J. Martinet

Character theory and Artin L-functions

J. Martinet

I. NON ABELIAN L-FUNCTIONS

The aim of this chapter is to describe the theory of Artin's non abelian L-functions, taking for granted the theory of abelian L-functions. This chapter owes much to a talk by Serre (Fonctions L non abéliennes, Séminaire de Théorie des Nombres, Bordeaux, 10 avril 1973).

§1. Frobenius

Two papers of Frobenius, both dating back to 1896, play a key role in the theory we are going to describe. The first one is devoted to what is now called the "Frobenius substitution". Let E/K be a finite normal extension of number fields with Galois group G, and let $\mathfrak{p}$ be a finite prime of K. Assume E/K is unramified at $\mathfrak{p}$. For every prime $\mathfrak{P}$ of E lying above $\mathfrak{p}$, there is a unique element $\sigma_{\mathfrak{P}} \in G$ (the

Frobenius substitution) such that, for any integral $x \in E$, the congruence $\sigma_{\mathfrak{P}}(x) \equiv x^{N(\mathfrak{p})} \bmod \mathfrak{P}$ holds, where $N(\mathfrak{p})$ is th absolute norm of $\mathfrak{p}$. Moreover, the conjugacy class of $\sigma_{\mathfrak{P}}$ in G does not depend on the particular choice of $\mathfrak{P}$ above $\mathfrak{p}$ in E. Frobenius stated in this paper a density theorem of the Čebotarev type, and proved the following result: for every cyclic subgroup C of G, there exist infinitely many primes $\mathfrak{P}$ such that $\sigma_{\mathfrak{P}}$ is a generator of C. Even disregardi questions of density, this is weaker than Čebotarev's theo which asserts that every generator of C is of the form $\sigma_{\mathfrak{P}}$ f infinitely many $\mathfrak{P}$.

The second paper of Frobenius we are concerned with is devoted to the definition of the characters. As will be seen in a moment, the theory of L-functions relies heavily on the consideration of both the notion of a character and of the Frobenius substitution. But Frobenius did not see the connection, and the sequel of his work deals mainly with the theory of characters.

§2. Weber

For an ideal $\mathfrak{f}$ of K, let $I_{\mathfrak{f}}$ be the group of ideals of K prime to $\mathfrak{f}$ and let $P_{\mathfrak{f}}$ be the subgroup of $I_{\mathfrak{f}}$ which consist of ideals which can be generated by a totally positive element α of K congruent to 1 mod $\mathfrak{f}$. Let H be a subgroup of $I_{\mathfrak{f}}$ containing $P_{\mathfrak{f}}$ (we call such a subgroup a congruence subgroup).

Weber called an abelian extension E of K "a class field for H" if the prime ideals of K which decompose completely in E are precisely those which belong to H, and if $\mathfrak{f}$ is in some sense the smallest possible ideal. In this situation, the prime divisors of $\mathfrak{f}$ are precisely the prime ideals of K which are ramified in E.

Now, for every character $\chi : I_{\mathfrak{f}}/H \to \mathbb{C}^*$, there is an L-function defined for Re(s) > 1 by:

$$L(s,\chi) = \prod_{\mathfrak{p}\nmid\mathfrak{f}} \frac{1}{1-\chi(\mathfrak{p})\ N(\mathfrak{p})^{-s}} .$$

The question arises of comparing the zeta function $\zeta_E(s)$ with the product $\prod L(s,\chi)$ when E is a class field for H. Generally, they are not equal, because of the possible existence of prime ideals which are ramified in E/K but not in the subfield corresponding to the kernel of χ. I shall write

$$\zeta_E(s) \sim \prod_{\chi} L(s,\chi)$$

to mean that the equality is true up to a finite number of factors.

To obtain an equality, one must, for each character χ, replace $\mathfrak{f}$ by the conductor of χ. This was known to Weber for those abelian extensions which were known to be class fields.

§3. Artin's first definition of L-functions

Artin's first definition of L-functions appeared in 1922 (on a new kind of L series). In the meantime (1920) Takagi had established in full generality the classical results of class field theory, namely the one-to-one correspondence between abelian extensions of number fields and congruence subgroups, and also the isomorphism theorem, which asserts that the Galois group G of the extension is isomorphic to the quotient $I_{\mathfrak{f}}/H$.

Using an isomorphism between $I_{\mathfrak{f}}/H$ and G, it would be possible to define L-functions for degree one characters of G. But Takagi's theory does not give any canonical isomorphism between $I_{\mathfrak{f}}/H$ and G. Nevertheless, Artin thought that the L-series we defined previously with a congruence class character could be identified with L-series defined for a degree one character ψ of G by the formula:

$$L(s,\psi) = \prod_{\substack{p \\ \text{unramified}}} \frac{1}{1-\psi(\sigma_p)\, N(p)^{-s}}$$

where $\sigma_{\mathfrak{p}}$ is the Frobenius substitution of one $\mathfrak{P}$ above $\mathfrak{p}$ (Note that $\sigma_{\mathfrak{p}}$ is well defined since G is abelian). This led Artin to conjecture that one obtains an isomorphism between $I_{\mathfrak{f}}/H$ and G by sending the class in $I_{\mathfrak{f}}/H$ of an unramified prime ideal $\mathfrak{p}$ onto the Frobenius substitution $\sigma_{\mathfrak{p}}$. This Artin called "the general law of reciprocity" (because it implies fairly easily the known laws of reciprocity). In his paper on L-functions, he proves the law of reciprocity for a lot of abelian extensions E/K (e.g. cyclotomic extensions, cyclic extensions of prime power degree p^n when K contains the p^n-th roots of unity, cyclic extensions of prime degree, ...). He was quite sure of the validity of his reciprocity law. Indeed, it is stated as a theorem (Satz), and his paper of 1927 on the reciprocity law is simply called "proof of the general reciprocity law".

We are now able to give Artin's first definition of L-functions:

<u>Definition</u> Let E/K be a finite normal extension of number fields with Galois group G. Let V be a finite dimensional complex vector space, and let $s \mapsto \rho(s)$ be a representation of G in V. Denote by χ the character of ρ, defined by

$\chi(s) = \mathrm{Tr}(\rho(s))$ for all $s \in G$. For a prime p in K, the determinant $\det(1 - N(p)^{-s}\, \rho(\sigma_P))$ does not depend on the choice of P above p, and takes the same value for two isomorphic representations. We can therefore define

$$L(s,\chi) = \prod_{\substack{p \\ \text{unramified}}} \frac{1}{\det(1-\rho(\sigma_P)N(p)^{-s})} .$$

The series is convergent for $\mathrm{Re}(s) > 1$.

It is then obvious that L is additive, i.e. :

(a) $L(s,\chi_1+\chi_2) = L(s,\chi_1)L(s,\chi_2)$.

The following equalities, however, are true only up to a finite number of Euler-factors (we use the notation "$\sim$").

Let H be a normal subgroup of G corresponding to an extension F/K . Let ρ be a representation of G/H with character χ and let ρ' be the lifting of ρ to G with character χ'. Then we have the lifting formula

(b) $L(s,\chi') \sim L(s,\chi)$.

Let H be a subgroup of G, and let χ be a character of H which induces the character χ^* of G. Then we have the induction formula

(c) $L(s,\chi^*) \sim L(s,\chi)$.

Moreover, Artin proved that $L(s,1) \sim \zeta_K(s)$.

Applying formula (c) to the unit character of a subgroup H of G corresponding to an extension F/K, we obtain the formula $\zeta_F(s) \sim L(s, r_{G/H})$, where $r_{G/H}$ is the character of the permutation representation of G on G/H.

Let us take H = (1) in the above formula. Then $r_{G/H}$ is the character r_G of the regular representation of G, which is just the sum $\sum_{\chi} \chi(1)\chi$ over all irreducible characters of G. Now applying formula (a), we get

$$\zeta_E(s) \sim \prod_{\chi \text{ irreducible}} L(s,\chi)^{\chi(1)} .$$

Assuming the reciprocity law, Artin gave a proof of the theorem of density conjectured by Frobenius. He stated the existence of an analytic continuation for his L functions (with perhaps "ramification" points) and of a functional equation relating $L(s,\chi)$ and $L(1-s, \bar{\chi})$ as had been proved in 1917 by Hecke for abelian L-functions. He also asked whether his L functions are holomorphic in the whole complex plane for a character which does not contain the unit character. We now call this statement "the Artin conjecture".

§4. The general definition of non abelian L-functions

Surprisingly, Čebotarev proved in 1926 the density theorem conjectured by Frobenius without using L-functions.

The main idea behind the proof is to reduce to the case of a cyclotomic extension. In 1927, using this device, Artin proved his general law of reciprocity. In 1930, he returned to the problems of L-functions in his paper "on the theory of L series with general characters". The two main problems are:

(i) To define local factors at ramified primes, in such a way as to put true equalities in the above formulae.

(ii) To define local factors at infinity and an exponential factor in order to get an analytic continuation and a functional equation.

(i) As always, we consider a normal extension E/K of number fields with Galois group G and a complex representation $\rho : G \to Gl(V)$ with character χ. Let p be a prime of K; choose a prime P above p. Let D_P and I_P denote, respectively, the decomposition group and the inertia group of P. Now, the quotient group D_P/I_P is isomorphic to the Galois group of the residue extension. Hence, we can define a Frobenius substitution σ_P belonging to D_P/I_P. The vector space V is acted on by G via the formula $\sigma x = \rho_\sigma(x)$ for all

$x \in V$ and all $\sigma \in G$. Let

$$V^{I_P} = \{x \in V \mid \forall\ \sigma \in I_P,\quad \sigma x = x\} ,$$

the subspace of elements of V fixed by I_P. Once more, the determinant of the transformation $(1-N(p)^{-s}\ \sigma_P)$ of V^{I_P} does not depend on the particular choice of P above p, and is the same for two isomorphic representations. We can thus define

$$L(s,\chi) = \prod_{p \text{ finite}} \frac{1}{\det_{V^{I_P}}(1-N(p)^{-s}\ \sigma_P)}$$

for $\text{Re}(s) > 1$.

Now, the induction formula and the lifting formula become equalities. We summarize the fundamental results (notation as above):

<u>Theorem</u> (a) $L(s,\chi_1+\chi_2) = L(s,\chi_1)\ L(s,\chi_2)$

(b) $L(s,\chi') = L(s,\chi)$

(c) $L(s,\chi^*) = L(s,\chi)$.

<u>Assume G is abelian.</u> Let χ be a degree one character of G, and let ψ be the corresponding congruence class character. Then,

(d) $L(s,\chi) = L(s,\psi)$.

An obvious corollary is the equality:

$$\zeta_E(s) = \prod_{\substack{\chi \\ \text{irreducible}}} L(s,\chi)^{\chi(1)} .$$

Moreover, if V is of dimension 1 and if $\rho(I_P)$ does not act trivially, then $V^{I_P} = (0)$. This explains why, for an abelian L function, local factors corresponding to the primes dividing the conductor reduce to 1.

Artin gave a more explicit description of his functions using an expansion of $\log L(s,\chi)$. Let us first consider the case of an unramified prime p of K. Let d be the dimension of V, and let $\lambda_i(p)$ $(1 \leq i \leq d)$ be the eigenvalues of $\rho(\sigma_P)$ for some P above p. Then,

$$\det(1-N(p)^{-s}\,\rho(\sigma_P)) = \prod_{i=1}^{d} (1-\lambda_i(p)\,N(p)^{-s}).$$

Thus,

$$\log \frac{1}{\det(1-N(p)^{-s}\,\rho(\sigma_P))} = \sum_{i=1}^{d}\sum_{m=1}^{\infty} \frac{\lambda_i(p)^m}{m\,N(p)^{ms}}$$

$$= \sum_{m=1}^{\infty} \frac{\chi(\sigma_P^m)}{m\,N(p)^{ms}} .$$

where $\chi(\sigma_P^m)$ is just the trace of the m-th power of the Frobenius substitution. For a prime P with ramification index e, the above definition of $\chi(\sigma_P^m)$ makes no sense, as σ_P belongs to D_P/I_P. We define however $\chi(\sigma_P^m)$ as an average,

$\chi(\sigma_p^m) = \frac{1}{e} \sum_{s \mapsto \sigma_p^m} \chi(s)$, where the sum is taken over the elements s of D_p which map onto σ_p^m in D_p/I_p.

The logarithmic expansion is now true for any prime p of K. Hence:

$$\log L(s,\chi) = \sum_p \sum_{m=1}^{\infty} \frac{\chi(\sigma_p^m)}{m\, N(p)^{ms}} ,$$

a formula which gives an expansion for the logarithmic derivative of $L(s,\chi)$:

$$\frac{L'(s,\chi)}{L(s,\chi)} = - \sum_p \log(N(p)) \sum_{m=1}^{\infty} \frac{\chi(\sigma_p^m)}{N\,(p)^{ms}} .$$

Remark. Let us choose a fixed algebraic closure $\bar{\mathbb{Q}}$ of $\mathbb{Q}$. Then every number field K can be considered as a subfield of $\bar{\mathbb{Q}}$. Let Ω_K be the (infinite) Galois group $Gal(\bar{\mathbb{Q}}/K)$. Then property (b) of the above theorem shows that an L function is attached to every finite dimensional complex representation of Ω_K with open kernel. Such a representation has a character, and we can define as usual virtual characters of Ω_K. Then property (a) allows us to define an L function $L(s,\chi)$ for every virtual character χ of Ω_K.

(ii) We are now going to define an enlarged L-function

Λ of the form $\Lambda(s,\chi) = A(\chi)^{s/2}\,\gamma_\chi(s)\,L(s,\chi)$, and to prove for it the existence of a meromorphic continuation together with a functional equation $\Lambda(s,\chi) = W(\chi)\,\Lambda(1-s,\bar{\chi})$ for some constant $W(\chi)$ of absolute value 1. According to the known properties of abelian L-functions, we must define Γ-factors and the constant $A(\chi)$.

* Let us begin with the Γ-factors. Put $\gamma(s) = \pi^{-s/2}\,\Gamma(s/2)$. We define γ_χ as a product $\gamma_\chi(s) = \prod_v \gamma_\chi^v(s)$, where v ranges over the infinite places of K, and γ_χ^v, the local factor at infinity, is defined in the following way: for v complex, we put $\gamma_\chi^v(s) = [\gamma(s)\,\gamma(s+1)]^{\chi(1)}$. Now, let v be a real place of K. To every place w of E above v corresponds a decomposition group (or inertia group) $G(w) = \{s \in G \mid sw = w\}$ of order 1 or 2. The generator of $G(w)$ plays the role of the Frobenius substitution, and is defined up to conjugacy by v. We write for V a direct sum decomposition $V = V_v^+ \oplus V_v^-$ corresponding to the eigenvalues +1 and -1 of $\rho(\sigma_w)$ for a fixed w above v, and we put

$$\gamma_\chi^v(s) = \gamma(s)^{\dim V_v^+}\,\gamma(s+1)^{\dim V_v^-}.$$

* The definition of $A(\chi)$ needs the notion of a conductor $\mathfrak{f}(\chi)$ which must generalise the conductors of class field

theory defined for abelian characters. The theory of this conductor, now called the Artin conductor, is developed in the paper "The group theoretical structure of the discriminants of algebraic number fields", written at the end of the year 1930.

Let p a prime ideal of K. Choose a prime ideal P above p. Let G_i $(i \geq 0)$ be the corresponding ramification groups (G_o is the inertia group) and let g_i be the order of G_i. We define a rational number

$$n(\chi,p) = \sum_{i=0}^{\infty} \frac{g_i}{g_o} \operatorname{codim} V^{G_i}$$

($n(\chi,p)$ is actually independent of the choice of P above p).

Theorem (Artin) $n(\chi,p)$ is an integer.

Nowadays, this is proved using Brauer's induction theorem (see Serre, Corps locaux, chap. VI, §1-3. for a proof).

To prove this theorem, Artin reduced to the case $G = G_1$, using an argument of Speiser. Now, G_1 is a p-group and it was known to Artin that every irreducible character of a p-group is induced by a character of degree one of some subgroup. As Artin had established induction properties for $n(\chi,p)$, the proof was reduced to the case of degree one characters. He could then complete the proof using a theorem of Hasse, now known as Hasse-Arf theorem after its generalization by Arf.

For an unramified prime ideal p, one has $n(\chi,p) = 0$. Therefore, the formula

$$\mathfrak{f}(\chi, E/K) = \mathfrak{f}(\chi) = \prod_{p} p^{n(\chi,p)}$$

defines an ideal of K, which is known as the Artin conductor.

The constant $A(\chi)$ is now defined by the formula

$$A(\chi) = |d_K|^{\chi(1)} N_{K/\mathbb{Q}}(\mathfrak{f}(\chi)) \quad ,$$

where d_K is the absolute discriminant of K.

Theorem Let Λ be the "enlarged" L-function defined by the formula $\Lambda(s,\chi) = A(\chi)^{s/2} \gamma_\chi(s) L(s,\chi)$ for $Re(s) > 1$. Then Λ possesses a meromorphic continuation in the whole complex plane, and satisfies the functional equation $\Lambda(1-s,\chi) = W(\chi) \Lambda(s,\bar{\chi})$ for some constant $W(\chi)$ of absolute value 1 (the so-called "Artin root number").

In the theorem, $\bar{\chi}$ is the complex conjugate of χ. If

χ is the character of a representation $\rho : G \to Gl(V)$, $\bar{\chi}$ is the character of the contragedient representation $\bar{\rho} : G \to Gl(V^*)$ (V^* is the dual space of V), defined by $\langle \bar{\rho}_s(f), x\rangle = \langle f, \rho_s^{-1}(x)\rangle$ for all $s \in G$, $x \in V$, $f \in V^*$.

Artin could not prove the existence of a meromorphic continuation for the function Λ. The theorem was proved in 1947 by Brauer. We now give the proof.

We must first establish properties (a), (b), (c) for the enlarged L-functions. Properties (a) (additivity) and (b) (lifting property) are easily verified for the functions L and γ_χ, as well as for the conductor $\mathfrak{f}(\chi)$. Thus, they are true for the constant $A(\chi)$, and hence for the function Λ (therefore, we can define $\gamma_\chi(s)$, $\mathfrak{f}(\chi)$, $A(\chi)$ and $\Lambda(s,\chi)$ for a virtual character of Ω_K). It is not difficult to show the invariant of γ_χ under induction. For the Artin conductor, the formula is a bit more complicated. Let H be a subgroup of G with fixed field F, and let χ be a character of H. The conductor of the character χ^* of G induced by χ is given by: $\mathfrak{f}(\chi^*) = D_{F/K}^{\chi(1)} N_{F/K}(\mathfrak{f}(\chi))$, where $D_{F/K}$ is the discriminant of the extension F/K.

A simple calculation using the transitivity formula for discriminants gives the equality $A(\chi^*) = A(\chi)$, and thus the induction formula $\Lambda(s,\chi^*) = \Lambda(s,\chi)$ for the enlarged L-function.

We now apply Brauer's induction theorem: there exist subgroups H_i $(1 \leqslant i \leqslant n)$ of G, degree one characters χ_i $(1 \leqslant i \leqslant n)$ of H_i and rational integers n_i $(1 \leqslant i \leqslant n)$ for some n such that the following equality holds:

$$\chi = \sum_{i=1}^{n} n_i \chi_i^* .$$

We thus have, by properties (a) and (c):

$$\Lambda(s,\chi) = \prod_{i=1}^{n} \Lambda(s,\chi_i)^{n_i}.$$

For $1 \leqslant i \leqslant n$, let F_i be the fixed field of H_i, H_i' the kernel of χ_i and F_i' the fixed field of H_i'. The extensions F_i'/F_i are cyclic extensions with Galois group $G_i = H_i/H_i'$. Writing χ_i' for the character of G_i defined by χ_i, we then have, by property (b):

$$\Lambda(s,\chi_i) = \Lambda(s,\chi_i').$$

We now use Hecke's results. By composition with the Artin map, the characters χ_i' define congruence class characters (or idèle class characters in modern language) ψ_i of F_i, and we know, by property (d), that the function $L(s,\chi_i')$ is equal to $L(s,\psi_i)$. Now, given an abelian L-function $L(s,\psi)$, Hecke defined an enlarged function $\Lambda'(s,\psi)$

by the formula

$$\Lambda'(s,\psi) = A'(\psi)^{s/2}\ \gamma'_{\psi}(s)\ L(s,\psi)\ ,$$

where $A'(\psi) = |d_K|\ N_{K/\mathbb{Q}}\ (\mathfrak{f}(\psi))$ and $\gamma'_{\psi}(s)$ is a product of gamma factors of the form $\gamma(s)$ or $\gamma(s+1)$ depending on the behaviour of ψ at infinity. He proved the existence of a meromorphic continuation in the whole complex plane for Λ' together with a functional equation

$$\Lambda'(1-s,\ \psi) = W'(\psi)\ \Lambda'(s,\bar{\psi})$$

for some constant $W'(\psi)$ of absolute value 1. Note that the analytic continuation of Λ' is in fact holomorphic when ψ is not the trivial character.

Now, given a degree one character χ on the Galois group of a cyclic extension F'/F and its corresponding idèle class character ψ, Artin proved the equality of the "Artin" conductor $\mathfrak{f}(\chi)$ and the conductor of ψ in the sense of class field theory. We thus have $A(\chi) = A'(\psi)$, and the equality of the gamma factors γ_{χ} and $\gamma_{\chi'}$ is easily verified.

Going back to our previous notation, we have $\Lambda(s,\chi_i') = \Lambda'(s,\psi_i)$ for all $s \in \mathbb{C}$ with $\mathrm{Re}(s) > 1$. This implies the existence of the meromorphic continuation for $\Lambda(s,\chi) = \prod_{i=1}^{n} \Lambda'(s,\psi_i)^{n_i}$ as well as the functional equation. Moreover, the equality $W(\chi) = \prod_{i=1}^{n} W'(\psi_i)^{n_i}$ shows that $W(\chi)$ is of absolute value 1.

Corollary With the notation of §3, the following properties hold for the Artin root number:

(a) $W(\chi_1+\chi_2) = W(\chi_1)\ W(\chi_2)$

(b) $W(\chi') = W(\chi)$

(c) $W(\chi^*) = W(\chi)$.

Note that properties (a) and (b) allow us to define $W(\chi)$ for a virtual character of Ω_K.

§5. Some elementary remarks on the Artin conjecture

Recall that the Artin conjecture is the following: for a character χ of a representation which does not contain the unit representation, the corresponding function $L(s,\chi)$ (or, which amounts to the same, the enlarged function $\Lambda(s,\chi)$) is holomorphic.

Artin's conjecture is true for characters of degree one (this is a consequence of Hecke's results for abelian L-functions). As we know that an L-function is meromorphic, it is enough to show that some power of it is holomorphic to prove Artin's conjecture. Thus, for a character χ which is a linear combination with positive rational coefficients of characters induced by non trivial degree one characters of subgroups, the corresponding L-function is holomorphic. Until recent work of Tate, this was the only way one could prove that a given L-function is holomorphic.*

The following well known example is due to Aramata and was rediscovered by Brauer:

Example. Let E/K be a normal extension. Then the augmentation representation of its Galois group (the regular representation minus the unit representation) has the above property. Consequently, the quotient $\zeta_E(s)/\zeta_K(s)$ is holomorphic, or, as one says, $\zeta_K(s)$ divides $\zeta_E(s)$.

Note that it is not known whether $\zeta_K(s)$ divides $\zeta_E(s)$ if E/K is not assumed to be normal. The result, however, would follow from a proof of Artin's conjecture.⊗

---

*Footnote: But see a recent paper of Langlands mentioned in Serre's talk (3.3)).

⊗Footnote: See here also Van der Waall's talk.

REFERENCES (CHAPTER I)

E. Artin, Über eine neue Art von L-Reihen, Hamb. Abh., 1 (1923), 89-108, Collected papers n°3.

E. Artin, Beweis des allgemeinen Reziprozitätsgesetzes, Hamb. Abh., 5 (1927), 353-363, Collected papers n° 5.

E. Artin, Zur Theorie der L-Reihen mit allgemeinen gruppencharakteren, Hamb. Abh., 8 (1930), 292-306, Collected papers n° 8.

E. Artin, Die gruppentheoretische Stuktur der Diskriminanten algebraischer Zahlkörper, J. Reine angew. Math., 164 (1931), 1-11, Collected papers n° 9.

R. Brauer, On Artin's L series with general group characters, Ann. of Math. (2) 48 (1947), 502-514.

N. Čebotarev, Die Bestimmung der Dichtigkeit einer Menge von Primzahlen, welche zu einer gegebene Substitutionsklasse gehören, Math. Ann., 95 (1925), 191-228.

F.G. Frobenius, Über Beziehungen zwischen den Primidealen eines algebraischen Zahlkörpers und den Substitutionen seiner Gruppe, Gesammelte Abhandlungen, Bd II, n° 52, 719-733.

F.G. Frobenius, Über gruppencharaktere, Gesammelte Abhandlungen, Bd III, n° 53, 1-37.

E. Hecke, Über die L-functionen und den Dirichletschen Primzahlsatz für einen beliebigen Zahlkörper, Nachrichten Göttingen (1917), 299-318, Werke, n° 9.

R.P. Langlands, Base change for GL(2) (Lecture notes, IAS Princeton, 1975).

J-P. Serre, Modular forms of weight one and Galois representation, Durham Symposium.

R.W. van der Waall, Holomorphy of quotients of Zeta functions Durham Symposium.

II. GALOIS ACTION ON ROOT NUMBERS

This chapter is devoted to Galois Gauss sums. The main result is a theorem of Fröhlich, which gives a formula for the Galois action on the Galois Gauss sum, and hence on the root number. Fröhlich proved his theorem by global methods, and the proof I gave in Durham closely followed his original proof. I give here a local version of this theorem, from which the global result is easily deduced. This has been made possible by the theory of local constants of Langlands and Deligue.

§1. More on the Artin conductor

The Artin conductor can be defined for more general extensions than extensions of number fields. Let A be a Dedekind ring and K its quotient field. Let E be a finite normal extension of K with Galois group G, and let ρ be a representation of G in a finite dimensional vector space V with character χ. Assume that all the residue class extensions are separable. Let $\mathfrak{p}$ be a prime ideal of K. Let us choose a prime ideal P in E above p. We can then define the ramification groups G_i of P. Writing g_i for the order of G_i, we define as in chapter I,

$$n(\chi,p) = \sum_{i=0}^{\infty} \frac{g_i}{g_o} \operatorname{codim} V^{G_i}.$$

<u>Theorem</u> 1.1. $n(\chi,p)$ is an integer.

(For a proof, see Serre, Corps Locaux, chap. VI, §1-3).

In particular, if E/K is unramified at p, then $n(\chi,p) = 0$, and if E/K is tamely ramified, then $n(\chi,p) = \operatorname{codim} V^{G_o}$.

We now define the Artin conductor by the formula:

idéal de K

$$\mathfrak{f}(\chi) = \prod_{p} p^{n(\chi,p)} .$$

The Artin conductor has the following 3 fundamental properties:

(a) $\mathfrak{f}(\chi + \chi') = \mathfrak{f}(\chi) \cdot \mathfrak{f}(\chi')$

(b) If χ is lifted from a character χ' of a quotient H of G, then:

$$\mathfrak{f}(\chi) = \mathfrak{f}(\chi') .$$

(c) Let H be a subgroup of G, corresponding to a subfield F of E; let χ be a character of H and let χ^* be the character of G induced by χ. Then:

$$\mathfrak{f}(\chi^*) = N_{F/K}(\mathfrak{f}(\chi)) . D(F/K)^{\chi(1)}$$

where D(F/K) is the discriminant (relative to the ring A) of the extension F/K.

Let $D_{\mathcal{P}}$ be the decomposition group of some ideal $\mathcal{P}$ above $\mathfrak{p}$, and let $\chi_{\mathcal{P}}$ be the restriction of χ to $D_{\mathcal{P}}$. Then χ is induced by $\chi_{\mathcal{P}}$. Let $E_{(\mathcal{P})}$ be the decomposition field of $\mathcal{P}$. Then, $E_{(\mathcal{P})}/K$ is unramified, and formula (c) shows the equality:

$$n(\chi,\mathfrak{p}) = n(\chi_{\mathcal{P}}, \mathcal{P} \cap E_{\mathcal{P}}).$$

Let $\hat{E}_{\mathcal{P}}$ (resp. $\hat{K}_{\mathfrak{p}}$) be the completion of E (resp. K) at $\mathcal{P}$ (resp. $\mathfrak{p}$). Then $D_{\mathcal{P}}$ is canonically isomorphic to the Galois group of $\hat{E}_{\mathcal{P}}/\hat{K}_{\mathfrak{p}}$, and the integer $n(\chi,\mathfrak{p})$ is the corresponding integer $n(\chi_{\mathcal{P}}, \hat{\mathfrak{p}})$ defined for this extension.

When A is a discrete valuation ring, there is no need to specify the ideal we choose, and we simply write $n(\chi)$ instead of $n(\chi, \mathfrak{p})$.

We now restrict ourselves to the case when K is a number field, and we define an integer $n(\chi, v)$ for every infinite place v of K. If v is complex, then so is every place of E above v; we say in this case that E/K is unramified at v, and simply put $n(\chi,v) = 0$.

$$\mathfrak{f}(\chi^*) = N_{F/K}(\mathfrak{f}(\chi)) . D(F/K)^{\chi(1)}$$

where D(F/K) is the discriminant (relative to the ring A) of the extension F/K.

Let D_P be the decomposition group of some ideal P above p, and let χ_P be the restriction of χ to D_P. Then χ is induced by χ_P. Let $E_{(P)}$ be the decomposition field of P. Then, $E_{(P)}/K$ is unramified, and formula (c) shows the equality:

$$n(\chi, p) = n(\chi_P, P \cap E_P).$$

Let $\hat{E}_P$ (resp. $\hat{K}_p$) be the completion of E (resp. K) at P (resp. p). Then D_P is canonically isomorphic to the Galois group of $\hat{E}_P/\hat{K}_p$, and the integer $n(\chi, p)$ is the corresponding integer $n(\chi_P, \hat{p})$ defined for this extension.

When A is a discrete valuation ring, there is no need to specify the ideal we choose, and we simply write $n(\chi)$ instead of $n(\chi, p)$.

We now restrict ourselves to the case when K is a number field, and we define an integer $n(\chi, v)$ for every infinite place v of K. If v is complex, then so is every place of E above v; we say in this case that E/K is unramified at v, and simply put $n(\chi, v) = 0$.

If v is real, let w be a place of E above v. In Chapter I, we defined the "inertia group" $I_w = \{s \in G | sw = w\}$. We consider that the extension E/K is tamely ramified at v, and we define $n(\chi,v)$ by the formula:

$$n(\chi,v) = \text{codim } V^{I_w}.$$

Of course, $n(\chi,v)$ does not depend on the choice of w above v, and $n(\chi,v) = 0$ if w is real. We can use the decomposition $V = V_v^+ \oplus V_v^-$ of V given in chapter I, §4. to compute $n(\chi,v)$. Clearly, $n(\chi,v)$ is the number of eigenvalues equal to -1 for a "real Frobenius" σ_v. Now, $\chi(\sigma_v) = \dim V_v^+ - \dim V_v^-$; the following formula holds:

$$n(\chi,v) = \frac{1}{2}\,(\chi(1) - \chi(\sigma_v)).$$

Remark 1. The integer $n(\chi,v)$ was used by Hasse to define the infinite components of the Artin conductor.

Remark 2. The same arguments can be used to compute $n(\chi,p)$ for an extension which is tamely ramified at p : $n(\chi,p)$ is the number of eigenvalues other than $+1$ for a generator σ_p of the inertia group of some ideal P above p.

We can also define an integer $n(\chi)$ in the local archimedean case. Then, E and K are isomorphic either to the field $\mathbb{R}$ of real numbers or to the field $\mathbb{C}$ of complex numbers, and we define $n(\chi)$ by the formula:

$$n(\chi) = \operatorname{codim} V^G.$$

Now, given a normal extension E/K of number fields, a place v of K and a character χ on $G = \mathrm{Gal}(E/K)$, one can define a local character χ_v on $\mathrm{Gal}(E_w/K_v)$, where K_v is the completion of K at v and E_w is the completion of E at some place w of E above v.

The situation is now the same as in the finite case, and the following equality holds:

$$n(\chi,v) = n(\chi_v) .$$

The proof is clear from the formulae $n(\chi,v) = \frac{1}{2}(\chi(1) - \chi(\sigma_v))$ and $n(\chi_v) = \frac{1}{2}(\chi_v(1) - \chi_v(\sigma_v))$, since χ_v is the restriction of χ to the subgroup $(1,\sigma_v)$ of G.

We end this § with the definition of the conductor for an infinite extension. We again use the definitions of the beginning of this section. Let L be an infinite normal extension of K with Galois group G. By a representation ρ of G, we understand a homomorphism ρ of G into the linear group of a finite complex vector space with open kernel. Such a representation factors through the Galois group of a finite extension. Recalling the invariance of the conductor under lifting, we define $\mathfrak{f}(\rho)$ to be the conductor of ρ', where ρ' is any representation of a finite Galois extension such that ρ' lifts to ρ on G. Such a representation has a character χ, and we can define $n(\chi)$ as above. Virtual characters are then defined in the usual way, and the definition of the conductor of a virtual character is immediate.

Remark We define an unramified (virtual) character as a character which is the difference of 2 unramified characters of representations. It is clear that such a character has a trivial conductor. The converse however is false, for the difference of two ramified characters can well have a trivial conductor.

Thus unramified characters are the characters which can be factored through a finite unramified extension. In the same way, we define a tame character to be a character which factors through a finite tame extension.

§2. Local Gauss sums

In this section, p is a fixed prime number and K a finite extension of the field $\mathbb{Q}_p$ of p-adic numbers. Let O_K (resp. $\mathcal{P}_K$, $\mathcal{D}_K$, U_K) be the valuation ring of K (resp. the maximal ideal of O_K, the different of the extension $K/\mathbb{Q}_p$, the group of units of O_K). For any integer $i \geq 0$, let U_K^i be the subgroup of those units of K which are congruent to 1 modulo $\mathcal{P}_K^i$ (thus, $U_K^0 = U_K$). We denote by π_K a uniformizing parameter of O_K ($\mathcal{P}_K = \pi_K O_K$).

We first define the non trivial additive character $\psi : K \to \mathbb{C}^*$ as the composition of the following 4 maps:

$$K \xrightarrow{(1)} \mathbb{Q}_p \xrightarrow{(2)} \mathbb{Q}_p/\mathbb{Z}_p \xrightarrow{(3)} \mathbb{Q}/\mathbb{Z} \xrightarrow{(4)} \mathbb{C}^*, \quad \text{where:}$$

(1) is the trace $Tr_{K/\mathbb{Q}_p}$

(2) is the canonical surjection

(3) is the canonical injection which maps $\mathbb{Q}_p/\mathbb{Z}_p$ onto the p-component of the divisible group $\mathbb{Q}/\mathbb{Z}$

(4) is the exponential map $x \mapsto e^{2\pi i x}$.

For every $x \in \mathbb{Q}_p$, there is a rational r, uniquely defined modulo 1, such that $x - r \in \mathbb{Z}_p$. Then $\psi(x) = \psi(r) = e^{2\pi i r}$.

The equality $\psi(x+y) = \psi(x)\psi(y)$ shows that $\psi(-x) = \psi(x)^{-1} = \overline{\psi(x)}$ for every $x \in K$. We also remark that ψ is trivial on the codifferent $\mathcal{D}_K^{-1}$, and that $\mathcal{D}_K^{-1}$ is actually the greatest ideal of K on which ψ is trivial.

The following lemma will be used to establish a basic property of Gauss sums.

Lemma 2.1. Let $n \geq 0$ be an integer and let d be an element of $\mathcal{D}_K^{-1} N(\mathfrak{p}_K)^{-n}$. Let S be a set of representatives of O_K modulo $\mathfrak{p}_K^n$. Then, the sum $\lambda = \sum_{y \in S} \psi(yd)$ does not depend on the particular choice of S. Moreover, $\lambda = N(\mathfrak{p}_K)^n$ if $d \in \mathcal{D}_K^{-1}$, and $\lambda = 0$ otherwise.

(For an ideal I, N(I) denotes the unique power of p which generates the ideal $N_{K/\mathbb{Q}_p}(I)$; if I is integral, $N(I) = \mathrm{card}(O_K/I)$).

Proof If $y' \equiv y \bmod \mathfrak{p}_K^n$, then $\psi(yd)\,\psi(y'd)^{-1} = \psi((y-y')d) = 1$; thus, λ does not depend on the choice of S. If $d \in \mathcal{D}_K^{-1}$, then $\psi(yd) = 1$ and

$$\lambda = \sum_{y \in O_K/\mathfrak{p}_K^n} 1 = N(\mathfrak{p}_K)^n.$$

Suppose now that d does not belong to $\mathcal{D}_K^{-1}$. For any integral z, y+z runs through a full set of representatives of O_K modulo $\mathfrak{p}_K^n$ when y does. Thus $\lambda = \sum_{y \in O_K/\mathfrak{p}_K^n} \psi((y+z)d) = \sum_{y \in O_K/\mathfrak{p}_K^n} \psi(yd)\psi(zd) = \psi(zd)\lambda$, and $(1-\psi(zd))\lambda = 0$. As ψ is not trivial on the ideal dO_K, one can choose z such that $\psi(zd) \neq 1$. Hence, $\lambda = 0$.

Now let $\theta: K^* \to \mathbb{C}^*$ be a character of K^* with open kernel. Let $n = n(\theta)$ be the valuation of the conductor $\mathfrak{f}(\theta)$ of θ, so that $\mathfrak{f}(\theta) = \mathfrak{p}_K^n$. The integer n is the least integer such that the character θ is trivial on the group U_K^n.

We say that θ is unramified if $n(\theta) = 0$. Then, for a non zero fractional ideal I, the value $\theta(x)$ of θ on a generator x of I does not depend on the choice of x; we call it $\theta(I)$.

<u>Definition</u> The local Gauss sum $\tau(\theta)$ is the sum

$$\tau(\theta) = \sum_{x \in U_K/U_K^n} \theta\left(\frac{x}{c}\right) \psi\left(\frac{x}{c}\right) ,$$

where c is a generator of the ideal $\mathcal{D}_\theta = \mathfrak{f}(\theta)\,\mathcal{D}_K$, and x runs through a set of representatives of U_K modulo U_K^n.

When θ is unramified, the sum reduces to 1 term, and we have the equality

$$\tau(\theta) = \theta(\mathcal{D}_K^{-1}) .$$

If moreover K is an unramified extension of $\mathbb{Q}_p$, then $\tau(\theta) = 1$.

<u>Remark</u> It is easily verified that $\tau(\theta)$ does not depend

on the choice of the representatives of U_K mod U_K^n. Hence, $\tau(\theta)$ does not depend on the choice of c.

Proposition 2.2. Let θ be a character of K^*. Then:

(i) $|\tau(\theta)| = \sqrt{N(\mathfrak{f}(\theta))}$

(ii) $\tau(\theta)\ \tau(\bar{\theta}) = \theta(-1)\ N(\mathfrak{f}(\theta))$.

Proof We first remark that (ii) is an easy consequence of (i), since

$$\tau(\bar{\theta}) = \sum_x \bar{\theta}(\tfrac{x}{c})\ \psi(\tfrac{x}{c}) = \sum_x \bar{\theta}(-\tfrac{x}{c})\ \psi(-\tfrac{x}{c})$$

$$= \bar{\theta}(-1) \sum_x \bar{\theta}(\tfrac{x}{c})\ \bar{\psi}(\tfrac{x}{c})$$

$$= \theta(-1)\ \overline{\tau(\theta)}.$$

Moreover, if θ is unramified, then $N(F(\theta)) = 1$ and

$$\tau(\theta)\ \overline{\tau(\theta)} = \theta(\mathcal{D}_K^{-1})\ \overline{\theta(\mathcal{D}_K^{-1})} = 1.$$

We now only have to prove (i) for a ramified character. We write $|\tau(\theta)|^2 = \tau(\theta)\ \overline{\tau(\theta)}$ as a double sum:

$$\tau(\theta)\ \overline{\tau(\theta)} = \sum_{x,y\in U_K/U_K^n} \theta(\tfrac{x}{c})\ \psi(\tfrac{x}{c})\ \bar{\theta}(\tfrac{y}{c})\ \bar{\psi}(\tfrac{y}{c}) .$$

Now, $\bar{\theta}(\frac{x}{c}) = \theta^{-1}(\frac{x}{c})$ and $\bar{\psi}(\frac{x}{c}) = \psi(-\frac{x}{c})$; replacing x by xy, we get the equality

$$\tau(\theta)\ \overline{\tau(\theta)} = \sum_{x,y} \theta(\tfrac{xy}{c})\ \theta^{-1}(\tfrac{y}{c})\ \psi(\tfrac{xy}{c})\ \psi(-\tfrac{y}{c})$$

$$= \sum_{x,y} \theta(x)\ \psi(y(\tfrac{x-1}{c}))$$

$$= \sum_{x} \theta(x)\ \Phi(x), \quad \text{where}$$

$$\Phi(x) = \sum_{y\varepsilon U_K/U_K^n} \psi(y(\tfrac{x-1}{c})).$$

We now write $\Phi(x)$ as the difference $\sum_{y\varepsilon O_K/p_K^n} \psi(y(\frac{x-1}{c}))$ - $\sum_{y\varepsilon p_K/p_K^n} \psi(y(\frac{x-1}{c}))$. By lemma 2.1., $\sum_{y\varepsilon O_K/p_K^n} \psi(y\ \frac{(x-1)}{c}) = 0$ if $x \not\equiv 1 \bmod p_K^n$, and $N(p_K)^n = N(\mathfrak{f}(\theta))$ otherwise; similarly,

$$\sum_{y\varepsilon p_K/p_K^n} \psi(y(\tfrac{x-1}{c})) = \sum_{y\varepsilon O_K/p_K^{n-1}} \psi(y\ \tfrac{(x-1)\pi_K}{c}) = 0 \text{ if } x \not\equiv 1$$

mod p_K^{n-1}, and $N(p_K)^{n-1}$ otherwise. We thus have the equality $|\tau(\theta)| = N(\mathfrak{f}(\theta)) - \sum_{x\varepsilon U_K^{n-1}/U_K^n} \theta(x)\ N(p_K)^{n-1}$, and we must prove that the sum $\mu = \sum_{x\varepsilon U_K^{n-1}/U_K^n} \theta(x)$ is zero. But, for any $z \in U_K^{n-1}$, $\theta(z)\,\mu = \sum_{x \in U_K^{n-1}/U_K^n} \theta(xz) = \mu$. By the definition of the conductor, there exist $z \in U_K^{n-1}$ such that $\theta(z) \neq 1$. Hence, $\mu = 0$, Q.E.D.

We can now define the local root numbers. Let K be a local field of characteristic 0, and let θ be a character of K^*.

Definition * For $K = \mathbb{R}$ or $K = \mathbb{C}$, define $W(\theta) = i^{-n(\theta)}$, where $n(\theta)$ is the integer defined in section 1.

* For K non archimedean, define $W(\theta) = \dfrac{\tau(\bar{\theta})}{\sqrt{N(\mathfrak{f}(\theta))}}$.

We now explain the connection between these local root numbers and the root number defined by Hecke for abelian L functions.

Let K be a number field, and let χ be an idèle class character (i.e., : χ is a continuous character on the group I_K of the idèles of K, trivial on the principal idèles). For every place v of K, the natural imbedding $K_v^* \to I_K$ defines a character χ_v on K_v^*. The following theorem was proved by Tate in 1950.

<u>Theorem</u> 2.3 $W(\chi) = \prod_v W(\chi_v)$.

For a proof, see Tate's thesis, in Cassels-Fröhlich, p. 305-347. (Note that the infinite product makes sense because $\tau(\chi_p) = N(\mathfrak{f}(\chi_p)) = 1$ for every finite prime p at which both the character χ and the extension $K/\mathbb{Q}$ are unramified).

§3. The transfer

Given a group G, we denote by G^{ab} the quotient of G by its commutator subgroup. Let G be a group and let H be a subgroup of finite index in G. Let $\theta : G/H \to H$ be a set of representatives for the left cosets of G modulo H. Given $s \in G$ and $t \in G/H$, we define an element $a_{s,t}$ of H by the formula:

$$s\,\theta(t) = \theta(st)a_{s,t}.$$

<u>Definition</u> Let $\bar{s} \in G^{ab}$, and let $s \in G$ be a representative of s. The image in H^{ab} of the element $\prod_{t\in G/H} a_{s,t}$ of H is called the transfer of $\bar{s}$.

<u>Notation</u> $Ver_G^H(\bar{s})$ or simply $Ver(\bar{s})$; we also define the transfer of s itself by $Ver(s) = Ver(\bar{s})$.

It can be shown that Ver(s) does not depend on the choices made in the definition, and that the transfer is a homomorphism of G^{ab} into H^{ab}. By duality, given an abelian group A, there is a transfer Ver : Hom(H,A) $\to$ Hom(G,A).

The transfer was first defined by Schur, and rediscovered by Artin in connection with class field theory. We shall use the transfer for its role in class field theory and for the calculation of the determinant of an induced representation.

a) Class field theory. For convenience, we use infinite Galois groups. For a topological group G, the group G^{ab} is the quotient of G by the closure of its commutator subgroup.

Proposition 3.1. The following two diagrams are commutative:

$$\begin{array}{ccc} \mathrm{Gal}(\bar{\mathbb{Q}}_p/K)^{ab} & \xrightarrow{\text{Ver}} & \mathrm{Gal}(\bar{\mathbb{Q}}_p/E)^{ab} \\ \uparrow & & \uparrow \\ K^* & \xrightarrow{\text{inclusion}} & E^* \end{array} \qquad \begin{array}{ccc} \Omega_K^{ab} & \xrightarrow{\text{Ver}} & \Omega_E^{ab} \\ \uparrow & & \uparrow \\ I_K & \xrightarrow{\text{inclusion}} & I_E \end{array}$$

local "global" (idèles)

In both diagrams, the vertical maps are Artin maps.

In the left hand diagram, E/K is a finite extension of fields of finite degree over $\mathbb{Q}_p$, contained in a given algebraic closure $\bar{\mathbb{Q}}_p$ of $\mathbb{Q}_p$.

In the right hand diagram, E/K is a finite extension of number fields, and I_K, I_E are the corresponding idèle groups.

We shall write $\mathrm{Ver}_{E/K}$ for the transfers involved in these 2 diagrams.

Proof This is a property of class formations (see e.g. Artin-Tate, Class Field Theory, chap. XIV, or Serre, Corps Locaux, chap. XI).

b) Induced representations. Given a representation ρ of a finite group G in a complex vector space V, the determinant of ρ depends only on the character of ρ. By linearity, we define the determinant of any virtual character χ of G. (Notation : $\det_\chi$).

Proposition 3.2. Let G be a finite group and let H be a subgroup of G. Let χ be a character of H, and let χ^* be the character of G induced by χ. For any element $s \in G$, let $\varepsilon_{G/H}(s)$ be the signature of the permutation of G/H defined by multiplication by s. Then:

$$\det_{\chi^*}(s) = \varepsilon_{G/H}(s)^{\chi(1)} \det_{\chi}(\mathrm{Ver}_G^H(s)) ,$$

or, more briefly:

$$\det_{\chi^*} = \varepsilon_{G/H}^{\chi(1)} \circ \mathrm{Ver}(\det_{\chi}).$$

<u>Proof</u> By linearity, we may assume that χ and χ^* are characters of representations. Thus, χ^* corresponds to a vector space V with G action, and χ to a subspace W of V invariant under H. The fact that the representation afforded by V is induced by the representation afforded by W can be described in the following way. Let $\theta = G/H \to G$ be a set of representatives of left cosets of G mod H. Let $W_\sigma = \theta(\sigma)\, W$. Then, V is the direct sum: $V = \bigoplus_{\sigma \in G/H} W_\sigma$. We must now find the determinant of the endomorphism $x \to sx$ of V for every $s \in G$. Write $x = \sum_{\sigma \in G/H} \theta(\sigma)\, x_\sigma$, with $x_\sigma \in W$. Then, $sx = \sum_{\sigma \in G/H} s\, \theta(\sigma) x_\sigma = \sum_{\sigma \in G/H} \theta(s\sigma)\, a_{s,\sigma} x_\sigma$. Thus, the map $x \to sx$ is the product vu, where u, defined by $\theta(\sigma)x_\sigma \mapsto \theta(\sigma)a_{s,\sigma}x_\sigma$, maps each W_σ onto itself, and v, defined by $\theta(\sigma)\, x_\sigma \mapsto \theta(s\,\sigma)\, \theta(\sigma)^{-1}\, x_\sigma$, maps $W_\sigma = \theta(\sigma)\, W$ onto $\theta(s\sigma)\, W$.

Now, everything is easy: first $\det_V(u) = \prod_{\sigma\in G/H} \det_{W_\sigma}(u|W_\sigma)$ $= \prod_{\sigma} \det_W(x \to a_{s,\sigma}x) = \det_W(x \to \prod_{\sigma} a_{s,\sigma}x) = \det_\chi(\mathrm{Ver}(s))$. Now let e_i $(1 \leqslant i \leqslant \chi(1))$ be a basis of W. Consider the basis $\theta(\sigma)e_i$ $(\sigma \in G/H,\ 1 \leqslant i \leqslant \chi(1))$ of V. For each i, v permutes the $\theta(\sigma)e_i$, and the signature of the permutation is $\varepsilon_{G/H}(s)$. As there are $\chi(1)$ indices i, $\det_V(v) = \varepsilon_{G/H}(s)^{\chi(1)}$, Q.E.D.

Corollary. If χ is a character of trivial determinant and of degree zero, so is the induced character χ^*.

§4. Local Galois Gauss sums

(θ non abélien)

Let p be a place of $\mathbb{Q}$, and let $\bar{\mathbb{Q}}_p$ be an algebraic closure of $\mathbb{Q}_p$ (thus, $\mathbb{Q}_\infty = \mathbb{R}$ and $\bar{\mathbb{Q}}_\infty = \mathbb{C}$). By a local field, we mean a finite extension of $\mathbb{Q}_p$ which is contained in $\bar{\mathbb{Q}}_p$. Given a local field K, we consider virtual characters of $\mathrm{Gal}(\bar{\mathbb{Q}}_p/K)$ which are differences of two characters of representations of open kernel. We simply write G_K for the Galois group $\mathrm{Gal}(\bar{\mathbb{Q}}_p/K)$.

For a local field K and a (virtual) character θ of G_K, Deligne and Langlands defined a local root number $W(\theta)$ (see Tate's lecture cf. [14]). The local root number is well defined by the following three properties:

(i) $W(\theta_1 + \theta_2) = W(\theta_1)\, W(\theta_2)$.

(ii) Let θ be a irreducible character of degree one, and let θ' be the character of K^* defined by θ via the Artin map. Then, $W(\theta)$ is the local root number $W(\theta')$ defined in section 2.

(iii) Let E be a finite extension of K, let θ be a character of degree zero of G_E and let θ^* be the character of G_K induced by θ. Then $W(\theta^*) = W(\theta)$.

We are now able to define the local Galois Gauss sum.

Definition Let K be a non archimedean local field, and let θ be a character of $\mathrm{Gal}(\bar{\mathbb{Q}}_p/K)$. The local Galois Gauss sum $\tau(\theta)$ is defined by the formula:

$$\tau(\theta) = W(\bar{\theta})\sqrt{N(\mathfrak{f}(\theta))},$$

where $\mathfrak{f}(\theta)$ is the Artin conductor of θ and the square root is the positive square root.

Note that $\mathfrak{f}(\bar{\theta}) = \mathfrak{f}(\theta)$. Hence

$$W(\theta) = \frac{\tau(\bar{\theta})}{\sqrt{N(\mathfrak{f}(\theta))}}.$$

The local Galois Gauss sum is well defined by the following three properties which are obvious consequences of the corresponding properties for local root numbers and conductors:

(i) $\tau(\theta_1 + \theta_2) = \tau(\theta_1)\ \tau(\theta_2)$.

(ii) Let θ be an irreducible character of degree one, and let θ' be the character of K^* defined by θ via the Artin map. Then, $\tau(\theta) = \tau(\theta')$, the local Gauss sum defined in section 2.

(iii) Let E be a finite extension of K, let θ be a character of degree 0 of G_E and let θ^* be the character of G_K induced by θ. Then $\tau(\theta^*) = \tau(\theta)$.

Notation. Given a local field K, an element $x \in K^*$ and an irreducible character of degree one θ of G_K, we write $\theta(x)$ for the element $\theta(\omega)$, where $\omega \in G_K^{ab}$ is the image of x under the Artin map.

Proposition 4.1. Let K be a finite extension of $\mathbb{Q}_p$, and let θ be a character of G_K. Then:

(i) $|\tau(\theta)| = \sqrt{N(\mathfrak{f}(\theta))}$

(ii) $\tau(\theta)\ \tau(\bar{\theta}) = N(\mathfrak{f}(\theta))\ \det_\theta(-1)$.

The following corollary is an easy consequence of the above proposition for an extension of $\mathbb{Q}_p$, and is obvious for $K = \mathbb{R}$ or $K = \mathbb{C}$:

Corollary. Let K be a local field. Then:

(i) $|W(\theta)| = 1$

(ii) $W(\theta)\, W(\bar{\theta}) = \det_\theta(-1)$.

Proof. We have only to prove the proposition when θ is an irreducible character of degree 1, and show that the 2 sides of the equalities are invariant under induction for characters of degree zero. Now, the case of an irreducible character of degree 1 has already been dealt with in §2, and both sides of the above equalities are invariant under induction when θ is of degree 0 (for (ii), just remark that $(\bar{\theta})^* = \bar{\theta}^*$).

Remark. Using part (ii) of proposition 4.1., one proves immediately the formula

$$W(\theta)\ \tau(\theta) = \det_\theta(-1)\sqrt{N(\mathfrak{f}(\theta))}\ .$$

§5. Galois action on Galois Gauss sums and root numbers (local theory)

Let K be local field, and let θ be a character of G_K. The values of θ are algebraic numbers. For any $\omega \in \Omega_{\mathbb{Q}}$ = Gal($\bar{\mathbb{Q}}/\mathbb{Q}$), we define θ^{ω} by the formula: $\theta^{\omega}(s) = (\theta(s))^{\omega}$ for every $s \in G_K$. We do not worry about left or right action of G_K as the results we are going to prove do not depend on the choice we make.

The aim of this section is to compute $W(\theta^{\omega})$ in terms of $W(\theta)$ and the theorem we shall prove is just a local version of a global theorem of Fröhlich. For an archimedean local field, $\theta^{\omega} = \theta$, and there is nothing to do. We thus restrict ourselves to finite extensions of $\mathbb{Q}_p$, p finite.

Now, $\tau(\theta)$ is an algebraic number: for a character of degree one, this is clear from the definition, and the general case is a consequence of the induction formula. Therefore, $W(\theta)$ itself is an algebraic number. We shall now compare $\tau(\theta^{\omega})$ with $\tau(\theta)^{\omega}$.

We first define a homomorphism u_p of $\Omega_{\mathbb{Q}} = \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ into U_p, the group of p-adic units.

Definition. Given $\omega \in \Omega_{\mathbb{Q}}$, $u_p(\omega)$ is the unique p-adic unit such that $\eta^{\omega^{-1}} = \eta^{u_p(\omega)}$, for every p^n-th root of unity η in $\bar{\mathbb{Q}}$. For any extension K of $\mathbb{Q}_p$, we view u_p as a homomorphism of $\Omega_{\mathbb{Q}}$ into K^*.

Theorem 5.1. Let K be a finite extension of $\mathbb{Q}_p$ for some finite p, and let θ be a character of G_K. Then, for any $\omega \in \Omega_{\mathbb{Q}}$,

$$\tau(\theta^{\omega^{-1}})^{\omega} = \tau(\theta)\ \det_{\theta}\ (u_p(\omega)).$$

Proof. The proof is in 2 steps.

Step 1. Let θ be a character of degree 0, and let F be a subfield of K. Assuming the formula is true for θ, we prove it for the character θ^* of G_F induced by θ. For the right hand side, observe that $\tau(\theta^*) = \tau(\theta)$ and that $\det_{\theta^*}(u_p(\omega)) = \det_{\theta}(u_p(\omega))$ by propositions 3.1. and 3.2. . For the left hand side notice that $(\theta^*)^{\omega^{-1}} = (\theta^{\omega^{-1}})^*$, hence $\tau(\theta^{*\omega^{-1}})^{\omega} = \tau((\theta^{\omega^{-1}})^*)^{\omega} = \tau(\theta^{\omega^{-1}})^{\omega}$.

Step 2. We prove the formula for an irreducible character of degree 1. Regarding θ as a character on K^*, we write, with the notation of §2, $\tau(\theta) = \sum_{x \in U_K/U_K^n} \theta(\frac{x}{c})\ \psi(\frac{x}{c})$. Then:

$$\tau(\theta^{\omega^{-1}})^{\omega} = \sum_{x \in U_K/U_K^n} [\theta^{\omega^{-1}}(\frac{x}{c})\ \psi(\frac{x}{c})]^{\omega} = \sum_{x \in U_K/U_K^n} \theta(\frac{x}{c})\ \psi(\frac{x}{c})^{\omega}.$$

Now, $\psi(\frac{x}{c})$ is a p^n-th root of unity for some n. Thus,

$$\psi(\frac{x}{c})^{\omega} = \psi(\frac{x}{c})^{u_p(\omega^{-1})} = \psi(\frac{x}{c})^{u_p(\omega)^{-1}} = \psi(\frac{x}{c}\ u_p(\omega)^{-1}) .$$

Therefore,

$$\tau(\theta^{\omega^{-1}})^{\omega} = \sum_{x \in U_K/U_K^n} \theta(\frac{x}{c})\ \psi(\frac{x}{c}\ u_p(\omega)^{-1})$$

$$= \sum_{x \in U_K/U_K^n} \theta(\frac{x}{c}\ u_p(\omega))\ \psi(\frac{x}{c}) \text{ (by the transformation } x \mapsto x\ u_p(\omega))$$

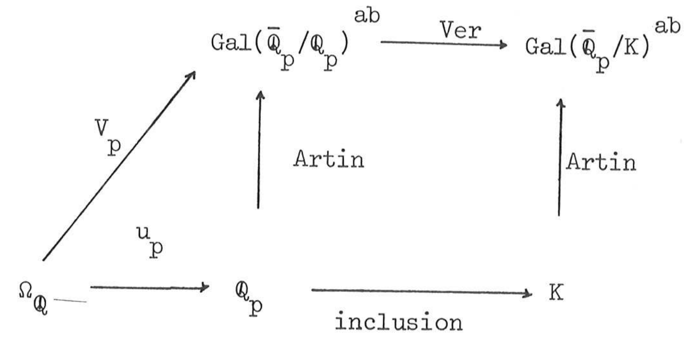
$$= \theta(u_p(\omega))\ \tau(\theta) = \tau(\theta)\ \det_\theta(u_p(\omega)), \quad \text{Q.E.D.}$$

We now state a corollary which is useful for the global theory. We defined a homomorphism $u_p : \Omega_{\mathbb{Q}} \to U_p \subset \mathbb{Q}_p^*$. By composition with the Artin map, we obtain a homomorphism $v_p : \Omega_{\mathbb{Q}} \to \mathrm{Gal}(\bar{\mathbb{Q}}_p/\mathbb{Q}_p)^{ab}$.

<u>Corollary</u> 5.2. The notation being as in the theorem,

$$\tau(\theta^{\omega^{-1}})^{\omega} = \tau(\theta)\ \det_{\theta}\ (\mathrm{Ver}_{K/\mathbb{Q}_p}(v_p(\omega))).$$

<u>Proof</u>. Obvious from the following commutative diagram:



<u>Remark</u> 1. Let ω' be an element in the inertia group of $G_{\mathbb{Q}_p}^{ab}$. As $\Omega_{\mathbb{Q}}^{ab}$ is abelian, this element ω' defines a unique element $\omega \in \Omega_{\mathbb{Q}}^{ab}$ via any imbedding of $\bar{\mathbb{Q}}$ in $\bar{\mathbb{Q}}_p$. To use the previous corollary, one must be able to compare ω' and $v_p(\omega)$. The result is actually the following one: $\omega' = v_p(\omega)$. The equality is true thanks to the minus sign in the definition of $u_p(\omega)$ (see Corps Locaux, last remark of chap. XIV, §7).

<u>Remark</u> 2. To finish this section, we come back to the root number itself. For any $\omega \in \Omega_{\mathbb{Q}}$, $\mathfrak{f}(\theta^{\omega}) = \mathfrak{f}(\theta)$. Thus, using the formula $W(\theta) = \dfrac{\tau(\bar{\theta})}{\sqrt{N(\mathfrak{f}(\theta))}}$, we see that theorem 5.1 gives a way of computing $W(\theta^{\omega})$ when $\mathfrak{f}(\theta)$ and

$W(\theta)$ are known. To express the result in terms of $W(\theta)$ itself, it is enough to know the action of ω on $\sqrt{N(\mathfrak{f}(\theta))}$.

The following proposition is obvious:

Proposition 5.3. Let θ be a character of G_K with trivial determinant. Assume that the norm of the conductor of θ is a square. Then, $W(\theta^\omega) = W(\theta)^\omega$.

§6. Real valued characters

In this section, K is a local field and θ a real valued character of G_K. The formula $W(\theta)\ W(\bar{\theta}) = \det_\theta(-1)$ reduces to $W(\theta)^2 = \det_\theta(-1)$. Thus, $W(\theta)$ is a fourth root of unity. Moreover, if $\det_\theta$ is trivial, then $W(\theta) = +1$ or -1.

The following two propositions give local versions of a global theorem of Fröhlich (see next section).

Proposition 6.1. Let K be a non archimedean local field, and let θ a real valued character of G_K with trivial determinant. Each of the following conditions implies the other:

(i) $W(\theta^\omega) = W(\theta)$ for every $\omega \in \Omega_{\mathbb{Q}}$

(ii) $\tau(\theta^{\omega}) = \tau(\theta)$ for every $\omega \in \Omega_{\mathbb{Q}}$

(iii) $\tau(\theta)$ is a rational number.

(iv) $N(\mathfrak{f}(\theta))$ is a square.

Proof. (i) => (ii). Since $\bar{\theta} = \theta$, $W(\theta) = \dfrac{\tau(\theta)}{\sqrt{N(\mathfrak{f})(\theta)}}$.

Since $\mathfrak{f}(\theta^{\omega}) = \mathfrak{f}(\theta)$, $\tau(\theta^{\omega}) = \tau(\theta)\,\dfrac{W(\theta^{\omega})}{W(\theta)} = \tau(\theta)$.

(ii) => (iii). By theorem 5.1., $\tau(\theta)^{\omega} = \tau(\theta^{\omega}) = \tau(\theta)$.

(iii) => (iv). $N(\mathfrak{f}(\theta)) = \dfrac{\tau(\theta)^2}{W(\theta)^2} = \tau(\theta)^2$.

(iv) => (i). Obvious by proposition 5.3.

Proposition 6.2. Let K be a non archimedean local field, and let θ be a real valued character of G_K. Assume moreover that θ is tame (i.e., θ factors through a finite tamely ramified extension). Then, the conductor of θ is a square, and therefore $W(\theta^{\omega}) = W(\theta)$ for every $\omega \in \Omega_{\mathbb{Q}}$.

Proof. We must prove that the integer $n(\theta)$ is even. We can view θ as a character of the Galois group of a finite tamely ramified extension E of K, and it is enough to give the proof when θ is a character of a representation ρ of G. Now, we know that $n(\theta)$ is the number of eigenvalues other than +1 of $\rho(\sigma)$, where σ is a generator of the inertia group. Let n^- be the number of eigenvalues of $\rho(\sigma)$ equal to -1. Since θ is real valued, the non real eigenvalues appear in pairs of conjugates; hence, $n(\theta) \equiv n^-$ mod 2. Now, the determinant of $\rho(\sigma)$ is the product of all eigenvalues of $\rho(\sigma)$. The product of the non real eigenvalues is +1. We thus have the equality $+1 = \det(\rho(\sigma)) = (-1)^{n^-}$. Hence, $n(\theta) \equiv n^- \equiv 0$ mod 2, Q.E.D.

Remark. Let θ be a character of a finite extension. The statement $W(\theta^\omega) = W(\theta)$ for every $\omega \in \Omega_{\mathbb{Q}}$ is equivalent to the following one : the value of $W(\theta)$ depends only on the simple factor of $\mathbb{Q}[G]$ corresponding to θ. Another example where this situation arises will be given in chapter III, §4.

§7. Global theory

In this section, K is a number field and χ is a virtual character of the infinite Galois group $\Omega_K = \mathrm{Gal}(\bar{\mathbb{Q}}/K)$ which factors through a finite extension of K.

The Galois Gauss sum was first defined by Hasse by a formula of the type $\tau(\chi) = W(\chi)\sqrt{\widetilde{N(\mathfrak{f}(\chi))}}$, where $W(\chi)$ is the Artin root number and the tilde means that one must first choose a sign for the absolute norm of the conductor and then extract an appropriate square root. Note that $\sqrt{N(\widetilde{\mathfrak{f}(\chi)})}$ is the product of the usual $\sqrt{N(\mathfrak{f}(\chi))}$ by a fourth root of unity. Following Fröhlich, we define this root of unity as an "infinite part" of the root number. Moreover, to be consistent with the preceding sections, we consider $W(\bar{\chi})$ instead of $W(\chi)$.

<u>Definition</u> 7.1. For every infinite place v of K, let $W_v(\chi) = i^{-n(\chi,v)}$, where $n(\chi,v)$ is the integer defined in §1. The infinite part of the root number is the complex number $W_\infty(\chi) = \prod_{v \text{ infinite}} W_v(\chi)$.

<u>Definition</u> 7.2. The Galois Gauss sum $\tau(\chi)$ is the complex number defined by

$$\tau(\chi) = W(\bar{\chi}) \sqrt{N(\mathfrak{f}(\chi))}\, W_\infty(\chi)^{-1} ,$$

where $W(\bar{\chi})$ is the Artin root number, and $\sqrt{N(\mathfrak{f}(\chi))}$ is the positive square root of the positive generator of the absolute norm of the Artin conductor.

Note that $\mathfrak{f}(\bar{\chi}) = \mathfrak{f}(\chi)$, and that $W_\infty(\bar{\chi}) = W_\infty(\chi)$ (For the latter equality, just remark that $n(\chi,v) = n(\chi_v)$, where χ_v is the local character on the completion of K at v defined by χ_v; hence, $\bar{\chi}_v = \chi_v$ and $W_v(\bar{\chi}_v) = W_v(\chi)$ for every infinite place v of K). Thus, the following equality holds:

$$W(\chi) = \frac{\tau(\bar{\chi})\ W_\infty(\chi)}{\sqrt{N(\mathfrak{f}(\chi))}}.$$

Remark (Exercise) $W(\chi)\ \tau(\chi) = \sqrt{N(\mathfrak{f}(\chi)}\ W_\infty(\chi)^{-1}$. (Hint: prove the equality $W_v(\chi)^2 = \det_{\chi_v}(-1)$ for any infinite place v).

Proposition 7.1. $$\tau(\chi) = \prod_{\mathfrak{p}\ \text{finite}} \tau(\chi_{\mathfrak{p}}),$$

where $\chi_{\mathfrak{p}}$ is the local character on the Galois group $G_{K_{\mathfrak{p}}} = \mathrm{Gal}(\bar{\mathbb{Q}}_p/K_{\mathfrak{p}})$ of the completion of K at $\mathfrak{p}$ ($\bar{\mathbb{Q}}_p$ is a given algebraic closure of $\mathbb{Q}_p$, and $\mathfrak{p}$ lies above p).

Proof. The Artin root number $W(\chi)$ is the product $\prod_v W(\chi_v)$ where v runs through all places of K (see J. Tate, Durham).

Now, $W_\infty(\chi) = \prod_{v\ \text{infinite}} W_v(\chi) = \prod_{v\ \text{infinite}} W(\chi_v)$.

Hence, $W(\bar{\chi})\ W_\infty(\chi)^{-1} = W(\bar{\chi})\ W_\infty(\bar{\chi})^{-1} = \prod_{\mathfrak{p}\ \text{finite}} W(\bar{\chi}_{\mathfrak{p}})$.

Now, the positive rational number $N(\mathfrak{f}(\chi))$ is also the product $\prod_{\mathfrak{p}\ \text{finite}} N(\mathfrak{f}(\chi_{\mathfrak{p}}))$. Therefore

$$\tau(\chi) = \frac{W(\bar{\chi})\ W_\infty(\bar{\chi})^{-1}}{\sqrt{N(\mathfrak{f}(\chi))}} = \prod_{p \text{ finite}} \frac{W(\bar{\chi}_p)}{\sqrt{N(\mathfrak{f}(\chi_p))}} = \prod_{p \text{ finite}} \tau(\chi_p)$$

We shall now use proposition 7.1. to derive global results from the local results of §5. and §6.

<u>Theorem</u> 7.2. (Fröhlich) For every $\omega \in \Omega_{\mathbb{Q}}$,

$$\tau(\chi^{\omega^{-1}})^{\omega} = \tau(\chi)\ \det_{\chi}(\mathrm{Ver}_{K/\mathbb{Q}}(\omega)) .$$

<u>Proof</u>. For every finite prime p of K, $(\chi_p)^{\omega^{-1}} = (\chi^{\omega^{-1}})_p$; hence,

$$\frac{\tau(\chi^{\omega^{-1}})^{\omega}}{\tau(\chi)} = \prod_{p \text{ finite}} \frac{\tau(\chi_p^{\omega^{-1}})^{\omega}}{\tau(\chi_p)} = \prod_{p \text{ finite}} \det_{\chi_p}(\mathrm{Ver}_{K_p/\mathbb{Q}_p} V_p(\omega))$$

with the notation of corollary 5.2.

The theorem we want to prove is now a consequence of the following lemma of class field theory.

<u>Lemma</u> 7.3. For any irreducible character of degree one ψ of Ω_K,

$$\psi(\mathrm{Ver}_{K/\mathbb{Q}}(\omega)) = \prod_{p \text{ finite}} \psi_p(\mathrm{Ver}_{K_p/\mathbb{Q}_p}(V_p(\omega))).$$

<u>Proof of the lemma</u>. When $K = \mathbb{Q}$, the formula we want to

prove is simply

$$\left[\ \psi(\omega) = \prod_{p \text{ finite}} \psi_p(V_p(\omega)) \text{ for any } \omega \in \Omega_{\mathbb{Q}}^{ab} .\ \right]$$

It is a consequence of the discussion of the reciprocity law over the rationals (see Artin-Tate's notes, chap. 6. §2). The general case is an easy consequence of the commutative diagram of §3.

__Remark.__ Theorem 7.2. can be stated in terms of idèles. Define $u : \Omega_{\mathbb{Q}} \to I_{\mathbb{Q}}$ by $u_\infty = 1$ and $u(\omega)_p = u_p(\omega)$ for every finite prime p. Then:

$$\tau(\chi^{\omega^{-1}})^{\omega} = \tau(\chi)\ \det_\chi(u(\omega)) ,$$

where $\det_\chi(x)$ for an idèle x is simply the value of $\det_\chi$ on the element $s \in \Omega_K^{ab}$ which is the image of x under the Artin map.

The particular case of tame and real valued characters can be dealt with easily, as in the local case. We obtain the following theorem due to Fröhlich.

__Theorem__ 7.4. Let K be a number field, and let χ be a character of Ω_K. Assume that χ is tame and real valued. Then, the following results hold:

(i) For every $\omega \in \Omega_K$, $W(\chi^\omega) = W(\chi)$

(ii) $\tau(\chi)/\ \tau(\det_\chi)$ is a rational number

(iii) $W_\infty(\chi)/W_\infty(\det_\chi) = +1$ or -1

(iv) if χ is a character with trivial determinant, then $\tau(\chi)$ is a rational number whose sign is the product of the signs of $W(\chi)$ and $W_\infty(\chi)$.

Proof As χ factors through a tamely ramified extension, so does $\det_\chi$. By additivity, $\tau(\chi)/\tau(\det_\chi) = \tau(\chi\text{-}\det_\chi)$ and $W_\infty(\chi)/W_\infty\ (\det_\chi) = W_\infty(\chi\text{-}\det_\chi)$. As $\chi\text{-}\det_\chi$ has trivial determinant, it is enough to prove (ii) and (iii) for a character with trivial determinant.

Now, for every finite prime p of K, χ_p is a tame real valued character with trivial determinant. Hence, by propositions 6.1. and 6.2., $\tau(\chi_p)$ is rational. As $\tau(\chi_p) = +1$ for almost all p, $\tau(\chi) = \prod_p \tau(\chi_p)$ is rational. We have thus proved (ii). Moreover, $N(\mathfrak{f}(\chi)) = \prod_p N(\mathfrak{f}(\chi_p))$ is a square by proposition 6.2. As χ is real valued, $W(\chi) = +1$ or -1. Hence, $W_\infty(\chi) = \frac{W(\chi)\sqrt{N(\mathfrak{f}(\chi))}}{\tau(\chi)}$ is a rational number. As it is a 4^{th} root of unity, $W_\infty(\chi) = +1$ or -1, and this proves the assertions (iii) and (iv).

We must now prove (i). We need the following lemma:

Lemma 7.5. Let ψ be a homomorphism of Ω_K into $\{-1,+1\}$. Then $W(\psi) = +1$.

Proof of the lemma. We know that the Artin root number of a zeta function is +1. If ψ is trivial, $L(s,\psi) = \zeta_K(s)$, hence $W(\psi) = +1$. If ψ is not trivial, then ψ corresponds to a quadratic extension E/K, and $L(s,\psi) = \zeta_E(s)/\zeta_K(s)$. Thus, $W(\psi) = W(\zeta_E)/W(\zeta_K) = +1$.

Proof of (i). Let $\omega \in \Omega_K$. By the above lemma, $W(\det_\chi) = W(\det_{\chi^\omega}) = +1$. Hence, $W(\chi^\omega) = W((\chi - \det_\chi)^\omega)$ and $W(\chi) = W(\chi - \det_\chi)$. We may therefore assume that χ is a character with trivial determinant. We now use the formula

$$W(\chi) = \prod_v W(\chi_v)$$

where v runs through all places of K. By the results of §6., $W(\chi_v^\omega) = W(\chi_v)$. Hence, $W(\chi^\omega) = \prod_v W(\chi_v) = W(\chi)$, Q.E.D.

Remark. Without the assumption that χ is tame conclusions (i), (ii) and (iv) of the theorem are no longer valid. See e.g. [7a] §9, or [7b] Theorem 19.

§8. Global induction formulae

We give in this section induction formulae for the infinite part of the root number and the Galois Gauss sum. These formulae were originally used by Fröhlich to prove the results of §7. We give them for their own interest.

Definition. Let K be a number field. For any finite extension E of K and any place at infinity v of K, define

$t(E/K,v) = 0$ if v is complex,

$t(E/K,v) =$ the number of complex places of E lying above v if v is real.

Put $t(E/K) = \sum_{v \text{ real}} t(E/K,v)$.

Theorem 8.1. Let E be finite normal extension of a number field K with Galois group G. Let H be a subgroup of G corresponding to a field F. Let χ be a character of H, and let χ^* be the character of G induced by χ.

(i) For every place v of K,

$$n(\chi^*,v) = \sum_{\substack{w \mid v \\ w \text{ in } F}} n(\chi, w) + \chi(1)\, t(F/K,v)$$

(ii) $W_\infty(\chi^*) = W_\infty(\chi)\, i^{-\chi(1)\, t(F/K)}$

(iii) $\tau(\chi^*) = \tau(\chi).[N(D(F/K))^{\frac{1}{2}} \,.\, i^{t(F/K)}]^{\chi(1)}$, where $N(D(F/K))$ is the absolute norm of the discriminant of F over K.

Proof. (ii) is an obvious consequence of (i), and (iii) is easily deduced from (ii): write

$$\frac{\tau(\chi^*)}{\tau(\chi)} = \frac{W(\chi^*)}{W(\chi)} \left[\frac{N(\mathfrak{f}(\chi^*))}{N(\mathfrak{f}(\chi))}\right]^{\frac{1}{2}} \left[\frac{W_\infty(\chi^*)}{W_\infty(\chi)}\right]^{-1}.$$

Then, $W(\chi^*) = W(\chi)$, $\dfrac{W_\infty(\chi^*)}{W_\infty(\chi)} = i^{-t(F/K)\chi(1)}$ by (ii) and the

equality $\dfrac{N(\mathfrak{f}(\chi^*))}{N(\mathfrak{f}(\chi))} = N(D(F/K))^{\chi(1)}$ is an easy consequence of the calculation of the conductor of an induced character.

We are now left with the proof of (i). If χ is of degree zero, the formula we want to prove is:

$$n(\chi^*, v) = \sum_{\substack{w|v \\ w \text{ in } F}} n(\chi, w).$$

But $n(\chi, w) = n(\chi_w)$ and $n(\chi^*, v) = n((\chi^*)v)$. Thus, the desired formula is a consequence of the formula which gives the restriction of an induced representation (see e.g. Serre, Représentations linéaires des groupes finis, chap. 7, prop. 22). It is thus enough to prove (i) when χ is the unit character.

Since $n(\chi,w) = 0$, formula (i) can be written

$$n(\chi^*, v) = t(F/K, v).$$

The equality is obvious when v is complex. Assume v is real, and let σ be the "Frobenius" of a place w above v in E. Then, $n(\chi^*, v) = \frac{1}{2}(\chi^*(1) - \chi^*(\sigma))$. Now $\chi^*(1) = [F:K]$, and $\chi^*(\sigma) = \sum_{t\epsilon G/H} \chi(t\sigma t^{-1})$. But $\chi(t\sigma t^{-1}) = 1$ if tw lies above a real place of F (for $t\sigma t^{-1} \epsilon H$) and $\chi(t\sigma t^{-1}) = 0$ otherwise. Hence, $\chi^*(1) - \chi^*(\sigma)$ is the number of elements of G mod H such that tw lies above a complex place of F, and this number is precisely $2t(F/K,v)$, Q.E.D.

III. ORTHOGONAL AND SYMPLECTIC REPRESENTATIONS

§1. Description of real valued characters

Let G be a finite group, and let K be a subfield of the field $\mathbb{C}$ of complex numbers. Given a finite dimensional K-vector space V and a representation $\rho : G \to Gl(V)$, we define a complex representation $\rho' : G \to Gl(\mathbb{C} \otimes_K V)$ by $\rho'_s(1 \otimes x) = 1 \otimes \rho_s(x)$. We call such a complex representation a K-representation.

Consideration of direct sums and tensor products of K-representations shows that the set R_G^K of characters of K-representations of G is a subring of the ring R_G of characters of G. Clearly, a character $\chi \in R_G^K$ has its values in K. The converse however is not true. We denote by $\bar{R}_G^K$ the subring of R_G which consists of characters of G with values in K.

We are interested in the case when $K = \mathbb{R}$, the field of real numbers. The rings $R_G^{\mathbb{R}}$ and $\bar{R}_G^{\mathbb{R}}$ are then related to geometrical invariants.

We denote by R_G^b the set of characters of R_G which are the difference of 2 characters of representations preserving a non degenerate bilinear form. We shall call a non-degenerate bilinear form orthogonal (resp. symplectic) if it is symmetric (resp. skew-symmetric). We define the subset R_G^o (resp. R_G^s) of R_G^b to be the set of characters $\chi \varepsilon \mathbb{R}_G$ which are differences of 2 characters of representations preserving an orthogonal (resp. symplectic) form. The virtual characters in R_G^o will be called orthogonal, those in R_G^s symplectic. The sets R_G^b, R_G^o and R_G^s are subgroups of R_G. Moreover, consideration of tensor products shows immediately that R_G^b and R_G^o are subrings of R_G, whereas R_G^s is a module over R_G^o. Note that every symplectic character has even degree and trivial determinant.

Let $T : R_G \to R_G$ be the map $\chi \longmapsto \chi + \bar{\chi}$.

<u>Theorem</u> 1.1.

(i) $R_G^b = \bar{R}_G^{\mathbb{R}}$

(ii) $R_G^o = R_G^{\mathbb{R}}$

(iii) $R_G^b = R_G^o + R_G^s$

(iv) $R_G^o \cap R_G^s = \mathrm{Im}\, T$.

For a proof, see e.g. Serre, [12], §13.

We can now define three (mutually exclusive) types of irreducible real valued characters.

Type 1. $\chi = \Phi + \bar{\Phi}$, where $\Phi \in R_G$ is absolutely irreducible and takes at least one non real value.

Type 2. χ is an absolutely irreducible character and is orthogonal.

Type 3. χ is an absolutely irreducible character and is symplectic.

These characters are irreducible real valued characters, and make a basis of $\bar{R}_G^{\mathbb{R}}$, from which bases of R_G^o and R_G^s are easily deduced.

Irreducible real valued characters are in one-to-one correspondence with the simple algebras which occur in a decomposition of the semi-simple algebra $\mathbb{R}(G)$. For χ of type (1), the centre of the corresponding algebra is $\mathbb{R}(\Phi) = \mathbb{C}$. Hence, the simple algebra corresponding to χ is isomorphic to $M_n(\mathbb{C})$ with $n = \chi(1)$. For χ of type (2), the corresponding simple algebra is obviously isomorphic to $M_n(\mathbb{R})$, with $n = \chi(1)$. Therefore, a character of type (3) corresponds to a simple algebra isomorphic to $M_n(\mathbb{H})$, where $\mathbb{H}$ denotes the skew-field of Hamilton quaternions and $2n = \chi(1)$. This last isomorphism can be described as follows: start with an absolutely irreducible symplectic representation $\rho : G \to Gl(V)$, where V is a complex vector space of dimension, say, 2n. Then ρ defines a representatio[n] $\rho_{\mathbb{R}} : G \to Gl(V_{\mathbb{R}})$ where $V_{\mathbb{R}}$ is the vector space V viewed as a real vector space (hence, $\dim V_{\mathbb{R}} = 4n$). Let D be the ring of those endomorphisms of $V_{\mathbb{R}}$ which commute with ρ_s for all $s \in G$. The ring D, which is a skew-field by Schur's lemma, is actually isomorphic to $\mathbb{H}$, and $V_{\mathbb{R}}$ can therefore be given a structure of $\mathbb{H}$-vector space of dimension n, say $V_{\mathbb{H}}$. Now the simple algebra corresponding to ρ is the ring $End_{\mathbb{H}}(V_{\mathbb{H}})$, isomorphic to $M_n(\mathbb{H})$.

§2. Induction theorems

a) The Brauer-Witt theorem Given a subfield K of $\mathbb{C}$ and a prime number p, one can define Γ_K-p-elementary groups, which are semi-direct products of a normal cyclic subgroup C of order prime to p by a p-group p (for a definition, see e.g. [12], §12). For $K = \mathbb{C}$, the semi-direct product is actually a direct product, and Γ_K-p-elementary groups are the "usual" elementary groups. For $K = \mathbb{R}$, the following condition must hold : for every $y \in P$, there exist $t \in \{-1, +1\}$, such that, for every $x \in C$, $yxy^{-1} = x^t$.

A group is called Γ_K-elementary if it is Γ_K-p-elementary for some p.

Theorem 2.1. (Brauer-Witt theorem) Every K-character of a finite group G is a $\mathbb{Z}$-linear combination of characters of the form $\mathrm{Ind}_H^G(\chi)$, where H is a Γ_K-elementary subgroup of G and χ is a K-character of H.

Remark. A Γ_K-elementary group is supersolvable (see the definition below). Hence, every irreducible character of H is induced by a character of degree one of some subgroup. Taking $K = \mathbb{C}$, one has the "usual" Brauer theorem used in chapter 1.

b) The Borel-Serre theorem. Call a group G supersolvable if there exists a sequence $\{e\} = G_o \subset G_1 \subset \ldots \subset G_{k-1} \subset G_k = G$ of normal subgroups of G such that G_i/G_{i-1} is cyclic.

The following theorem was proved by Borel and Serre in 1953 ([2]).

Theorem 2.2. (Borel-Serre theorem) Let L be a compact Lie group, and let G be a supersolvable subgroup of L.

Then, G is contained in the normalizer N of a maximal torus T of L.

We make a few comments on this theorem.

1) The inclusion $G \subset N$ simply means that, for every $s \in G$ and every $t \in T$, $sts^{-1} \in T$.

2) Two maximal tori of L are conjugate.

§3. Induction theorems for orthogonal characters

Definition The dihedral group D_{2n} of order 2n is the group on 2 generators σ and τ with relations $\sigma^n = \tau^2 = 1$, $\tau\sigma\tau^{-1} = \sigma^{-1}$. Note that it is the semidirect product of its subgroups generated by σ and by τ.

All the characters of D_{2n} are orthogonal. There are 2 (resp. 4) irreducible characters of degree one of D_{2n} if n is odd (resp. even). The remaining irreducible characters of D_{2n} are of degree 2.

Definition Let G be a finite group. An character χ of G is called a dihedral character if χ factors through a dihedral quotient of G and is irreducible of degree 2.

The following theorem is extracted from Serre's paper on Artin-conductors ([13] ; see also D. Quillen, [10], lemma 2.4).

<u>Theorem</u> 3.1. (Serre) Let G be a finite group, and let χ be an orthogonal character of G. Then, χ is a $\mathbb{Z}$-linear combination of characters of the form $\mathrm{Ind}_H^G(\Phi)$ where H is a subgroup of G and Φ satisfies one of the 3 following conditions:

(i) Φ is a homomorphism of H into $\{-1, +1\}$

(ii) $\Phi = \psi + \bar{\psi}$, where ψ is an irreducible character of degree one of H

(iii) Φ is a dihedral character of H.

<u>Proof</u>. By theorem 2.1, we may assume that G is a $\Gamma_{\mathbb{R}}$-elementary group and that χ is an irreducible orthogonal character. Since every $\Gamma_{\mathbb{R}}$-elementary group is supersolvable, theorem 3.1 is a consequence of the following more precise result for supersolvable groups.

<u>Theorem</u> 3.2. Let G be a finite supersolvable group and let χ be an irreducible orthogonal character of G. Then, one of the following conditions holds:

(i) χ is a homomorphism of G into $\{-1, +1\}$

(ii) $\chi = \psi + \bar{\psi}$, where ψ is induced by an irreducible character of degree 1 of some subgroup of G

(iii) χ is induced by a dihedral character of some subgroup of G.

<u>Proof</u>. Let $n = \chi(1)$. The character χ is the character of a representation $\rho : G \to Gl(V)$ where V is a real vector space of dimension n. The group $\rho(G)$ is contained in the orthogonal group O(V) of some positive definite bilinear form on V. By theorem 3.2, $\rho(G)$ is contained in the normalizer of a maximal torus T of O(V). Let $m = [\frac{n}{2}]$. There exists a subspace W of V of dimension 2m such that the matrix of T in a suitable basis $e_1, \ldots, e_{2m}$ of W is of the form

$$\begin{pmatrix} \boxed{SO_2} & & & 0 \\ & \boxed{SO_2} & & \\ & & \ddots & \\ 0 & & & \boxed{SO_2} \end{pmatrix}$$

Let w_i $(1 \leq i \leq m)$ be the subspace of W spanned by the vectors e_{2i-1}, e_{2i}. Now, there are two possibilities:

a) <u>n is odd</u>. Since W is invariant under the action of G, V contains an invariant subspace W' of dimension 1. Since ρ is irreducible, $W = (0)$ and $V = W'$. The character χ is then of type (i).

b) <u>n is even</u>. Let H be the subgroup of those elements $s \in G$ such that $\rho_s(W_1) \subset W_1$. Since $\rho(G)$ is contained in the normalizer of T, $\rho(G)$ permutes the subspaces W_i. Since ρ is irreducible, this permutation is transitive. This means that ρ is induced by the representation $\rho_1 : H \to Gl(W_1)$ deduced from ρ by restriction to H. But ρ_1 is a real representation. Therefore, $\rho_1(H)$ is isomorphic to a subgroup of $O_2(\mathbb{R})$ and χ is of type (iii) or (ii) according to whether ρ_1 is absolutely irreducible or not.

We shall now give a corollary of theorem 3.1. due to Deligne ([4] ; Deligne's paper also contains a purely group theoretic proof of theorem 3.1). We must first extend slightly the definition of a dihedral character : we consider that a character lifted from a character χ' of a quotient of G isomorphic to D_4 is a dihedral character if χ' is the sum of 2 distinct irreducible characters of degree 1.

Definition Let G be a finite group. Let χ be a dihedral character of G lifted from a character χ' of a dihedral quotient G' of G. Then, $\chi' = \mathrm{Ind}_{H'}^{G'}(\Phi')$, where H' is a cyclic subgroup of G' of index 2 and Φ' is an irreducible character of degree 1. We call r_χ the character of G lifted from $\mathrm{Ind}_{H'}^{G'}(\Phi'-1)$.

Note that r_χ has degree 0 and trivial determinant.

Theorem 3.3. (Deligne) Let G be a finite group. Every orthogonal character of G of degree 0 and trivial determinant is a $\mathbb{Z}$-linear combination of characters of the form $\mathrm{Ind}_H^G(\Phi)$ where Φ is either a character r_χ or a sum $\psi+\bar{\psi}$ with $\psi(1) = 0$.

Proof. Let χ be a character of G of degree 0 and trivial determinant. By Brauer-Witt's theorem, the unit character of G can be written as a sum $1 = \sum_H n_H \mathrm{Ind}_H^G(\Phi_H)$ where H ranges over the $\Gamma_{\mathbb{R}}$-elementary subgroups of G and Φ_H is an orthogonal character of H. Now, $\chi = \chi.1 = \sum_H n_H \mathrm{Ind}_H^G(\mathrm{Res}_G^H(\chi).\Phi)$. Since $\mathrm{Res}_G^H(\chi)$ has degree 0 and trivial determinant, so does $\mathrm{Res}_G^H(\chi).\Phi$. We may therefore assume that G is a $\Gamma_{\mathbb{R}}$-elementary group.

Let A be the subgroup of R_G^O generated by the characters of the form of theorem 3.3. With the notation of theorem 3.2, let B (resp. C, D) be the subgroup of R_G^o generated by characters of type (i) (resp. (ii), (iii)).

Lemma 3.4. If G is $\Gamma_{\mathbb{R}}$-elementary, then $R_G^o = A+B$.

Proof of lemma 3.4. It is enough to prove that every irreducible orthogonal character χ belongs to A+B. If $\chi(1) = 1$, there is nothing to prove. We can therefore prove the lemma by induction on $\chi(1)$. If $\chi \in C$, say $\chi = \mathrm{Ind}_H^G(\psi + \bar{\psi})$ with $\psi(1) = 1$, write

$$\chi = \mathrm{Ind}_H^G\ [(\psi(1) - 1) + \overline{(\psi(1)}] - 1) \ + 2.1^*.$$

Since $1^*(1) < \chi(1)$, the induction process works.

If $\chi \in D$, say $\chi = \mathrm{Ind}_H^G(\Phi)$ where Φ is a dihedral character, write $\Phi = r_\Phi + (\Phi - r_\Phi)$. Since $\Phi - r_\Phi$ contains the unit character, the induction process works.

Proof of theorem 3.3. By lemma 3.4., it is enough to show that any character $\chi \in B$ with degree 0 and trivial determinant belongs to A. Since $\chi(1) = 0$, we may write χ as a sum $\chi = \sum_{i=1}^{n} \varepsilon_i (\Phi_i - 1)$, where the Φ_i's are homomorphisms of G onto $\{-1,+1\}$ and $\varepsilon_i = +1$ or -1. Since

$2(\Phi_i - 1) = \overline{(\Phi_i - 1)} + (\Phi_i - 1) \in A$, we may assume that $\varepsilon_1 = \varepsilon_2 = +1$ and $\varepsilon_i = -1$ for $i \geq 3$. The result we want to prove is obvious for $n \leq 2$. For $n = 3$, $\chi = \Phi_1 + \Phi_2 - \Phi_3 - 1$. Since $\det_\chi$ is trivial, $\Phi_3 = \Phi_1 \Phi_2$. If $\Phi_1 = \Phi_2$, then $\chi = 2(\Phi_1 - 1) \in A$. If $\Phi_1 \neq \Phi_2$, let $H = \operatorname{Ker} \Phi_1 \cap \operatorname{Ker} \Phi_2$. Then, G/H is isomorphic to D_4, and $\psi = r_{\Phi_1+\Phi_2} \in A$. For $n > 3$, the theorem is obvious by induction on n : just write $\chi = (\Phi_1 + \Phi_2 - \Phi_1 \Phi_2 - 1) + (\Phi_1 \Phi_2 - 1) - \sum_{i=3}^{n} (\Phi_i - 1)$, and remark that χ is congruent mod A to $(\Phi_1 \Phi_2 - 1) + (\Phi_3 - 1) - \sum_{i=4}^{n} (\Phi_i - 1)$.

§4. Some arithmetic properties of orthogonal characters

We first prove a theorem of Serre on conductors of real representations.

Theorem 4.1. Let K be a number field or a finite extension of a p-adic field. Let E be a finite normal extension of K with Galois group G, and let χ be a real-valued character of G. Assume that one of the following conditions holds:

(i) E/K is tamely ramified

(ii) χ is an orthogonal character

Then, $\mathfrak{f}(\chi)/\mathfrak{f}(\det_\chi)$ is the square of an ideal.

Corollary 4.2. Under the assumptions of the theorem, the class of the ideal $\mathfrak{f}(\chi)$ is a square.

Proof. There is nothing to prove if $\det_\chi$ is trivial. If $\det_\chi$ is not trivial, then it is the character of a quadratic extension F/K, and $\mathfrak{f}(\det_\chi)$ is the discriminant of the extension F/K. Hence, its class is a square.

Corollary 4.3. Let K be a finite extension of a p-adic field. Assume that χ has trivial determinant. Then, under the assumption of the theorem, the local root number $W(\chi)$ depends only on the conjugacy class of χ (i.e., : $W(\chi^\omega) = W(\chi)$ for any $\omega \in \Omega_{\mathbb{Q}}$).

Proof. This is an obvious consequence of chap. II, prop. 6.1.

Proof of theorem 4.1. We first remark that $\mathfrak{f}(\chi)/\mathfrak{f}(\det_\chi) = \mathfrak{f}(\chi - \det_\chi)$. We may therefore assume that χ is a character with trivial determinant; we must then prove that $\mathfrak{f}(\chi)$ is a square, or, with the notation of chap. II, §1, that $n(\chi,\mathfrak{p})$ is an even integer for every finite prime $\mathfrak{p}$ of K.

Since $n(\chi,p) = n(\chi_p)$, it is enough to prove the theorem when K is a finite extension of a p-adic field.

There is a field E', $K \subset E' \subset E$, such that E'/K is unramified and E/E' is totally ramified. If H is the subgroup of G corresponding to E', then the conductors of χ and $\chi|H$ have the same valuation. Hence, we may assume that E/K is totally ramified.

Now, the case of a tame extension has already been dealt with (chap. II. §6). We therefore assume that χ is an orthogonal character. Since $\mathfrak{f}(\chi) = \mathfrak{f}(\chi - \chi(1).1)$, we may assume that χ is a character of degree 0. By theorem 3.3., we are reduced to the case when $\chi = \Phi + \bar{\Phi}$ or $\chi = r_\Phi$. Since $\mathfrak{f}(\chi + \bar{\chi}) = \mathfrak{f}(\chi)^2$, we need only consider the case when E/K is a totally ramified dihedral extension and χ is a character of the form r_Φ.

The character r_Φ is induced by a character of the form $(\Phi - 1)$ of a cyclic subgroup H of G of index 2, where Φ is irreducible of degree 1. Denote by F the fixed field of H. Using the Artin map, we can view Φ as a character on F^*. We know that the conductor of Φ is the least integer t such that Φ is trivial on U_F^t, and we must prove that this integer is even. The following proof has been given to me by Serre. (cf. Exercise 7).

Any easy calculation shows that the transfer from G^{ab} to H is trivial. Hence, Φ has a trivial restriction to K^*. On the other hand, since F/K is totally ramified, the inclusion $i : K^* \to F^*$ induces for every n an isomorphism $i_n : U_K^n/U_K^{n+1} \to U_F^{2n}/U_F^{2n+1}$. Therefore, if Φ is trivial on U_F^{2n+1}, then Φ is trivial on U_F^{2n}. Hence, the least integer t such that Φ is trivial on U_F^t is even, Q.E.D.

<u>Remark</u> 4.1. The conclusion of theorem 4.1. need not hold if the real valued character χ is not orthogonal; for example, see [13], or [7a] (Theorem 6).

<u>Remark</u> 4.2. Serre actually proved a more general theorem, namely : let A be a Dedekind domain with quotient field K; let E be finite normal extension of K with Galois group G, and let χ be a character of G. Assume that all the residue extensions of E/K are separable. Then, under the assumptions of theorem 4.1., $\mathfrak{d}(\chi)/\mathfrak{d}(\det_\chi)$ is a square. The proof is also by reduction to the dihedral case. (cf. Exercise 8).

Remark 4.3. The corresponding global statement to corollary 4.3. is true. By a theorem of Fröhlich and Queyrut (see Tate (Durham)), $W(\chi) = +1$. The equality $W(\chi^{\omega}) = W(\chi)$ for every $\omega \in \Omega_{\mathbb{Q}}$ is therefore trivial. Note that the original proof of the theorem of Fröhlich and Queyrut used a reduction to the case of a dihedral extension; the equality $W(\chi) = +1$ was then proved by direct calculation.

§5. Induction theorems for symplectic characters.

Definition. The quaternion group H_{4n} or order $4n$ is the group on 2 generators σ and τ with relations : $\sigma^n = \tau^2$, $\tau^4 = 1$, $\tau\sigma\tau^{-1} = \sigma^{-1}$; it contains a unique element of order 2, namely τ^2; H_4 is cyclic; for $n > 1$, $\{1,\tau^2\}$ is the centre of H_{4n}, and $H_{4n}/\{1,\tau^2\}$ is the dihedral group D_{2n} of order $2n$. Note that H_{4n} is the non-trivial extension of the group C_2 of order 2 by the cyclic subgroup generated by σ, the action of the generator of C_2 being given by $\sigma \longmapsto \sigma^{-1}$.

The group H_{4n} has 4 characters of degree 1. The other irreducible characters are real-valued characters of degree 2. Those which factor through a dihedral quotient are orthogonal, and those which do not are symplectic.

Definition Let G be a finite group. A quaternion character of G is an absolutely irreducible character of degree 2 of G which is lifted from a symplectic character of a quaternion quotient of G.

Theorem 5.1. Let G be a finite group and let χ be a symplectic character of G. Then, χ is a $\mathbb{Z}$-linear combination of characters of the form $\mathrm{Ind}_H^G(\Phi)$ for some subgroup H of G, where:

(i) either $\Phi = \psi + \bar{\psi}$, where ψ is an irreducible character of degree 1 of H,

(ii) or Φ is a quaternion character of H.

Proof. Write for the unit character of G a decomposition $1 = \sum_H n_H \mathrm{Ind}_G^G (\chi_H)$ where H ranges over the $\Gamma_{\mathbb{R}}$-elementary subgroups of G, $n_H \in \mathbb{Z}$ and χ_H is an orthogonal character. Then,

$$\chi = \chi.1 = \sum_H n_H \mathrm{Ind}_H^G (\mathrm{Res}_G^H(\chi).\chi_H).$$

Since R_G^s is a module over R_G^o, $\mathrm{Res}_G^H(\chi).\chi_H$ is a symplectic character. Since a $\Gamma_{\mathbb{R}}$-elementary group is supersolvable, theorem 5.1. is a consequence of the following more precise result for supersolvable groups :

<u>Theorem</u> 5.2. Let G be a finite supersolvable group, and let χ be an irreducible symplectic character of G.

Then one of the following conditions holds :

(i) $\chi = \Phi + \bar{\Phi}$, where Φ is induced by an irreducible character of degree one of some subgroup of G;

(ii) χ is induced by a quaternion character of some subgroup of G.

<u>Proof</u>. Let $\rho_{\mathbb{C}}$ be a complex representation with character χ. If χ is absolutely irreducible, we know from §1 that $\rho_{\mathbb{C}}$ comes from a quaternion representation $\rho : G \to V$ where V is a (say, left) vector space over the field $\mathbb{H}$ of Hamilton quaternions. The same is true if χ not absolutely irreducible. In both cases, the representation ρ is irreducible as a quaternion representation.

Let B be a quaternion-hermitian form on V invariant under G, and let L be the group of automorphisms of V which preserve B. Then, L is a compact Lie group, and $\rho(G)$ is contained in the normalizer of a maximal torus T of L.

Now, consider in $GL_n(\mathbb{H})$ the diagonal matrices

$$\begin{pmatrix} q_1 & & 0 \\ & \ddots & \\ 0 & & q_n \end{pmatrix}$$

with $|q_i| = 1$, where $|q|$ is the norm of the quaternion q. These matrices form a compact subgroup. Take for each index i a subgroup S_i of $\mathbb{H}^*$ isomorphic to the circle. Then, it can be proved that the subgroup

$$\begin{pmatrix} S_1 & & 0 \\ & \ddots & \\ 0 & & S_n \end{pmatrix}$$

of $Gl_n(\mathbb{H})$ is a maximal torus, and every maximal torus of Gl(V) is obtained by this construction after having choosen a suitable basis $e_1, \ldots, e_n$ of V, since two maximal tori are conjugate.

Going back to the proof of theorem 5.2, we can choose a basis $e_1, \ldots, e_n$ of V and subgroups $S_1, \ldots, S_n$ of $\mathbb{H}^*$ such that

$$T = \begin{pmatrix} S_1 & & 0 \\ & \ddots & \\ 0 & & S_n \end{pmatrix} .$$

Let V_i $(1 \leqslant i \leqslant n)$ be the quaternion line $\mathbb{H} e_i$, and let H be the group of those $s \in G$ such that $\rho_s(V_1) \subset V_1$. Since $\rho(G)$ is contained in the normalizer of T, $\rho(G)$ permutes the V_i's. Since ρ is irreducible, the permutation is transitive. Hence ρ is induced by ρ_1, the representation of H in $Gl(V_1)$ obtained by restriction of ρ to H. Now, $\rho_1(H)$ is a finite subgroup of $\mathbb{H}^*$, and the complete list of the finite subgroups of $\mathbb{H}^*$ is known : if K is a non cyclic subgroup of $\mathbb{H}^*$, K contains the elements $\{-1, +1\}$ of $\mathbb{H}^*$, and $K/\{-1, +1\}$ is isomorphic to a finite subgroup of $SO_3(\mathbb{R})$, hence is cyclic, dihedral or isomorphic to one of the three groups A_4, D_4, A_5. Therefore, K itself is cyclic, quaternion or isomorphic to one of the three "binary polyhedral groups" $\tilde{A}_4$, $\tilde{S}_4$, $\tilde{A}_5$. But the last three groups are not supersolvable, since A_4, S_4, A_5 are not. Hence, $\rho_1(H)$ is cyclic or quaternion, and ρ is of type (i) if $\rho_1(H)$ is cyclic, of type (ii) otherwise. (Here is alternative proof : $\rho_1(H)$ is contained in the normalizer N_1 of S_1, and it is easy to find the structure of N_1 : $N_1 = \langle S_1, n \rangle$, with $nsn^{-1} = s^{-1}$ for every $s \in S_1$ and $n^2 = -1$. Hence, either $\rho_1(H)$ is contained in S_1 and $\rho_1(H)$ is cyclic, or $\rho_1(H)$ is not contained in S_1 and $\rho_1(H)$

is quaternion.)

Remark. The conclusion of theorem 2.2 holds without the assumption that L should be compact. Hence, one can apply this theorem to the "usual" symplectic group $Sp_{2n}(\mathbb{C})$ to obtain a proof of theorem 5.2. Nevertheless, quaternions are more suitable to study symplectic representations. Note that the unitary group associated to a quaternion-hermitian form is often called "the symplectic group" in the theory of Lie groups.

REFERENCES (II and III)

1. E. Artin and J. Tate, Class Field Theory, Princeton (1952).

2. A. Borel et J.-P. Serre. Sur certains sous-groupes des groupes de Lie compacts. Comm. Math. Helv., 27 (1953), 128-139.

3. J.W.S. Cassels and A. Fröhlich. Algebraic Number Theory. London and New York, Academic Press, 1967.

4. P. Deligne. Les constantes locales de l'équation fonctionnelle de la fonctions L d'Artin d'une représentation orthogonale (à paraître).

5. A. Fröhlich. Artin Root Numbers and Normal Integral Bases for Quaternion Fields., Invent. Math., 17, 2 (1972), 143-166.

6. A. Fröhlich. Resolvent and Trace Form. Math. Proc. Camb. Phil. Soc., 78 (1975), 185-210.

7. A. Fröhlich. Arithmetic and Galois Module Structure. To appear in Crelle.

7a. A. Fröhlich, Artin Root Numbers, Conductors and Representations for generalized Quaternion groups. Proc. London Math. Soc., 28 (1974) 402-438.

7b. A. Fröhlich, Galois module structure, Durham Symposium.

8. H. Hasse. Artinsche Führer, Artinsche L-Funktionen und Gaussssche Summen über endlich-algebraischen Zahlkörper., Universidad Salamanca (1954).

9. J. Martinet. Modules sur l'algèbre du groupe quaternionien., Ann. Sci. E.N.S., 4 (1971), 399-408.

10. D. Quillen. The Adams conjecture, Topology, 10 (1971), 67-80.

11. J.-P. Serre. Corps Locaux (deuxième édition) Paris, Hermann, 1968.

12. J.-P. Serre. Représentations linéaires des groupes finis, (deuxième édition). Paris, Hermann, 1971.

13. J.-P. Serre. Conducteurs d'Artin des caractères réels, Invent. Math. 14, 3 (1971), 173-183.

14. J. Tate, Local Constants, Durham Symposium.

IV. EXERCISES (Prepared jointly with J.-P. Serre)

Exercise 1 (Dedekind) : Non abelian cubic fields.

Express the zeta function of a "pure" cubic field $K = \mathbb{Q}(\sqrt[3]{\alpha})$ in terms of abelian L-functions of $\mathbb{Q}(\sqrt[3]{1})$. Generalize to any non abelian cubic field of discriminant D replacing $\mathbb{Q}(\sqrt[3]{1})$ by $\mathbb{Q}(\sqrt{D})$.

Exercise 2 : Artin conductors.

In this exercise, A is a Dedekind domain with quotient field K, and E is a finite normal extension of K with separable residue extensions. We consider representations ρ, ρ_1, ρ_2 of $G = \mathrm{Gal}(E/K)$ into the linear groups of complex vector spaces V, V_1, V_2 of respective dimensions n, n_1, n_2. Let $N = [E : K]$. Discriminants and conductors are relative to A (cf. II. §1).

a) Prove that $\mathfrak{f}(\det_\rho)$ divides $\mathfrak{f}(\rho)$. (Hint: view $\det_\rho$ as a representation of G into $\mathrm{Gl}(\overset{n}{\wedge} V)$).

b) Prove that if ρ is faithful, then the primes of K which divide $\mathfrak{f}(\rho)$ are exactly those which divide the discriminant D(E/K). More precisely:

b_1) If ρ is irreducible, then $\mathfrak{f}(\rho)^n$ divides D(E/K).

b_2) D(E/K) divides $\mathfrak{f}(\rho)^{N-1}$.

b_3) If $\det_\rho$ is trivial, then $D(E/K)^2$ divides $\mathfrak{f}(\rho)^{N-1}$

(Hint : D(E/K) is the conductor of the regular representation; observe for b_3) that if $\det_\rho$ is trivial, then, for any subgroup H of G, $V^H = V$ or codim $V^H \geq 2$).

c) Prove that $\mathfrak{f}(\rho_1 \otimes \rho_2)$ divides $\mathfrak{f}(\rho_1)^{n_2}\, \mathfrak{f}(\rho_2)^{n_1}$, and that these 2 ideals are equal if $\mathfrak{f}(\rho_1)$ and $\mathfrak{f}(\rho_2)$ are coprime. (Hint: use the inclusion $V_1^G \otimes V_2^G \subset V_1 \otimes V_2)^G$, and the equality $V_1^G \otimes V_2 = (V_1 \otimes V_2)^G$ if G acts trivially on V_2).

d) Let $\bar{\rho}$ be the contragredient representation of ρ. Prove that $\mathfrak{f}(\rho \otimes \bar{\rho})$ divides $\mathfrak{f}(\rho)^{2(n-1)}$.

<u>Exercise</u> 3 : <u>Artin root numbers of tensor products</u>.

a) Let K be a finite extension of a p-adic field, and let χ_1, χ_2 be two characters on $G_K = \mathrm{Gal}(\bar{\mathbb{Q}}_p/K)$. Assume that χ_1 is unramified (i.e. χ_1 factors through an unramified extension). Prove the following two formulae:

a_1) $W(\chi_1\ \chi_2) = W(\chi_1)^{\chi_2(1)}\ W(\chi_2)^{\chi_1(1)}\ \det_{\chi_1}(\mathfrak{f}(\chi_2))$

a_2) $\tau(\chi_1\ \chi_2) = \tau(\chi_1)^{\chi_2(1)}\ \tau(\chi_2)^{\chi_1(1)}\ \det_{\bar{\chi}_1}(\mathfrak{f}(\chi_2))$

b) Let K be a number field, and let ρ_1 and ρ_2 be two representations of $\Omega_K = \mathrm{Gal}(\bar{Q}/K)$ with coprime conductors. Prove the following equality relating Galois Gauss sums and conductors:

$$\tau(\rho_1 \otimes \rho_2) = \tau(\rho_1)^{\rho_2(1)}\ \tau(\rho_2)^{\rho_1(1)}\ \det_{\bar{\rho}_1}(\mathfrak{f}(\rho_2))\ \det_{\bar{\rho}_2}(\mathfrak{f}(\rho_1)),$$

where $\bar{\rho}_i$ is the contragredient representation of ρ_i.

c) Under the assumptions of b), let E be a finite normal extension of K with Galois group G such that ρ_1 and ρ_2 factor through G. For every real place v of K, let $\sigma_v \in G$ be a real Frobenius substitution and let $n_i(v)$ be the number of eigenvalues of $\rho_i(\sigma_v)$ equal to -1. Prove the formula (cf. Weil, Lecture Notes 189 (1971) p. 152, lemma B):

$$W(\rho_1 \otimes \rho_2) =$$

$$W(\rho_1)^{\rho_2(1)}\ W(\rho_2)^{\rho_1(1)}\ \det_{\rho_1}(\mathfrak{f}(\rho_2)) \det_{\rho_2}(\mathfrak{f}(\rho_1)(-1)^{\sum_{v \text{ real}} n_1(v)n_2(v)}$$

Hint. To prove a), one may assume that χ_1 is irreducible of degree 1. Consider for any finite extension F of K the functions $\chi_2 \to W(\chi_{1,F}\chi_2)$ and $\chi_2 \to W(\chi_2)^{\chi_1(1)} \det_{\chi_1}(N_{F/K}(\mathfrak{f}(\chi_2)))$, where χ_1 is a fixed unramified character of Ω_K and $\chi_{1,F}$ is the restriction of $\det_{\chi_1}$ to Ω_F. Show that both functions are invariant under induction from Ω_F to $\Omega_{F'}$, for any field

F' with $K \subset F' \subset F$ when $\chi_2(1) = 0$, and prove that they are equal when χ_2 is irreducible of degree 1.

<u>Exercise</u> 4 : <u>Zeta functions with a zero at</u> $s = \frac{1}{2}$. (cf. J.V. Armitage, Invent. Math., 15 (1972), 199-205).

Let K be a number field. Denote by H_K its ideal class group. For a character $\psi : H_K \to \mathbb{C}^*$, let $\psi' : \Omega_K \to \mathbb{C}^*$ be the character which corresponds to ψ via the Artin map.

a) Let χ be a character of Ω_K. Prove the formula

$$W(\chi\ \psi') = W(\chi)\ W(\psi')^{\chi(1)}\ \psi(\mathfrak{f}(\chi))$$

(Use exercise 3).

b) Let E be a finite normal extension of K with Galois group G and let χ be a real valued character of G such that $W(\chi) = -1$. Prove that the function $s \mapsto L(s,\chi)$ has a zero or a pole of odd order at $s = \frac{1}{2}$.

c) Under the assumption of b), prove that the zeta function of E has a zero at $s = \frac{1}{2}$.

d) Let χ be a real valued character. Assume that the class in H_K of $\mathfrak{f}(\chi)$ is not a square. Prove that the zeta function of E or of some quadratic extension of E has a zero at $s = \frac{1}{2}$.

e) Use a) together with the theorem of Fröhlich and Queyrut to prove that the class in H_K of the conductor of an orthogonal representation is a square (cf. III, cor. 4.2).

Note. The proof of c) runs as follows : by Artin's induction theorem, there exist a positive integer N, cyclic subgroups H_i $(1 \leq i \leq r)$, integers n_i $(1 \leq i \leq r)$ and irreducible characters of degree one Φ_i of H_i for some integer r such that $N\chi = \sum_{i=1}^{r} n_i \operatorname{Ind}_{H_i}^{G} (\Phi_i)$.

We thus have the equality $L(s,\chi)^N = \prod_{i=1}^{r} L(s,\Phi_i)^{n_i}$. Since the L functions $s \to L(s,\Phi_i)$ are holomorphic at $s = \frac{1}{2}$, one of them has a zero at $s = \frac{1}{2}$. We have thus proved the existence of a cyclic subgroup H of G and of an irreducible degree 1 character Φ of H such that $L(\frac{1}{2}, \Phi) = 0$. Write now the zeta function of E as a product $\zeta_E(s) = L(s,\Phi) \prod_{\psi \neq \Phi} L(s,\psi)$ where ψ runs through the irreducible degree 1 characters of H. Then, $L(s,\psi)$ is holomorphic at $s = \frac{1}{2}$ for every ψ. Since $L(\frac{1}{2}, \Phi) = 0$, $\zeta_E(\frac{1}{2}) = 0$, Q.E.D.

Exercise 5 : Simple zeros of zeta functions (cf. Stark, Invent. Math., 23 (1974), §3, p.144).

Let K be a number field and let E be a finite normal extension of K with Galois group G. Let $s \in \mathbb{C}$. For any virtual character χ of G, let $v_s(\chi)$ be the order at $z = s$ of the L-function $z \to L(z,\chi)$. Since the function $\chi \to v_s(\chi)$ is additive and takes integral values, there exists a virtual character $\psi_s^G \in R_G$ such that

$$v_s(\chi) = \langle \chi, \psi_s^G \rangle \quad \text{for every } \chi \in R_G.$$

a) Prove that for any subgroup H of G, ψ_s^H is the restriction of ψ_s^G to H.

Assume now that s is a simple zero of the zeta function of E.

b) Prove that ψ_s^G is an irreducible character of degree 1 of G; hence, for any representation of G, the corresponding L-function is holomorphic at s.

(Hint : prove first the result for ψ_s^H where H is a cyclic subgroup of G. Then, show that it implies the equality $\langle \psi_s^G, \psi_s^G \rangle_G = 1$. Therefore, ψ_s^G is irreducible, and the result follows from the equality $\psi_s^G(1) = 1$.)

c) Let K_s be the cyclic extension of K corresponding to Ker ψ_s. Show that the zeta function of a field F between K and E has a zero at s if and only if $F \supset K_s$.

d) Assume that s is real. Show that ψ_s^G takes its values in $\{\pm 1\}$; thus, $K_s = K$ or $[K_s : K] = 2$.

Exercise 6 : Normal extensions with Galois group A_5 (cf. E. Artin, Collected papers n° 2 and 3).

a) Prove that the alternating group on 5 letters of order 60 has 5 irreducible characters χ_1, χ_3, χ'_3, χ_4, χ_5 of respective degrees 1, 3, 3, 4, 5.

(Remark : χ_3 and χ'_3, are conjugate and take their values in $\mathbb{Q}(\sqrt{5})$; they come from icosahedral representations $A_5 \to SO_3(\mathbb{R})$. The character χ_4 comes from the simplex representation $A_5 \to SO_4(\mathbb{R})$.)

b) Prove that $\chi_3 + \chi'_3$, $1 + \chi_4$ and χ_5 are monomial. Hence, the L-functions $L(s, \chi_3 + \chi'_3)$, $L(s, \chi_5)$ and $\zeta_{\mathbb{Q}}(s)\, L(s,\chi_4)$ are holomorphic (the last one for $s \neq 1$ only). It is not known whether $L(s,\chi_3)$, $L(s,\chi'_3)$ and $L(s,\chi_4)$ are holomorphic.

Exercise 7 : Dihedral and quaternion extensions (cf. Fröhlich, Proc. London Math. Soc. 28 (1974), 402-438).

Let K be a local field, and let E be a quadratic extension of K corresponding to a character $\varepsilon: K^* \to \{\pm 1\}$. Let F be a cyclic extension of degree N of E, corresponding to a character $\Phi : E^* \to \mathbb{C}^*$.

a) Prove that F/K is normal if and only if Ker Φ is invariant under the action of $g = \mathrm{Gal}(E/K)$.

Assume now that F/K is normal with Galois group G. Let H = Gal(F/E).

b) Prove that the non trivial element of g = G/H acts on H by $s \mapsto s^{-1}$ if and only if $\Phi(N_{E/K}(E^*)) = \{1\}$, i.e. $\Phi(\mathrm{Ker}\ \varepsilon) = \{1\}$.

c) Assume that $\Phi(\mathrm{Ker}\ \varepsilon) = \{1\}$. Prove that

(i) either Φ has a trivial restriction to K^*, and then G is dihedral

(ii) or the restriction of Φ to K^* is equal to ε, and G is quaternion.

d) State and prove the corresponding results in the global case.

(Hint : for c), consider the transfer from G^{ab} to H).

<u>Exercise</u> 8 : <u>Quasi-finite residue fields</u>.

a) Let k be a field. Show that there exists an extension k_1 of k which is a quasi-finite field. (Hint : let $\bar{k}$ be an algebraic closure of k; show the existence of a normal extension k' of $\bar{k}(t)$ with Galois group isomorphic to $\hat{\mathbb{Z}}$, and use the method of Corps Locaux, ch. XIII. §2, Exer. 3a); hence, one can take for k_1 a field of transcendence degree at most 1 over k.)

b) Let K be a local field with residue field k, and let L be a totally ramified extension of K. Let k_1 be an extension of k. Show the existence of local field K_1 with residue field k_1 which is an extension of K and is linearly disjoint over K with L, i.e. : $L_1 = L \otimes_K K_1$ is a field. (Hint : reduce to the case when k_1 is generated over k by a single element).

c) Combine a) and b) to prove the following "meta-theorem" : every statement about the ramification groups of a normal totally ramified extension of a local field which is true in the case when the residue fields are quasi-finite is true in general.

d) Application : prove Serre's theorem on conductors in full generality (cf. III, theorem 4.1 and Remark 4.2).