extent to which this $\rho(s, \chi, K/k)$ fails to have the induced character property. As the global root numbers do have the induced character property we may expect some kind of product formula involving these local "error" terms $\chi(m, K/k)$. An example of such a product formula shall now be given:

Theorem

Let k be an algebraic number field, K an abelian extension field, δ a character of G_K and φ the character $\delta \circ \Pi_{K/k}$ of G_K . If γ is a prime of k then there exists an integer m_γ such that $\mathfrak{p}^{1+m_\gamma}$ is the conductor of $\varphi_{\mathfrak{p}}$ for each prime \mathfrak{p} of K which extends γ . Let r_γ be the number of primes of K which extend γ . Then $\prod_{\mathfrak{p}} [\chi(m_\gamma, K_{\mathfrak{p}}/k_{\mathfrak{p}})]^{r_\gamma} = 1$ the product being taken over all valuations of k .

Proof

Let χ be the character of $\Pi_{K/k}$ induced by φ . Let $\sigma = \tau_1, \dots, \tau_n$ be the group characters of G_K which are trivial on $\Pi_{K/k} G_K$. Precisely as in the local case (of chapter I),

$$\chi = \sum_{j=1}^n (\delta \tau_j) \circ \mathcal{N}_{\Pi_{K/k} \rightarrow G_K}$$

and therefore, using a slightly simpler notation for Hecke L-series,

$$\frac{L(1-s, \overline{\varphi}, K)}{L(s, \varphi, K)} = \prod_{j=1}^n \left[\frac{L(1-s, \delta \tau_j, k)}{L(s, \delta \tau_j, k)} \right]$$

From the functional equation of the Hecke L-series, it follows that

$$1 = \prod_{\mathfrak{y}} \left\{ \frac{\prod_{j=1}^{n_{\mathfrak{y}}} [\rho(s, (\theta \tau_j)_{\mathfrak{y}}, k_{\mathfrak{y}}) Z'(s, (\theta \tau_j)_{\mathfrak{y}}, k_{\mathfrak{y}})]}{\prod_{\mathfrak{p}|\mathfrak{y}} [\rho(s, \varphi_{\mathfrak{p}}, K_{\mathfrak{p}}) Z'(s, \varphi_{\mathfrak{p}}, K_{\mathfrak{p}})]} \right\}.$$

It only remains to show that the term $\{ \}$ is $[\chi(m_{\mathfrak{y}}, K_{\mathfrak{y}}/k_{\mathfrak{y}})]^{K_{\mathfrak{y}}}$. It follows from the isomorphism between completions of K at primes which extend \mathfrak{y} that the denominator is

$[\rho(s, \varphi_{\mathfrak{p}}, K_{\mathfrak{p}}) Z'(s, \varphi_{\mathfrak{p}}, K_{\mathfrak{p}})]^{K_{\mathfrak{y}}}$ where \mathfrak{p} now denotes a fixed extension of \mathfrak{y} . Let L be the decomposition subfield of K at \mathfrak{y} , and let H be the group of characters of $G_{\mathfrak{y}}$ which are trivial on $N_{L/K} G_L$. Arranging G in cosets of H , let $\tau_1, \dots, \tau_{n_{\mathfrak{y}}}$ be representatives of the distinct cosets. As the restriction of each element of H to $k_{\mathfrak{y}}^*$ is trivial, whence the $\{ \}$ may be written

$$\left[\frac{\prod_{j=1}^{n_{\mathfrak{y}}} [\rho(s, (\theta \tau_j)_{\mathfrak{y}}, k_{\mathfrak{y}}) Z'(s, (\theta \tau_j)_{\mathfrak{y}}, k_{\mathfrak{y}})]}{\rho(s, \varphi_{\mathfrak{p}}, K_{\mathfrak{p}}) Z'(s, \varphi_{\mathfrak{p}}, K_{\mathfrak{p}})} \right]^{K_{\mathfrak{y}}}$$

Letting $\chi_{\mathfrak{y}}$ be the character of the local Weil group, $W_{K_{\mathfrak{p}}/k_{\mathfrak{y}}}$ induced by $\varphi_{\mathfrak{p}}$ of $K_{\mathfrak{p}}^*$ and noting that $\{(\theta \tau_j)_{\mathfrak{y}}\}_{j=1}^{n_{\mathfrak{y}}}$ is the group of characters of $k_{\mathfrak{y}}^*$ which are trivial on $N_{K_{\mathfrak{p}}/k_{\mathfrak{y}}} K_{\mathfrak{p}}^*$, it follows that

$$\chi_{\mathfrak{y}} = \sum_{j=1}^{n_{\mathfrak{y}}} (\theta \tau_j)_{\mathfrak{y}} \circ \mathcal{W}_{W_{K_{\mathfrak{p}}/k_{\mathfrak{y}}}} \rightarrow K_{\mathfrak{p}}^* \quad \text{and that}$$

$\prod_{j=1}^{n_{\mathfrak{y}}} Z(s, (\theta \tau_j)_{\mathfrak{y}}, k_{\mathfrak{y}})$ is just the local zeta function, $Z(s, \chi_{\mathfrak{y}}, K_{\mathfrak{p}}/k_{\mathfrak{y}})$. As these zeta functions satisfy the local induced character condition, it follows that the $\{ \}$ is

$$\left[\frac{\prod_{j=1}^{n_y} \rho(s, (\sigma \tau_j)_y, K_y)}{\rho(s, \sigma \tau, K \tau)} \right]^{n_y} \text{, from which the theorem follows.}$$

The question of whether a product formula of this type exists for general normal extensions which are locally abelian remains unanswered.

§6 The Partial Extension of Tate's Function

If k is a local number field, K a normal extension, then the local Weil group $W_{K/k}$ has abelian invariant subgroup K^* of finite index. The factor group $W_{K/k}/K^*$ is isomorphic to the galois group $G(K/k)$ which is always solvable. As indicated above, this is not enough to satisfy the conditions of lemma 7 (§1). If $G(K/k)$ is "super-solvable", i.e. has a principal series whose prime factor groups are cyclic and if X is an irreducible character of the Weil group then there exists a character φ of degree 1 of a subgroup g , which contains K such that φ induces X . Unfortunately φ is not necessarily even essentially unique, i.e. there may exist another subgroup g' of $W_{K/k}$ with character φ' of degree 1 such that φ' also induces X and such that there exists no inner automorphism of $W_{K/k}$ which maps g onto g' and relates φ with φ' . This may occur even if $G(K/k)$ is abelian. It is only when $G(K/k)$ is cyclic that g is determined uniquely by X (of Lemmas 5 and 6) and the determination in that case follows from the fact that if a group has a cyclic factor group over its center then the

group is abelian.

The problem of extending Tate's function to characters of local Weil groups may now be considered. This function is defined by Tate for all irreducible characters of Weil groups $W_{K/k}$ ($= k^*$). If X is a linear character of $W_{K/k}$ then X is trivial on the closure of the commutator subgroup and therefore there exists a unique linear character θ (of degree 1) of k^* such that $X = \theta \circ \rho_{W_{K/k}} \rightarrow k^*$. It is then natural to define $\rho(s, X, K/k) = \rho(s, \theta, k/k)$, for characters X of degree 1, and this definition may be extended in a natural way to characters of $W_{K/k}$ which are sums of such characters. If X is an irreducible character of $W_{K/k}$ and $G(K/k)$ is "super-solvable" then there exists a subgroup $W_{K/L}$ containing K^* with character φ of degree 1 which induces X . $\rho(s, \varphi, K/L)$ being already defined, it would be natural to set $\rho(s, X, K/k)$ equal to it (that is to use the Induced Character property to define the extended Tate coefficient of X) but φ and L are not uniquely determined by X and therefore this would not in general be a canonical definition of the extended Tate coefficient of X . Indeed even if K/k is abelian, $\rho(s, \varphi, K/L)$ would actually not be uniquely determined by X (however there are good reasons to believe that the fourth power of $\rho(s, \varphi, K/L)$ is uniquely determined for K/k abelian and furthermore if $\deg(K/k)$ is odd then even the square of $\rho(s, \varphi, K/L)$ is probably uniquely determined by X). If however $G(K/k)$ is cyclic then (Lemma 6, §1) $W_{K/L}$ is uniquely determined by X and φ is unique to within inner auto-

morphisms of $W_{K/k}$. The remainder of this discussion is restricted to the cyclic case.

K/k cyclic

If X is an irreducible character of $W_{K/k}$ then there exists a unique subgroup $W_{K/L}$ containing K^* for which there exists a linear character which induces X . If φ and φ' are characters of $W_{K/L}$ which induce X then by lemma 6 there exists $x \in W_{K/k}$ such that $\varphi' = \varphi^x$. Let θ be the unique character of L^* such that $\varphi = \theta \circ \mathcal{N}_{W_{K/L} \rightarrow K^*}$. As $W_{K/k}/W_{K/L} \cong G(L/k)$ we may identify the class of x modulo $W_{K/L}$ with its natural image σ in $G(L/k)$. It then follows that $\varphi' = \theta^\sigma \circ \mathcal{N}_{W_{K/L} \rightarrow K^*}$, θ^σ being the character, $w \rightarrow \theta(\sigma(w))$, of L^* . As σ certainly leaves the elements of the closure, R , of Q in k fixed, it follows from the definition of the Tate coefficients that $\rho(s, \theta, L/L) = \rho(s, \theta^\sigma, L/L)$, whence by the previous definitions (for linear characters of Weil groups) $\rho(s, \varphi, K/L) = \rho(s, \varphi', K/L)$ and therefore $\rho(s, X, K/k)$ may be well defined by setting it equal to $\rho(s, \varphi, K/L)$.

Having extended the definition to irreducible characters of the local Weil group, the statement of property I is used to define $\rho(s, X, K/k)$ for reducible characters of $W_{K/k}$. Properties I and V then held trivially; it only remains to verify properties II, III, IV. Property III can cause no difficulty, for if θ is a character of k^* and $X = \theta \circ \mathcal{N}_{W_{K/L} \rightarrow K^*}$, then θ is the sum of characters of k^* of degree one and likewise X is the sum of such characters, whence from the definitions, $\rho(s, X, K/k) = \rho(s, \theta, k/k)$.

For property IV, we may assume φ an irreducible character of $W_{L/k}$,
 X the character $\varphi \circ \tau_{K/k \rightarrow L/k}$ of $W_{K/k}$. Then there exists a unique
 subgroup $W_{L/k'}$ of $W_{L/k}$ ($L \supset k' \supset k$) with linear character σ which
 induces φ . The kernel of $\tau_{K/k \rightarrow L/k}$ being the closure of the
 commutator subgroup of $W_{K/L}$, it follows that $W_{K/k'} = \tau_{K/k \rightarrow L/k}^{-1}(W_{L/k'})$.
 Let σ' be the character $\sigma \circ \tau_{K/k \rightarrow L/k}$ of $W_{K/k'}$. It follows by
 an argument similar to that of the proof of Lemma 7 (§1) that X
 is induced by σ' . As σ is linear there exists θ , a character of
 k'^* such that $\sigma = \theta \circ \mathcal{N}_{W_{L/k'} \rightarrow L^*}$, whence $\sigma' = \theta \circ \mathcal{N}_{W_{K/k'} \rightarrow K^*}$.

As X is irreducible, the property follows from the definitions,

$$\rho(s, X, K/k) = \rho(s, \sigma', K/k') = \rho(s, \theta, k'/k') = \rho(s, \sigma, L/k') = \rho(s, \varphi, L/k).$$

Thus the definition of the extension of the Tate function
 to characters of $W_{K/k}$ has been formulated in such a manner that
 the conditions I, III, IV, and V are satisfied almost trivially.
 Condition II cannot be expected to be satisfied as the previous
 illustration shows that cyclic counter examples exist. The final
 lemma completes the proof the main conjecture for K/k cyclic.

Lemma

If $K \supset L \supset k$, φ a character of $W_{K/L}$, X the induced character
 of $W_{K/k}$ then

$$\rho(s, X, K/k) \equiv \rho(s, \varphi, K/L) \pmod{\gamma}$$

where $\gamma =$ group of the fourth roots of 1 if $(-1, K/k) = -1$
 group of square roots of 1 if $(-1, K/k) = +1$.

Proof

Using property I, it may be assumed that φ is irreducible. Then there exists a subgroup $W_{K/F}$ of $W_{K/L}$ for which there exists a linear character σ which induces X . Furthermore there exists θ , a character of F^* such that $\sigma = \theta \circ \mathcal{N}_{W_{K/F}} \rightarrow K^*$. Let X' be the character of $W_{F/k}$ induced by θ . As $W_{K/F} = \tau_{K/k}^{-1} \rightarrow F/k(F^*)$, an argument similar to the one involved in the proof of Lemma 7 shows that $X = X' \circ \tau_{K/k} \rightarrow F/k$. Hence by the definition and known properties of the extension of the Tate coefficients, it follows that

$$\frac{\rho(s, X, K/k)}{\rho(s, \varphi, K/L)} = \frac{\rho(s, X', F/k)}{\rho(s, \theta, F/F)} = \frac{\rho(s, X', F/k)}{\rho(s, \theta, F/F)}.$$

As $(-1, K/k) = 1$ implies $(-1, F/k) = 1$, it is enough to show that if δ is a character of K^* of degree 1 and X is the induced character of $W_{K/k}$ then $\rho(s, \delta, K/K) \equiv \rho(s, X, K/k) \pmod{\gamma}$.

Let $G(K/L)$ be the subgroup of $G(K/k)$ whose elements leave δ fixed. Let φ be the character of $W_{K/L}$ induced by δ . Let σ be a generator of the cyclic group $G(K/L)$. $\delta^{\sigma-1} = 1$ implies that δ is trivial on the kernel in K^* of $W_{K/L}$, whence $\delta = \mu \circ N_{K/L}$, μ a character of L^* . Then $\varphi = \sum_{j=1}^f (\mu \tau_j) \circ \mathcal{N}_{W_{K/L}} \rightarrow K^*$, where τ_1, \dots, τ_f are the characters of L^* trivial on $W_{K/L}K^*$. For simplicity, let $\varphi_j = (\mu \tau_j) \circ \mathcal{N}_{W_{K/L}} \rightarrow K^*$. Then $\varphi = \sum_{j=1}^f \varphi_j$.

$$\frac{\rho(s, \varphi, K/L)}{\rho(s, \delta, K/K)} = \frac{\prod_{j=1}^f \rho(s, \mu \tau_j, L/L)}{\rho(s, \delta, K/K)} = \chi(s, K/L)$$

where φ^{1-m} is the conductor of θ . Let X_j be the character of $W_{K/k}$ induced by φ_j , then $X = \sum_{j=1}^r X_j$. If X' is any irreducible character of $W_{K/k}$ occurring in X then θ occurs in the restriction of X' to K^* , whence by Lemma 5, X' is induced by a character of $W_{K/L}$ of degree one, whence $X'(1) = \deg L/k = X_j(1)$. Hence X is the sum of r irreducible characters of degree $X_j(1)$ and therefore $X_1 + \dots + X_j$ is the decomposition of X into irreducible characters. Hence by definition, $\rho(s, X, K/k) = \prod_{j=1}^r \rho(s, X_j, K/k) = \prod_{j=1}^r \rho(s, \varphi_j, K/L) = \rho(s, \varphi, K/L)$. As $\chi(m, K/L) \in \gamma$, the assertion is proven.

§ 7. Reformulation of the problem

The basic approach to the problem of determining a canonical factorization of the root numbers of characters of Weil groups has been to start with Tate's canonical factorization (§5) of the ratio $L(1-s, \bar{\theta}, k/k) / L(s, \theta, k/k)$ between associated Hecke L-series and to attempt to extend these local factors to a function on characters of local Weil groups which satisfy the local Artin conditions. (It should be noted that for given θ , character of G_K , almost all of the local factors are trivial). It has been shown that this factorization cannot lead in this way to the full solution of the problem. This suggests the question: (1) Does there exist another canonical factorization of $L(1-s, \bar{\theta}, k/k) / L(s, \theta, k/k)$ (with the property that almost all local factors are trivial) which could lead to a full solution of the problem? This suggests

the questions:

(2) What are the set of all canonical functions T on multiplicative characters of local fields with the property that if θ is a character of G_K then

(a) $T(\theta_y) = 1$ for almost all primes of k .

(b) $\prod_y T(\theta_y) = 1$, (the product being over all primes of k)?

(If a is a fixed rational number then the function $\theta_y \rightarrow \theta_y^a$ has this property).

(3) Does there exist a function T , satisfying ^{the} conditions ^{of (2)} such that the function $\theta_y \rightarrow T(\theta_y) \rho_k(\theta_y)$ can be extended to a function on characters of local Weil groups which satisfies the local Artin conditions? (This is equivalent to question (1).)

The results of §5 show that if T satisfies the conditions of (3) then it must satisfy the condition:

If K/k is a local abelian extension, X a character of K^* obtained by composition with $N_{K/k}$ from a character of k^* then in the notation of chapter III,

$1 = \chi(m, K/k) (\prod_{\mu} T(\mu)) / T(X)$, the product being taken over all characters μ of k^* for which $X = \mu \circ N_{K/k}$ and where $1+m$ is the exponent of the conductor of X .

These criteria may provide a means of disposing of question 1 (particularly if the answer to question (3) is negative).

