THE METHOD OF HADAMARD AND DE LA VALLÉE-POUSSIN (ACCORDING TO PIERRE DELIGNE)

Autor(en): **Moreno, Carlos J.**

Objekttyp: **Article**

Zeitschrift: **L'Enseignement Mathématique**

Band (Jahr): **29 (1983)**

Heft 1-2: **L'ENSEIGNEMENT MATHÉMATIQUE**

PDF erstellt am: **21.07.2024**

Persistenter Link: https://doi.org/10.5169/seals-52974

L'Enseignement Mathématique, t. 29 (1983), p. 89-128

THE METHOD OF HADAMARD AND DE LA VALLÉE-POUSSIN

(According to Pierre Deligne)

by Carlos J. Moreno

Contents

INTRODUCTION

The method of Hadamard and de la Vallée-Poussin arises in the proof that certain classical series, like Riemann's zeta function and Dirichlet's L-functions, do not vanish on the line of absolute convergence. Many interesting equidistribution Theorems are consequences of this result, e.g. the prime number theorem and Dirichlet's Theorem on the infinitude of primes in arithmetic progressions.

Motivated by results of Yoshida [12], Deligne has obtained in his paper *The Weil Conjecture II* ([3], §2) a generalization of the method of Hadamard and de la Vallée-Poussin and has applied it to some very non-classical situations which deal with zeta and L-functions of algebraic varieties over finite fields. Deligne's main result, which is given in Part II and proved in Part III, establishes the non-vanishing on the line of absolute convergence of most of the L-functions which appear naturally in number theory and algebraic geometry; its main merit is its application to L-functions which are not expressible as finite products of Artin L-functions where Brauer induction ordinarily would not suffice.

The present notes, which are an expanded version of the rather concise §2 of [3], have as a purpose to make Deligne's results more accessible to number theorists. We believe that because of its importance the subject deserves a fuller treatment.

In order to reduce the degree of generality in the statement of Deligne's theorem and in his argument, and to give some content to the main result which would be easily understood by number theorists, we start Part I with a series of relatively simple examples taken from elementary algebraic geometry; these are close to the spirit of Artin's thesis [1] as well as that of the beautiful paper of Davenport and Hasse [4]. We hope that the reader will find in Part I some familiar things.

The reader who is only interested in Deligne's Theorem and its proof can consult the last section of Part II and the proof of the main lemma in Part III. In this way he will avoid several excursions that we have taken through the countryside of representation theory. A short sketch of Deligne's application of his result to the proof of the Hard Lefschetz Theorem is given in [6].

We acknowledge several conversations we had with Pierre Deligne about his methods. We also wish to express our deep gratitude to Nick Katz for explaining to us his own ideas on Deligne's results. Without his help and Lecture Notes [5] it would have been almost impossible to write this article. The reader familiar with Katz's Notes (pp. 94-134) will recognize that at times we have followed his

presentation rather closely especially in the proof we give of The Main Lemma in Part III. Most of this article was prepared while the author visited the IHES (1979-80). The present version was presented in three seminars at the University of Illinois in the Spring of 1981.

PART I: EXAMPLES

§1. THE ZETA FUNCTION OF THE PROJECTIVE LINE. Let $\mathbf{F}_q$ be the finite field of q elements and let $A = \mathbf{F}_q[x]$ be the ring of polynomials with coefficients in $\mathbf{F}_q$. The set of closed points on the projective line $\mathbf{P}^1$ can be identified with the set of monic irreducible polynomials in A plus the rational function $\frac{1}{x}$ which corresponds to the point at infinity on $\mathbf{P}^1$. If P is a polynomial in A of degree d, we put

$$NP = q^d .$$

The zeta function of the affine line $\mathbf{A}^1 = \mathbf{P}^1 - \{\infty\}$ is defined, for s a complex number, by

$$Z(s, \mathbf{A}^1) = \sum_a Na^{-s},$$

where a runs over all monic polynomials in A including $a = 1$. Since

$$\# \{a \in A \mid a \text{ monic, } \deg(a) = n\} = q^n ,$$

it follows that

$$Z(s, \mathbf{A}^1) = \sum_{n=0}^{\infty} q^{n-ns} = \frac{1}{1 - q^{1-s}};$$

hence $Z(s, \mathbf{A}^1)$ is an absolutely convergent series for $R(s) > 1$. Furthermore, since A is a unique factorization domain, we have an Euler product expansion

$$Z(s, \mathbf{A}^1) = \prod_P \frac{1}{1 - NP^{-s}},$$

where P runs over all monic irreducible polynomials in A of degree $\geqslant 1$. If we include in this Euler product the factor $(1-q^{-s})^{-1}$, which corresponds to the rational function $P_\infty = \frac{1}{x}$, we obtain the zeta function of the projective line

$$\begin{aligned} Z(s, \mathbf{P}^1) &= \prod_P \frac{1}{1 - NP^{-s}} \\ &= \frac{1}{1 - q^{-s}} \cdot \frac{1}{1 - q^{1-s}} . \end{aligned}$$

To study $Z(s, \mathbf{A}^1)$ we can also proceed in a slightly different way. First we recall that a fundamental lemma in the arithmetic of the ring A is Gauss' result that for any positive integer $n \geqslant 1$

$$x^{q^n} - x = \prod_{d|n} F_d(x) ,$$

where $F_d(x)$ is the product of all monic irreducible polynomials in A of degree d. By comparing the degrees on both sides of this identity we obtain

$$q^n = \sum_{d|n} dN_d ,$$

where N_d is the number of monic irreducible polynomials in A of degree d. In the Euler product for $Z(s, \mathbf{A}^1)$ we collect those polynomials P of degree d and use the last equality to obtain

$$Z(s, \mathbf{A}^1) = \prod_{d=1}^{\infty} \left(\frac{1}{1 - q^{-ds}} \right)^{Nd} .$$

By taking the logarithm of both sides we get

$$\begin{aligned} \log Z(s, \mathbf{A}^1) &= \sum_{d=1}^{\infty} N_d \sum_{k=1}^{\infty} q^{-sdk}/k \\ &= \sum_{m=1}^{\infty} \frac{1}{m} q^{-sm} \sum_{d|m} dN_d \\ &= \sum_{m=1}^{\infty} \frac{1}{m} (q^{1-s})^m \\ &= \log \frac{1}{1 - q^{1-s}} ; \end{aligned}$$

this agrees with the expression obtained earlier for $Z(s, \mathbf{A}^1)$. Three observations are in order at this point:

(1.1) $Z(s, \mathbf{P}^1)$ is meromorphic in the region $R(s) \geqslant 1$ and has a simple pole at $s = 1$; this implies that

(1.2) The Euler product expansion of $Z(s, \mathbf{P}^1)$ has an infinite number of local factors (Euler's proof of the infinitude of primes!)

(1.3) $Z(1 + it, \mathbf{P}^1) \neq 0$ for all real values of t.

§2. Gauss sums. If $x \in \mathbf{C}$ and if m is an integer $\geqslant 1$, we put

$$e_m(x) = e^{2\pi i\, x/m}\,.$$

Let p denote a prime number. If $x \in \mathbf{Z}$, and μ_p denotes the group of p-th roots of unity, then the map $x \to e_p(x)$ defines by passage to the quotient an isomorphism

$$e_p : \mathbf{Z}/p\mathbf{Z} \to \mu_p\,.$$

Let $k = \mathbf{F}_q$ denote the finite field with $q = p^a$ elements. For $x \in \mathbf{F}_q$ we put

$$\mathrm{Tr}_k(x) = x + x^p + \ldots + x^{p^{a-1}}\,;$$

since $\mathrm{Tr}_k(x)$ belongs to $\mathbf{Z}/p\mathbf{Z}$, the map

$$\mathbf{F}_q \to \mu_p$$

given by $\psi_k(x) = e_p(\mathrm{Tr}_k(x))$ is a non-trivial additive character of $\mathbf{F}_q$. Any other additive character ψ' of $\mathbf{F}_q$ has the form $\psi'(x) = \psi_k(cx)$ for some $c \in \mathbf{F}_q$. Let $\mathbf{F}_q^* = \mathbf{F}_q - \{0\}$ be the multiplicative group of $\mathbf{F}_q$. With each of the $q - 1$ characters χ of $\mathbf{F}_q^*$ there is associated a Gauss sum

$$g(\chi, \psi) = \sum_{x \in \mathbf{F}_q} \chi(x)\psi(x)\,;$$

The one corresponding to the trivial character $\chi_0 \equiv 1$ has the value $g(\chi_0, \psi) = -1$. A well known property of $g(\chi, \psi)$ with χ a non-trival character is $|\, g(\chi, \psi)\,|^2 = q$.

For a monic polynomial in the ring $A = \mathbf{F}_q[x]$

$$a = x^n + a_1x^{n-1} + \ldots + a_n$$

we put

$$\Lambda(a) = \chi(a_n)\psi(a_1)\,;$$

if b is another monic polynomial

$$b = x^m + b_1x^{m-1} + \ldots + b_m\,,$$

Then

$$a \cdot b = x^{m+n} + (a_1+b_1)x^{m+n-1} + \ldots + a_nb_m\,;$$

from this it follows easily that

$$\Lambda(a{\cdot}b) = \Lambda(a)\Lambda(b)\,.$$

We can thus form the zeta function

$$Z(s, \mathscr{L}_\chi) = \sum_a \Lambda(a)Na^{-s}$$

$$= \prod_P \frac{1}{1 - \Lambda(P)NP^{-s}}\,,$$

where the product runs over all irreducible monic polynomials in A. From the properties of $Z(s, \mathbf{A}^1)$ it follows easily that $Z(s, \mathscr{L}_\chi)$ is absolutely convergent for $R(s) > 1$. The Dirichlet series $Z(s, \mathscr{L}_\chi)$ is also expressible in the form

$$Z(s, \mathscr{L}_\chi) = 1 + \sum_{d=1}^{\infty} q^{-ds} S_d ,$$

where

$$S_d = \sum_a \Lambda(a)$$

and the sum runs over all monic polynomials of degree d. As all monic polynomials of degree 1 in A are of the form $a = x + c$ with $c \in \mathbf{F}_q$, and since $\Lambda(x+c) = \chi(c)\psi(c)$, we obtain for $d = 1$ the Gauss sum $S_1 = g(\chi, \psi)$. Also all irreducible monic polynomials in A of degree 2 have the form $a = x^2 + bx + c$, $b, c \in \mathbf{F}_q$; for these we have

$$\begin{aligned} S_2 &= \sum_a \Lambda(x^2+bx+c) \\ &= \sum_b \sum_c \chi(c)\psi(b) \\ &= \sum_c \chi(c) \big(\sum_b \psi(b)\big) = 0 . \end{aligned}$$

A similar argument shows that for all $d \geqslant 3$ we have $S_d = 0$. Hence we obtain

$$Z(s, \mathscr{L}_\chi) = 1 + g(\chi, \psi)q^{-s} .$$

This representation proves that $Z(s, \mathscr{L}_\chi)$, defined for $R(s) > 1$ has a holomorphic continuation to all values of the complex variable s; from the fact $| g(\chi, \psi) | = q^{\frac{1}{2}}$ it also follows that the zeros of $Z(s, \mathscr{L}_\chi)$ are all located on the line $R(s) = \frac{1}{2}$. The trivial fact $| g(\chi, \psi) | < q$ would suffice to show that $Z(1+it, \mathscr{L}_\chi) \neq 0$ for all real values of t.

§3. KLOOSTERMAN SUMS. Let φ be an additive character of $\mathbf{F}_q$. For a monic polynomial in A of the form

$$a = x^n + a_1 x^{n-1} + \dots + a_n , \qquad a_n \neq 0 ,$$

we define a function

$$\Lambda(a) = \psi(a_1)\varphi(a_{n-1}\bar{a}_n) , \qquad a_n \bar{a}_n = 1 ,$$

with the proviso that

$$\Lambda(x+c) = \psi(c)\varphi(c^{-1}) .$$

If $b \in A$ is another polynomial of the form

$$b = x^m + b_1 x^{m-1} + \dots + b_m ,$$

we have

$$ab = x^{m+n} + (a_1+b_1)x^{m+n-1} + \dots + (a_nb_{m-1}+b_ma_{n-1})x + b_nb_m .$$

By noting that $(a_nb_{m-1}+b_ma_{n-1})\bar{a}_n\bar{b}_m = b_{m-1}\bar{b}_m + a_{n-1}\bar{a}_n$ we obtain

$$\Lambda(a\cdot b) = \Lambda(a)\Lambda(b) .$$

Thus we can define a new zeta function by putting

$$\begin{aligned} Z(s, Kl) &= \sum_a \Lambda(a)Na^{-s} \\ &= \prod_P \frac{1}{1 - \Lambda(P)NP^{-s}} , \end{aligned}$$

where the sum is taken over the set of monic polynomials a in A with non-zero constant term including the polynomial $a = 1$, and the product is taken only over the subset of those which are irreducible.

By grouping together terms in the Dirichlet series $Z(s, Kl)$ corresponding to polynomials of the same degree we obtain

$$Z(s, Kl) = 1 + \sum_{d=1}^{\infty} q^{-ds}S_d ,$$

where

$$S_d = \sum_a \Lambda(a) ,$$

and the sum runs over all monic polynomials a in A of degree d with non-zero constant term. Let us look more closely at the sums S_d for small d. For $d = 1$ all the monic polynomials in A are of the form $x + c$ with $c \in \mathbf{F}_q$, and

$$\begin{aligned} S_1 &= \sum_{c\in\mathbf{F}_q^*} \Lambda(x+c) \\ &= \sum_{c\in\mathbf{F}_q^*} \psi(c)\varphi(c^{-1}) ; \end{aligned}$$

since $\varphi(x) = \psi(bx)$ for some $b \in \mathbf{F}_q^*$, we obtain then that

$$S_1 = \sum_{c\in\mathbf{F}_q^*} \psi(c+bc^{-1}) .$$

If $\mathbf{F}_q = \mathbf{Z}/\mathbf{Z}_p$, then S_1 reduces to the well known Kloosterman sum

$$Kl(p) = \sum_{c\in\mathbf{F}_p^*} e^{\frac{2\pi i}{p}(ac+bc^{-1})} .$$

In the following we denote S_1 by $-K(\varphi)$. All monic polynomials of degree 2 with non-zero constant term are given by $a = x^2 + cx + b$, with $c \in \mathbf{F}_q$, $b \in \mathbf{F}_q^*$, and hence

$$\begin{aligned} S_2 &= \sum_a \Lambda(x^2+cx+b), \\ &= \sum_{c\in\mathbf{F}_q}\sum_{b\in\mathbf{F}_q^*} \psi(c)\varphi(cb^{-1}) \\ &= \sum_{b\in\mathbf{F}_q^*}\sum_{c\in\mathbf{F}_q} \psi_b(c), \end{aligned}$$

where $\psi_b(c) = \psi(c(1+\bar{b}a_0))$, and $\varphi(c) = \psi(a_0c)$. Now $\psi_b(c) \equiv 1$ if and only if $1 + \bar{b}a_0 = 0$ and this occurs only once when $b = -a_0$. For this particular value of b, the inner sum is equal to $\#\mathbf{F}_q = q$. If $b \neq -a_0$, then ψ_b is a non-trivial additive character and the inner sum has the value zero. Therefore we have $S_2 = q$. For $d = 3$ we have from the definition of Λ that

$$S_3 = \sum_b\sum_c\sum_d \Lambda(x^3+bx^2+cx+d),$$

with $b, c, d \in \mathbf{F}_q$ and $d \neq 0$, and hence

$$S_3 = \sum_c\sum_d \varphi(c\bar{d}) \sum_{b\in\mathbf{F}_q} \psi(b) = 0.$$

For similar reasons we also obtain $S_d = 0$ for $d \geqslant 3$. We can now write

$$\begin{aligned} Z(s, Kl) &= \prod_P \frac{1}{1 - \Lambda(P)NP^{-s}} \\ &= 1 - K(\varphi)q^{-s} + q^{1-2s}. \end{aligned}$$

This shows that the function $Z(s, Kl)$ is holomorphic for all complex values of s. It is clear that $Z(s, Kl) \neq 0$ for $R(s) > 1$; the simple observation $|\,K(\varphi)\,| < q$ would also give that

$$Z(1+it, Kl) \neq 0$$

for all real values of t. Let us pretend for a moment that we do not know this fact and show how it can be derived, in an unnecessarily complicated way, from the method of Hadamard and de la Vallée-Poussin. Suppose then that $1 + it_0$ is a zero of multiplicity m. For $\sigma > 1$ and $Z(s, Kl) = Z(s, \Lambda)$ we have

$$-\frac{Z'}{Z}(\sigma+it, \Lambda) = \sum_{\substack{P\\ n>0}} (\log NP)NP^{-n\sigma}(NP^{-it}\Lambda(P))^n.$$

If we put $\lambda_P = NP^{-it_0}\Lambda(P)$, then clearly $\lambda_P \cdot \bar{\lambda}_P = 1$ and

$$\begin{aligned} R\left\{-6\frac{Z'}{Z}(\sigma, 1) - 8\frac{Z'}{Z}(\sigma+it_0, \Lambda) - 2\frac{Z'}{Z}(\sigma+2it_0, \Lambda^2)\right\} \\ = \sum_{\substack{P\\ n>0}} (\log NP)NP^{-n\sigma}\{2 + \lambda_P^n + \bar{\lambda}_P^n\}^2 > 0. \end{aligned}$$

On the other hand for $\sigma > 1$ and close to 1 we have

$$-\frac{Z'}{Z}(\sigma, 1) = \frac{1}{\sigma - 1} + f_1(\sigma),$$

$$\frac{Z'}{Z}(\sigma+it_0, \Lambda) = \frac{m}{\sigma - 1} + f_2(\sigma),$$

where f_i remains finite as $\sigma \to 1$. We thus obtain

$$\frac{6}{\sigma - 1} - \frac{8m}{\sigma - 1} \gg 1 .$$

But this is false for σ sufficiently close to 1 unless $m = 0$ in which case $Z(s, Kl)$ does not vanish on the line of absolute convergence. It is a simple matter to obtain, say via a Tauberian argument, that

$$\sum_{NP \leqslant x} \Lambda(P) = \delta_\Lambda x + o(x),$$

where $\delta_\Lambda = 0$, unless $\Lambda \equiv 1$ in which case $\delta_\Lambda = \frac{1}{\log q}$. This circle of ideas has been introduced by Kornblum (*Math. Zeitschr.* Vol. 5 (1919), p. 100) in order to establish an analogue of Dirichlet's Theorem on arithmetic progressions for the ring $A = \mathbf{F}_q[x]$; they were later developed more fully and systematically by Artin in the second part of his thesis ([1], II). It is a consequence of Weil's proof of the Riemann Hypothesis for curves over finite fields that the zeros of $Z(s, \Lambda)$ are all located on the critical line $R(s) = \frac{1}{2}$. This gives the much sharper estimate $\delta_\Lambda x + O(x^{\frac{1}{2}})$ for the above sum. The equality $Z(s, Kl) = 1 - K(\varphi)q^{-s} + q^{1-2s}$ also implies $| K(\varphi) | \leqslant 2q^{\frac{1}{2}}$, an estimate which is best possible.

§4. Equidistribution of the arguments of Gauss sums. Let $\mathbf{F}_p$ be the finite field of p elements; let $\psi : \mathbf{F}_p \to \mathbf{C}^*$ be a fixed non-trivial additive character of $\mathbf{F}_p$ as in §2. With each of the $p - 1$ characters χ of the multiplicative group $\mathbf{F}_p^* = \mathbf{F}_p - \{0\}$ we define a Gauss sum

$$g(\chi, \psi) = \sum_{x \in \mathbf{F}_q^*} \chi(x)\psi(x) .$$

If χ is one of the $p - 2$ non-trivial multiplicative characters of $\mathbf{F}_p^*$, we have $| g(\chi, \psi) | = p^{\frac{1}{2}}$, and hence

$$g(\chi, \psi) = p^{\frac{1}{2}} e^{2\pi i \theta_p(\chi)},$$

with $\theta_p(\chi) \in [0, 1)$. For each prime p, and for a fixed choice of additive character ψ we consider the sequence of $p - 2$ angles

$$\Theta_p = \{\theta_p(\chi_j)\}_{1 \leqslant j \leqslant p-2},$$

which result from all the non-trivial characters of $\mathbf{F}_p^*$. As p ranges over the primes in increasing order we obtain a triangular array

$$\Theta = \{\Theta_p \mid p \quad \text{a prime}\}$$

of points in $[0, 1)$. For a prime p and a subinterval J in $[0, 1)$, we denote by $A(p, J)$ the number of angles $\theta_p(\chi_j)$, $1 \leqslant j \leqslant p - 2$ which belong to J, $\mid J \mid$ is the length of J. The sequence Θ is uniformly distributed in $[0, 1)$; in fact it can be shown that (Smith [10]),

$$\operatorname*{Sup}_J \mid (p-2)^{-1} A(p, J) - \mid J \mid \mid \ll p^{-\frac{1}{4}}.$$

In particular one obtains the estimate

$$A(p, J) = \mid J \mid p + O(p^{\frac{3}{4}}).$$

To establish these results we put, for h a non-zero integer,

$$S_p(h) = \frac{1}{p-2} \sum_{\chi}{}' e^{2\pi i h \theta_p(\chi)},$$

where the sum runs over the non-trivial characters of $\mathbf{F}_p^*$. The Erdös-Turan inequality [1]) gives, for any integer $m \geqslant 1$

$$\operatorname*{Sup}_J \mid (p-2)^{-1} A(p, J) - \mid J \mid \mid \leqslant \frac{4}{m+1} + \frac{4}{\pi} \sum_{h=1}^{m} \frac{1}{h} \mid S_p(h) \mid.$$

To get an estimate for $S_p(h)$, we observe that since $g(\chi, \psi) = p^{\frac{1}{2}} e^{2\pi i \theta_p(\chi)}$, we have

$$\begin{aligned}\sum_{\chi}{}' g(\chi, \psi)^h &= p^{h/2} \sum_{\chi}{}' e^{2\pi i h \theta_p(\chi)} \\ &= p^{h/2}(p-2) S_p(h).\end{aligned}$$

On the other hand we have the combinatorial identity

$$\sum_{\chi}{}' g(\chi, \psi)^h = (-1)^{h+1} + (p-1) \sum_{xi} \psi(x_1 + \ldots + x_h), \tag{4.1}$$

[1]) H. Montgomery has obtained a conceptually simple proof of this inequality along the lines of his article in *Bull. A.M.S.* vol. 84 (1978), 546-567.

where the sum on the right hand side is taken over all the h-tuples $(x_1, ..., x_h) \in (\mathbf{F}_p)^h$ which satisfy $x_1 \cdot x_2 \cdot ... \cdot x_h = 1$. The sum

$$Kl_h(p) = \sum_{x_i} \psi(x_1 + ... + x_h)$$

is usually called a hyper Kloosterman sum. As a generalization of the function $Z(s, Kl)$ considered in §3 it is natural to consider a function $Z(s, Kl_h)$ defined by the following Euler product

$$Z(s, Kl_h)^{(-1)^{h+1}} = \prod_{P\in|X_0|} \frac{1}{1 - \Lambda(P)NP^{-s}},$$

where X_0 is the affine variety defined over $\mathbf{F}_p$ by $x_1 ... x_h = 1$, $| X_0 |$ is the set of closed points on X_0 and $\Lambda : | X_0 | \to \mathbf{C}^*$ is a function which takes the value

$$\Lambda(P) = \psi(a_1 + ... + a_n),$$

when P is the closed point $(a_1, ..., a_n) \in X_0(\mathbf{F}_p)$ defined by the maximal ideal $(x_1 - a_1, ..., x_h - a_n)$ in $\mathbf{F}_p[x_1, ..., x_h]$. The function $Z(s, Kl_h)$ can be shown to be a polynomial of degree h in p^{-s}, where the coefficient of p^{-s} is the hyper Kloosterman sum $Kl_h(p)$. It is a consequence of Deligne's proof of the Weil conjecture that the zeros of $Z(s, Kl_h)$ are all located on the line $R(s) = \dfrac{h-1}{2}$. This implies in particular that

$$| Kl_h(p) | \leqslant hp^{(h-1)/2}. \tag{4.2}$$

The weaker result $| Kl_h(p) | \leqslant hp^{\frac{h}{2}-\delta}$, for some $\delta > 0$ would follow from the non-vanishing of $Z(s, Kl_h)$ on the line $R(s) = \dfrac{h}{2}$; this would be enough to establish the equidistribution of the angles of the Gauss sums.

From Deligne's estimate (4.2) and the combinatorial identity we obtain that

$$\begin{aligned} S_p(h) &= \frac{1}{p-2} \sum_{\chi}{}' e^{2\pi i h \theta_p(\chi)} \\ &= \frac{1}{p-2} \cdot p^{-\frac{h}{2}} \sum_{\chi}{}' g(\chi, \psi)^h \\ &= (p-2)^{-1} p^{-\frac{h}{2}} \{(-1)^{h+1} + (p-1)Kl_h(p)\}, \end{aligned}$$

and hence

$$| S_p(h) | < 2hp^{-\frac{1}{2}}.$$

When this estimate is substituted into the Erdös-Turan inequality with $m = [p^{\frac{1}{4}}]$, we get

$$\operatorname*{Sup}_{J} | (p-2)^{-1}A(p, J) - | J | | \leqslant \frac{1}{m+1} + \frac{8}{\pi} mp^{-\frac{1}{2}} \ll p^{-\frac{1}{4}}.$$

This establishes the result. A comparison of the estimate $A(p, J) = p | J | + O(p^{\frac{3}{4}})$ with some of the classical prime number theorems suggests that perhaps the stronger result

$$A(p, J) = p | J | + O(p^{\frac{1}{2}+\varepsilon})$$

should be true.

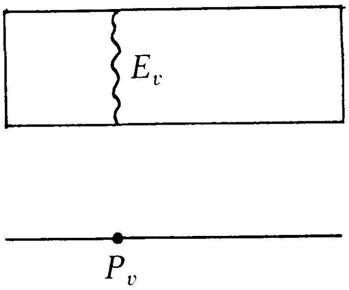
PART II: STATEMENT OF THE THEOREM

§1.1. INTRODUCTION. In the statement of Deligne's theorem there appear certain Euler products which are generalizations of the Artin-Grothendieck L-functions and which satisfy some rather natural growth conditions; these conditions are stated below in §2 as Axioms A and B. In order to elucidate the applicability of the theorem, to introduce some relevant concepts from representation theory, and to prepare the notation that goes into the statement of the theorem, we now give two examples one of a geometric nature, the other of an arithmetic nature. The expert will realize that both examples are intimately connected, say via the Selberg-trace Formula.

§1.2. GEOMETRIC EXAMPLE. As in Part I, let $\mathbf{F}_q$ be the finite field of q elements and let $A = \mathbf{F}_q[T]$ be the coordinate ring of the affine line $\mathbf{A}^1$. For technical reasons and to simplify our presentation, we assume the characteristic of $\mathbf{F}_q$ is not 2 or 3. The closed points on the affine line $\mathbf{A}^1$ are in one-to-one correspondence with the irreducible monic polynomials in A. Now if $P = P_v$ is such an irreducible polynomial in A, then the image of T under the reduction map

$$\begin{aligned} A &\to A/(P) = \mathbf{F}_{q_v} \\ T &\to t_v, \end{aligned}$$

gives an element t_v in the finite field $\mathbf{F}_{q_v}$ with $q_v = q^{\deg (P)}$ elements. We can now consider the elliptic family



$$\begin{tikzcd} E : y^2 = x(x-1)(x-T)\,, \arrow[d] \\ \mathbf{A}^1 \end{tikzcd}$$

where $E_v : y^2 = x(x-1)(x-t_v)$ is the fiber in E above the point P_v. If we exclude from $\mathbf{A}^1$ the points corresponding to the polynomials $P_r = T$, $P_v = T - 1$, then each fiber E_v is an elliptic curve defined over the finite field $\mathbf{F}_{q_v}$. A well known theorem of Hasse established in 1934 states that

$$\#\{(x, y) \in (\mathbf{F}_{q_v})^2 \mid y^2 = x(x-1)(x-t_v)\} = q_v - (\alpha_v + \beta_v) + 1\,,$$

where

$$\alpha_v = q_v^{\frac{1}{2}} e^{i\theta_v}\,, \qquad \beta_v = q_v^{\frac{1}{2}} e^{-i\theta_v}\,,$$

where $\theta_v \in [0, 2\pi)$.

Let $SU(2)$ be the group of special unitary matrices of size 2×2 and consider the trivial extension

$$0 \to SU(2) \to G \to \mathbf{Z} \to 0$$

given by the direct product $G = SU(2) \times \mathbf{Z}$. Let Σ be the set of all irreducible monic polynomials in $A = \mathbf{F}_q[T]$. For each $v \in \Sigma$ we have an element in G

$$\left\{\begin{pmatrix} e^{i\theta_v} & 0 \\ 0 & e^{-i\theta_v} \end{pmatrix}, -\deg v\right\};$$

denote by x_v the conjugacy class of this element in $G = SU(2) \times \mathbf{Z}$. Let ω_1 be the quasi-character

$$\omega_1 : \mathbf{Z} \to \mathbf{R}_+$$

which sends the integer n to $\omega_1(n) = q^n$, and for s a complex number put $\omega_s = \omega_1^s : \mathbf{Z} \to \mathbf{C}^*$; this gives by composition with the projection map $G \to \mathbf{Z}$ a representation

$$\omega_s : G \to \mathbf{C}^*\,.$$

The finite dimensional representations of $SU(2)$ are well known; they have the following structure: for each positive integer k, there is a representation

$$\mathrm{Sym}^k\, r : SU(2) \to GL(k+1, \mathbf{C})\,.$$

For $k = 0$, this is the trivial representation of $SU(2)$; for $k = 1$ $\mathrm{sym}^1\, r = r$ is just the standard representation which sends an element in $SU(2)$ into the same element in $GL(2, \mathbf{C})$. In general, if $g = \begin{pmatrix} \alpha & 0 \\ 0 & \beta \end{pmatrix} \in SU(2)$ then $\operatorname{sym}^k r(g)$ is the diagonal matrix in $GL(k+1, \mathbf{C})$ given by

$$\operatorname{Sym}^k r(g) = \operatorname{Diag}\,[\alpha^k, \alpha^{k-1}\beta, ..., \alpha\beta^{k-1}, \beta^k]\,.$$

It can easily be shown that the set of all finite dimensional representations of the locally compact group G are of the form

$$\tau = (\operatorname{Sym}^k r)\cdot\omega_s\,,$$

for some positive integer k and a complex number s; for such a representation, if $s = \sigma + it$, we call σ the real part of τ and write

$$R(\tau) = \sigma\,.$$

In particular if τ is an arbitrary representation then $R(\tau\cdot\omega_s) = R(\tau) + R(s)$. With the above notations we now associate to each representation τ of G the L-function

$$L(\tau) = \prod_{v\in\Sigma} \frac{1}{\det(I-\tau(x_v))}\,;$$

an easy comparison of $L(\tau)$ with the zeta function $Z(s, \mathbf{A}^1)$ of §1 of Part I shows that $L(\tau)$ converges absolutely if $R(\tau) > 1$. It is a consequence of Grothendieck's Trace formula that $L(\tau)$ has a holomorphic continuation to the region $R(\tau) \geqslant 1$ except for a simple pole at $\tau = \omega_1$. Deligne's generalization of the method of Hadamard and de la Vallée-Poussin will imply that

$$L(\tau) \neq 0 \quad \text{for all } \tau \text{ with} \quad R(\tau) = 1\,.$$

From here on one takes the familiar road of analytic number theory and applies criteria of the Weyl-type as well as Tauberian theorems to obtain equidistribution results. ([9], [12].)

§1.3. ARITHMETIC EXAMPLE. Let us consider our favorite arithmetic function: the Ramanujan function $\tau(n)$ which is defined by the formal expansion

$$x\prod_{n=1}^{\infty}(1-x^n)^{24} = \sum_{n=1}^{\infty}\tau(n)x^n\,.$$

Let Σ denote the set of rational primes. For each prime $p \in \Sigma$ it follows from Deligne's proof of the Ramanujan conjecture that

$$\tau(p) = (e^{i\theta_p} + e^{-i\theta_p})p^{11/2}\,,$$

with $\theta_p \in [0, 2\pi)$. In this arithmetic situation we consider the trivial group extension

$$0 \to SU(2) \to G \to \mathbf{R} \to 0$$

given by the direct product $G = SU(2) \times \mathbf{R}$. With each prime p we associate the element

$$\left\{\begin{pmatrix} e^{i\theta_p} & 0 \\ 0 & e^{-i\theta_p} \end{pmatrix}, -\log p\right\},$$

and denote by x_p the conjugacy class in G which contains it. Let ω_1 be the quasi-character

$$\omega_1 : \mathbf{R} \to \mathbf{R}_+^*$$
$$r \to \omega_1(r) = e^r ;$$

for each complex number s, let ω_s be the 1-dimensional complex representation

$$\omega_s : G \to \mathbf{C}^*$$

obtained by composing ω_1^s with the projection map $G \to \mathbf{R}$. Again it is not very difficult to show that all the finite dimensional representations of G are of the form

$$\tau = (\text{sym}^k r) \cdot \omega_s$$

for some positive integer k and a complex number s. For such a representation τ with $s = \sigma + it$, we put $R(\tau) = \sigma$ and call it the real part; it is clear that we have $R(\tau \cdot \omega_s) = R(\tau) + R(s)$. With the above notation, and with τ a finite dimensional representation of G, we define an L-function

$$L(\tau) = \prod_{p \in \Sigma} \frac{1}{\det(I \cdot - \tau(x_p))};$$

a comparison of this L-function with the ordinary Riemann zeta function shows that it is absolutely convergent for $R(\tau) > 1$. It is known that $L(\tau)$ has a holomorphic continuation to the region $R(\tau) \geqslant 1$ for $\tau = (\text{sym}^k r) \cdot \omega_s$ with $k = 1, 2, 3$ and possibly other values not known to the author. Clearly $L(\omega_s) = \zeta(s)$ and so it has a simple pole at $s = 1$. If it could be established that $L(\tau)$ has a holomorphic continuation to $R(\tau) \geqslant 1$ for all representations $\tau = (\text{sym}^k r) \cdot \omega_s$, $k \geqslant 1$, then Deligne's generalization of the method of Hadamard and de la Vallée-Poussin would imply that

$$L(\tau) \neq 0 \quad \text{for all } \tau \text{ with} \quad R(\tau) = 1 .$$

By well known techniques in analytic number theory [9], it would then be possible to prove

The Sato-Tate Conjecture: for large x

$$\sum_{p \leqslant x} \chi(\theta_p) \sim \frac{2}{\pi} \int_J (\sin \theta)^2 d\theta \cdot \frac{x}{\log x},$$

where χ is the characteristic function of the subinterval $J \subset [0, 2\pi)$.

§2. The general setting: Axioms A and B. Deligne's generalization of the Hadamard and de la Vallée-Poussin method applies to a broad class of L-functions which are subjected to two basic axioms. Before we give the statement of the main result we introduce some notation and define the class of L-functions that will be considered.

Let Γ be a group which is isomorphic to $\mathbf{Z}$ or to $\mathbf{R}$. Let $\omega_1 : \Gamma \to \mathbf{R}_+^*$ be a non-trivial quasi-character. Let G be a locally compact group which is an extension of Γ by a compact group $\overset{\circ}{G}$:

$$0 \to \overset{\circ}{G} \to G \to \Gamma \to 0\,.$$

Σ will denote an infinite countable set, and $(x_v)_{v \in \Sigma}$ will be a family of conjugacy classes in G indexed by Σ. The examples of the previous section motivate the following restrictions on the above data.

Axiom A (i) If Γ is isomorphic to $\mathbf{R}$, the extension G is trivial.

(ii) If Γ is isomorphic to $\mathbf{Z}$, the center of G is mapped onto a subgroup of finite index in $\mathbf{Z}$.

It should be observed that since $H^2(\mathbf{R}, \overset{\circ}{G}) = \{1\}$ for any compact group $\overset{\circ}{G}$, the condition $A(i)$ is automatically satisfied, i.e. $G = \overset{\circ}{G} \times \mathbf{R}$ a direct product. One of the many applications that Deligne makes of his main result is to the proof of the Weil conjecture. In this situation it suffices to consider the case where G is the direct product of $\Gamma = \mathbf{Z}$ by a compact Lie group $\overset{\circ}{G}$, whose connected component of the identity $\overset{\circ\circ}{G}$ is semisimple.

The condition $A(ii)$ is not really necessary in the proof of the main result; what does seem to be needed is some sort of control on the growth of the matrix coefficients $\rho_{ij}(g)$ of a continuous finite dimensional representation $\rho : G \to GL(V_{\mathbf{C}})$, for example the boundedness of the matrix coefficients $\rho_{ij}(g)$ will guarantee that the representation ρ is unitarizable. Below we shall see that actually polynomial growth as measured by a power of $\omega_1(g)$ will suffice. In the proof of the Weil conjecture the group G admits a linear representation whose restriction to $\overset{\circ}{G}$ has a finite kernel; for this type of group G it can be shown that A(ii) is automatically satisfied.

With the non-trivial quasi-character $\omega_1 : \Gamma \to \mathbf{R}_+^*$, we associate a family of morphisms

$$\omega_s : G \xrightarrow{pr} \Gamma \to \mathbf{C}^* ,$$

parametrized by complex numbers $s \in \mathbf{C}$:

$$\omega_s(g) = \omega_1(pr(g))^s .$$

The norm of an element $v \in \Sigma$ is defined by $N_v = \omega_{-1}(x_v)$. If Γ is isomorphic to $\mathbf{Z}$, then $\{\omega_1(\gamma) : \gamma \in \Gamma\}$ is a discrete cyclic subgroup of $\mathbf{R}_+^*$ and hence of the form $\{q^{\mathbf{Z}}\}$, where q is a positive real number > 1. This gives rise to an isomorphism

$$\deg : \Gamma \to \mathbf{Z}$$

whose sign we select so that $\omega_1(\gamma) = q^{-\deg(\gamma)}$. We also denote by deg the morphism

$$\deg : G \to \Gamma \to \mathbf{Z}$$

Obtained by composing the projection map $G \to \Gamma$ with deg. In the following we define the degree of an element $v \in \Sigma$ by $\deg(v) = \deg(x_v)$.

In case $\Gamma \simeq \mathbf{Z}$, Axióm A implies there is an element g in the center of G whose image in Γ is non-trivial. Weyl's unitary trick can be used to show that a complex linear representation $\tau : G \to GL(V)$ is equivalent to a unitary representation if and only if $\tau(g)$ is. In fact if ψ is a Hermitian structure on V which is invariant under g, i.e.

$$\psi(\tau(g) \cdot v, \tau(g) \cdot w) = \psi(v, w) , \qquad v, w \in V,$$

then integration over the compact group $H = G/g^{\mathbf{Z}}$ gives a G-invariant form

$$\tilde{\psi}(v, w) = \int_H \psi(\tau(g) \cdot v, \tau(g) \cdot w) dg ,$$

which also defines a Hermitian structure on V. Hence τ is equivalent to a unitary representation.

Consider now the general situation. Let $\tau : G \to GL(V)$ be an irreducible complex linear representation. Let ψ define a Hermitian structure on V. If g belongs to the center, then Schur's Lemma implies $\tau(g)$ is a scalar multiple of the identity. Hence there is a complex number λ such that

$$\psi(\tau(g) \cdot v, \tau(g) \cdot w) = |\lambda|^2 \psi(v, w) .$$

Denote by σ the real number such that $|\lambda| = \omega_1(g)^\sigma = \omega_\sigma(g)$ and observe that the Hermitian form

$$\psi(\tau \cdot \omega_{-\sigma}(g) \cdot v, \tau \cdot \omega_{-\sigma}(g) \cdot w)$$

is now invariant under the action of the center of G. Integration over the quotient. of G by its center gives a G-invariant Hermitian form. Therefore the representation $\tau\omega_{-\sigma}$ is equivalent to a unitary representation. The number σ will be called the real part of the representation τ and is denoted $R(\tau)$. If τ is unitary, then $R(\tau) = 0$ and also $R(\tau\omega_s) = R(\tau) + R(s)$.

The irreducible representations of G of the form $\tau \cdot \omega_s$ with τ unitary will be called quàsi-unitary. We denote by $\tilde{G}$ the family of isomorphism classes of irreducible quasi-unitary representations of G; we let $\hat{G}$ be the subfamily of those which are unitary. On $\tilde{G}$ we consider the equivalence relation: $\tau, \tau' \in \tilde{G}$ are equivalent if τ is in the class of $\tau' \cdot \omega_s$ for some $s \in \mathbf{C}$. Under this equivalence relation $\tilde{G}$ is partitioned into a disjoint union

$$\tilde{G} = \bigcup_{\tau \in \hat{G}} \{\tau \cdot \omega_s \mid s \in \mathbf{C}\}\,.$$

By introducing the parameter s, we may now view an equivalence class of quasi-unitary representations as a Riemann surface. In fact the map $s \to \tau \cdot \omega_s$ identifies the set $\{\tau \cdot \omega_s \mid s \in \mathbf{C}\}$ with

i) The complex plane $\mathbf{C}$ if $\Gamma \simeq \mathbf{R}$ or

ii) with the strip $\mathbf{C} / \dfrac{2\pi i}{\log q} \mathbf{Z}$, if $\Gamma \simeq \mathbf{Z}$ and q is the real number with $\omega_1(\gamma) = q^{-\deg \gamma}$.

As is well known, by viewing $\tilde{G}$ as a collection of Riemann surfaces, it makes sense to talk about the regularity of a function of quasi-unitary representations at a point or in a region, or about its singularities. The question of analytic continuation, when considered on each connected surface, also makes sense.

Remark. It is in the above spirit that the zeros of an L-function should be considered as a discrete set of quasi-unitary representations on the same connected component, and the explicit formulas of number theory should be considered as generalized trace formulas.

Axïom B (i) For every $v \in \Sigma$, one has $Nv > 1$.

(ii) The infinite product $\prod_{v \in \Sigma} (1 - Nv^{-s})^{-1}$ converges absolutely for $R(s) > 1$.

For Γ isomorphic to $\mathbf{Z}$, the first relation means: $\deg(v) > 0$; B(ii) means that

$$\sum_{m=1}^{\infty} \frac{1}{m} \left\{ \sum_{d \mid m} dN_d \right\} q^{-ms}\,,$$

where

$$N_m = \# \{v \in \Sigma \mid \deg(v) = m\}\,,$$

which is the logarithm of the infinite product, converges absolutely for $R(s) > 1$, that is to say for every $\varepsilon > 0$

$$N_m = O(q^{(1+\varepsilon)m}).$$

The condition B(ii) assures that for every $\tau \in \tilde{G}$, the infinite product

$$L(\tau) = \prod_{v \in \Sigma} \frac{1}{\det(I - \tau(x_v))}$$

converges absolutely for $R(\tau) > 1$. Also each factor is holomorphic in τ for $R(\tau) > 0$, and the function $L(\tau)$ is holomorphic for $R(\tau) > 1$ and does not vanish in this region. In the following we put $L(s, \tau) = L(\tau \cdot \omega_s)$.

§3. THEOREM (Deligne). *With the assumptions and notations as above, suppose that* $L(\tau)$ *as a function of* τ *has a meromorphic continuation to* $R(\tau) \geqslant 1$, *and that in this region* $R(\tau) \geqslant 1$ *it is holomorphic except for a simple pole at* ω_1. *Then the function* $L(\tau)$ *does not vanish for* $R(\tau) = 1$, *except possibly for at most one representation* τ_0, *of dimension* 1 *and defined by a character* $\omega_1 \varepsilon$ *with* ε *of order* 2.

§4. THE MAIN LEMMA. For a complex linear representation $\tau : G \to GL(V)$, of dimension d, not necessarily irreducible, we have associated the zeta function

$$L(\tau) = \prod_v L_v(\tau),$$

where

$$L_v(\tau) = \frac{1}{\det(I - \tau(x_v))} = \prod_{i=1}^{d} \frac{1}{1 - \beta_i(v)},$$

and $\beta_1(v), \ldots, \beta_d(v)$ are the eigenvalues of a matrix in the conjugacy class of $\tau(x_v)$. Now for s a complex number we put

$$L(\tau, s) = L(\tau \cdot \omega_s)$$

and define

$$L'(\tau) = \frac{d}{ds} L(\tau\omega_s)\,|_{s=0}\,.$$

In particular, in the domain of absolute convergence for the product

$$L(\tau\omega_s) = \prod_{v \in \Sigma} \prod_{i=1}^{d} \frac{1}{1 - \beta_i(v) N v^{-s}},$$

that is to say for $R(\tau\omega_s) > 1$, we can take the logarithmic derivative with respect to the complex variable s and obtain

$$-\frac{L'}{L}(\tau\omega_s) = \sum_{\substack{v\in\Sigma \\ n>0}} (\log Nv) \cdot Nv^{-sn}\, \chi_\tau(x_v^n)\,.$$

If we let $s = 0$ in the above formula, we obtain for $R(\tau) > 1$

$$-\frac{L'}{L}(\tau) = \sum_{\substack{v\in\Sigma \\ n>0}} (\log Nv)\chi_\tau(x_v^n)\,.$$

In order to deal with L-functions of arbitrary representations we now observe that the above definitions can be extended by linearity to all virtual representations. Let

$$\tau = \sum_{\rho\in\hat{G}} n(\rho)\rho$$

be an element of the Grothendieck group of the category of representations of G; the $n(\rho)$ are integers and all but a finite number are zero. We put

$$L(\tau) = \prod_{\rho\in\hat{G}} L(\rho)^{n(\rho)}$$

and similarly

$$\frac{L'}{L}(\tau) = \sum_{\rho\in\hat{G}} n(\rho)\frac{L'}{L}(\rho)\,.$$

Let μ be a measure on the group G, which we can also consider as a measure on the space of conjugacy classes of G. For every virtual unitary representation

$$\tau = \sum_{\rho\in\hat{G}} n(\rho)\rho\,, \qquad n(\rho) = 0 \qquad \text{for almost all } \rho\,,$$

we put

$$\hat{\mu}(\tau) = \int_G \chi_\tau(g)d\mu\,,$$

where χ_τ is the trace of the representation τ. Since χ_τ is bounded, the integral converges if the total mass of $|\mu|$ is finite. The function $\tau \to \hat{\mu}(\tau)$ will be called the Fourier transform of the measure μ. In analogy with the Harmonic analysis on the group $\mathbf{R}_+^*$, it is useful to consider the integrals $\hat{\mu}(\tau)$ for τ not necessarily unitary; we then refer to $\tau \to \hat{\mu}(\tau)$ as the Fourier-Laplace transform of μ.

Definition. A not necessarily continuous function $f : G \to \mathbf{C}$ is called positive definite if for every choice of $c_1, \ldots, c_n \in \mathbf{C}$ and $g_1, \ldots, g_n \in G$ we have

$$\sum_{i,j} c_i\bar{c}_j f(g_i g_j^{-1}) \geqslant 0\,.$$

A measure μ on the group G is positive, denoted $\mu \geqslant 0$, if for every non-negative function $f : G \to \mathbf{R}_+$ we have $\int_G f(g) d\mu \geqslant 0$.

If μ is a positive measure of finite total mass, then we have for every virtual unitary representation ρ

$$\hat{\mu}(\rho \otimes \bar{\rho}) \geqslant 0 \qquad (\text{for } \mu \geqslant 0) .$$

In fact, since $\chi_{\rho\otimes\bar{\rho}} = | \chi_\rho |^2$ (see Part III, §1) we have

$$\hat{\mu}(\rho \otimes \bar{\rho}) = \int_G \chi_{\rho\otimes\bar{\rho}}(g) d\mu = \int_G | \chi_\rho(g) |^2 \, d\mu \geqslant 0 .$$

More generally, if $c_1, ..., c_n \in \mathbf{C}$ and $\rho_1, ..., \rho_n$ are virtual unitary representations, then we have for any positive measure μ on G with finite total mass

$$\sum_{i,j} c_c \bar{c}_j \hat{\mu}(\rho_i \otimes \bar{\rho}_j) = \int_G | \sum_{i=1}^{n} c_i \chi_{\rho_i}(g) |^2 \, d\mu \geqslant 0 .$$

For a real number $s = \sigma > 1$ and a virtual unitary representation τ, we have that the expression $\Lambda_\sigma(\tau) = -\frac{L'}{L}(\tau\omega_\sigma)$ is the Fourier Transform of the positive measure of finite total mass

$$\mu_\sigma = \sum_{\substack{v \in \Sigma \\ n > 0}} (\log Nv) \cdot Nv^{-n\sigma} \cdot \delta[x_v^n]$$

defined on G, where $\delta[a]$ denotes the Dirac measure concentrated at a. Therefore we have, for every virtual unitary representation ρ of G and $\sigma > 1$

$$\Lambda_\sigma(\rho \otimes \bar{\rho}) = \hat{\mu}_\sigma(\rho \otimes \bar{\rho}) \geqslant 0 .$$

Let $\tau \in \hat{G}$ and let $\nu(\tau)$ denote the order of the pole of L at $\tau\omega_1$, that is to say we write

$$L(\tau\omega_s) = \frac{\tilde{L}(\tau\omega_s)}{(s-1)^{\nu(\tau)}} ,$$

where $\tilde{L}(\tau\omega_s)$ remains bounded and non-zero as $s \to 1$. Since

$$-\frac{L'}{L}(\tau\omega_s) = \frac{\nu(\tau)}{s-1} + f(\tau\omega_s) ,$$

i.e. $\nu(\tau)$ is the residue of $-\frac{L'}{L}$ at $\tau\omega_1$, we can extend the definition of $\nu(\tau)$ by additivity to the Grothendieck group of the category of unitary representations of G. For these we have

$$\begin{aligned} \nu(\tau) &= \lim_{\sigma \to 1^+} (\sigma - 1)\left(-\frac{L'}{L}(\tau\omega_\sigma) + f(\tau\omega_\sigma) \right) \\ &= \lim_{\sigma \to 1^+} (\sigma - 1)\Lambda_\sigma(\tau)\,. \end{aligned}$$

Hence from the inequality $\Lambda_\sigma(\rho \otimes \bar{\rho}) \geqslant 0$ which holds true for $\sigma > 1$, we obtain, since $\sigma - 1 > 0$, that

$$\nu(\rho \otimes \bar{\rho}) \geqslant 0$$

for every virtual unitary representation ρ of G. More generally if $c_1, ..., c_n \in \mathbf{C}$ and $\rho_1, ..., \rho_n$ are virtual unitary representations, then we have

$$\sum_{i,\,j} c_k \bar{c}_j \bar{\nu}(\rho_i \otimes \bar{\rho}_j) \geqslant 0\,,$$

i.e. the symmetric matrix $\{\nu(\rho_i \otimes \bar{\rho}_j)\}$ is positive semi-definite.

The assumptions in the Main Theorem can now be translated into properties about the integer valued function $\nu(\tau)$. First of all the fact that $L(\tau)$ has an analytic continuation to the region $R(\tau) \geqslant 1$ and that $L(\tau)$ is holomorphic in this region except for $L(\omega_s)$ which has a simple pole at $s = 1$ implies that $\nu(\tau) \leqslant 0$ for all $\tau \neq 1$ and $\nu(1) = 1$. If $L(\tau\omega_s)$ has a zero at $s = 1$, then by conjugating the Euler product that defines $L(\tau\omega_0)$ for σ a real number, we see that $L(\bar{\tau}\omega_s)$ also has a zero at $s = 1$ of the same order as $L(\tau\omega_s)$; hence $\nu(\tau) = \nu(\bar{\tau})$. This then reduces the proof of Deligne's Theorem to the following:

Main Lemma. *Let G be a locally compact group; let $\hat{G}$ be the space of irreducible unitary representations of G; consider a function*

$$\nu : \hat{G} \to \mathbf{Z}$$

that satisfies the following conditions:

a) *for the trivial representation* 1, $\nu(1) = 1$

b) $\nu(\tau) = \nu(\bar{\tau})$

c) $\nu(\tau) \leqslant 0$ *for* $\tau \neq 1$

d) $\nu(\tau \oplus \lambda) = \nu(\tau) + \nu(\lambda)$

e) $\nu(\rho \otimes \bar{\rho}) \geqslant 0$ *for every unitary representation* ρ, *i.e.* ν *is positive semi-definite.*

Then $\nu(\tau) = 0$ *for all* $\tau \neq 1$ *except possibly for at most one* τ *of dimension* 1 *and defined by a character of order two.*

§5. Reduction to the compact case: reformulation of the Main Lemma. In outline the proof of the Main Lemma is an adaptation to locally compact groups of the following argument which works for any finite group. The Plancherel theorem for a finite group G gives the decomposition of the regular representation r_G into its irreducible constituents; if χ_r is the character of r_G and χ_τ runs over the characters of the irreducible representation τ of G, then we have

$$\chi_r = \sum_{\tau \in \hat{G}} (\dim \tau)\chi_\tau .$$

Now we recall that the support of χ_r is concentrated at the identity e of G, in fact $\chi_r = | G | \delta[e]$. If we now use that $0 \leqslant \chi_r$ and evaluate the function ν which appears in the Lemma at χ_r and use the property e) we obtain

$$0 \leqslant \sum_{\tau \in \hat{G}} (\dim \tau)\nu(\tau) .$$

Properties a) and c) imply that all the terms in the above sum except $\nu(1) = 1$ are non-positive and therefore at most one other term can have $\nu(\tau) = -1$ and for this representation $\dim \tau = 1$ and $\tau = \bar{\tau}$. Hence such a τ is defined by a character of order 2. In particular, if G admits no subgroup of index two, then there is no exceptional representation.

The adaptation of the above idea consists in obtaining uniform approximations to the character of the regular representation of G by a finite linear combination with positive integer coefficients of the characters of finite dimensional irreducible unitary representations. The approximation should be fairly good so that the character of the corresponding representation is still a non-negative function. As is well known, the proper framework for the study of this type of approximation is the theory of almost periodic functions on the group G. Rather than using the full theory we shall work with an intermediary object, the Bohr Compactification G^b of G, which is a compact group. This will simplify the analysis, since on G^b we can use the full strength of the Peter-Weyl Theorem. In fact, for our purposes, even the Stone-Weierstrass approximation Theorem would suffice.

In the following we recall the basic facts about the Bohr Compactification. The reader can find an exposition of the theory in Weil [11], Chap. VII.

If $\tau : G \to GL(H_\tau)$ is an irreducible unitary linear representation, then the image of G under τ is contained in a unitary subgroup $U(H_\tau)$ of $GL(H_\tau)$; since each $U(H_\tau)$ is a compact group, their product $\prod_{\tau \in \hat{G}} U(H_\tau)$ is also a compact group. We thus obtain a map

$$\eta : G \to \prod_{\tau \in \hat{G}} U(H_\tau)$$
$$g \to (\tau(g))_{\tau \in \hat{G}} .$$

The Bohr compactification of the group G, which we denote by G^b is the closure in $\prod_{\tau \in \hat{G}} U(H_\tau)$ of the image of G under the map η. The main reason for introducing the group G^b is that it is compact and that any irreducible unitary finite dimensional representation $\tau : G \to U(H_\tau)$ factors through a finite dimensional unitary representation of G^b:

$$G \to G^b \to \prod_{\tau \in \hat{G}} U(H_\tau) \xrightarrow{pr_\tau} U(H_\tau) .$$

Now since G has a dense image in G^b, any representation of G^b is irreducible if and only if its restriction to G is irreducible. The group G^b is uniquely defined up to isomorphism by G. By projection, any unitary representation of G can be extended to G^b:

$$\begin{tikzcd} \tau : G \arrow[r] \arrow[d] & U(H_\tau) . \\ G^b & \end{tikzcd}$$

This then establishes an equivalence between the category of finite dimensional unitary representations of G^b and the category of finite dimensional unitary representations of G under which irreducible representations correspond.

More to the point at hand, which is that of obtaining good uniform approximations to the character of the regular representation of G, is the fact that the continuous functions on G^b are in one-to-one correspondence with the almost periodic functions on the locally compact group G in the sense of von Neumann.

For a locally compact abelian group G, Pontrjagin's duality theory gives very precise information about the group G^b. In fact in this case all irreducible representations of G are of dimension 1. The Pontrjagin dual of G is the group of all continuous homomorphisms

$$\hat{G} = \mathrm{Hom}_c(G, \mathbf{T}) ,$$

where $\mathbf{T} = \{z \in \mathbf{C} : |z| = 1\}$ is the circle group; furthermore $\hat{\hat{G}} = G$ and the dual of a compact group is a discrete group and vice versa. Now G^b is a compact abelian group and its character group is

$$\begin{aligned} \hat{G^b} &= \mathrm{Hom}_c(G^b, \mathbf{T}) \\ &= \mathrm{Hom}_c(G, \mathbf{T}) \\ &= \hat{G} . \end{aligned}$$

Hence G^b is the Pontrjagin dual of $\hat{G}$ viewed as a discrete group, i.e. the group of not necessarily continuous homomorphisms

$$G^b = \mathrm{Hom}_{gp}(\hat{G}, \mathbf{T}) .$$

Example 1. If $G = \mathbf{R}$, then $G^b = \mathrm{Hom}_{gp}(\mathbf{R}, \mathbf{T})$, i.e. G^b is the group of all exponential functions $f(x) = e^{ixy}$. The Weierstrass Approximation Theorem describes the relation between the almost periodic functions on $\mathbf{R}$ and the continuous functions on G^b.

Example 2. If $G = \mathbf{Z}$, then $G^b = \mathrm{Hom}_{gp}(\mathbf{T}, \mathbf{T})$. The almost periodic functions on G are closely related with the trigonometric sums

$$\sum_{\lambda} c(\lambda)\chi_{\lambda} , \qquad \sum | c(\lambda) | < \infty ,$$

where $\chi(n) = e^{i\lambda n}$, with real frequencies λ.

Example 3. An example relevant to the theorem at hand is $G = K \times \mathbf{R}$, the direct product of a compact group K and the group of real numbers. The Bohr compactification of G is

$$G^b = K^b \times \mathbf{R}^b .$$

In this situation the general theory shows that the class of central functions f on G with the property that if $\varepsilon > 0$, there exist a finite set of characters of unitary representations $\chi_1, ..., \chi_N$ of K and almost periodic functions $a_1, ..., a_N$ on $\mathbf{R}$ such that for all $g = (k, x)$ in G

$$| f(g) - \sum_{i=1}^{N} \chi_i(k) a_i(x) | < \varepsilon ,$$

coincides with the class of central continuous functions on G^b.

Remark. After this brief interlude into the realm of almost periodic functions on the group G, the reader should keep in mind that it is quite immaterial whether we work with G or with its Bohr compactification. What is really at the heart of the argument is the family of functions F on the group G which can be uniformly approximated by finite linear combinations of the characters of irreducible unitary representations of G with complex coefficients; the structure of F can in turn be described by the Stone-Weierstrass approximation theorem.

In order to establish the Main Lemma we may then assume that G is compact. Most of Part III is devoted to the proof of the following lemma.

Main Lemma (Reformulation). *Let* G *be a compact group; let* $\hat{G}$ *be the space of irreducible unitary representations of* G*; consider a function*

$$\nu : \hat{G} \to \mathbf{Z}$$

that satisfies the following conditions

a) *for the trivial representation* 1, $\nu(1) = 1$

b) $\nu(\tau) = \nu(\bar{\tau})$

c) $\nu(\tau) \leqslant 0$ *for* $\tau \neq 1$

d) $\nu(\tau \oplus \lambda) = \nu(\tau) + \nu(\lambda)$

e) $\nu(\rho \otimes \bar{\rho}) \geqslant 0$ *for every unitary representation* ρ, *i.e.* ν *is positive semi-definite.*

Then $\nu(\tau) = 0$ *for all* $\tau \neq 1$ *except possibly for at most one* τ_0 *of dimension* 1 *and defined by a character of order two.*

Part III: Proof of the Main Lemma

§1. Review of the representation theory of compact groups. We start by recalling some known facts which are standard results from the representation theory of compact groups. Some of these results are elementary, others arise in the proof or are consequences of the Peter-Weyl Theorem.

G will denote a compact topological group; G is endowed with an invariant measure $d\mu$ which we normalize so that $\int_G d\mu = 1$. An important set of functions on G is the space of square integrable functions:

$$L^2(G) = \{f : G \to \mathbf{C} \mid \int_G |f|^2 d\mu < \infty\}.$$

In the following we shall also consider the space of central square integrable functions on G:

$$L_c^2(G) = \{f \in L^2(G) \mid f(aga^{-1}) = f(g) \qquad \text{for all } a \in G\}.$$

Both $L^2(G)$ and $L_c^2(G)$ are Hilbert spaces with the inner product

$$(f, h) = \int_G f \cdot \bar{h} d\mu.$$

By $\hat{G}$ we denote the set of isomorphism classes of irreducible unitary representations of G. To avoid complicated notation, we shall not distinguish between an isomorphism class and its members: each $\rho \in \hat{G}$ is to be thought of as a specific continuous homomorphism

$$\rho : G \to U(V_\rho)$$

into the unitary subgroup $U(V_\rho)$ of a specific Hilbert space V_ρ. The irreducibility of ρ implies that V_ρ has finite dimension which is also called the dimension of ρ and denoted by $\dim(\rho)$.

The Peter-Weyl Theorem. There is an isomorphism of Hilbert spaces

$$(1.1) \qquad L^2(G) \simeq \bigoplus_{\rho\in\hat{G}} V_\rho \otimes V_\rho^* \qquad \text{(Hilbert space direct sum)};$$

in this decomposition the action of G on $L^2(G)$ induced by left translation corresponds to the action on the left factors V_ρ; more precisely, if

$$< , > : V_\rho \otimes V_\rho^* \to \mathbf{C}$$

is the canonical bilinear pairing, we then have a mapping of Hilbert spaces

$$T_\rho : V_\rho \otimes V_\rho^* \to L^2(G)$$

given by $T_\rho(v \otimes \lambda) = < \lambda, \rho(g^{-1})v >$, where the inner product in $V_\rho \otimes V_\rho^*$ is normalized by dividing by $\dim(\rho)$. Similarly the right translation action corresponds to the dual action on the dual space V_ρ^*. The isomorphism (1.1) is obtained by putting together the T_ρ's:

$$T = \bigoplus_{\rho\in\hat{G}} T_\rho : \bigoplus_{\rho\in\hat{G}} V_\rho \otimes V_\rho^* \to L^2(G)\,.$$

To each $\rho \in \hat{G}$ one associates the function

$$\chi_\rho : g \to \text{Trace } \rho(g)\,,$$

the so called character of ρ. Since the eigenvalues of $\rho(g)$ are complex numbers of absolute value 1, χ_ρ is a bounded continuous central function and satisfies

$$|\chi_\rho(g)| \leqslant \chi_\rho(e) = \dim(\rho)\,, \qquad \chi_\rho(g^{-1}) = \chi_{\bar{\rho}}(g)\,.$$

If $\tau, \rho \in \hat{G}$, then it is immediate from the definition of the direct sum $\tau \oplus \rho$ and the tensor product $\tau \otimes \rho$ that

$$\chi_{\rho\oplus\tau} = \chi_\rho + \chi_\tau \qquad \text{and} \qquad \chi_{\rho\otimes\tau} = \chi_\rho \cdot \chi_\tau\,.$$

If ρ and σ are unitary representations of G, their tensor product $\rho \otimes \sigma$ is also a unitary representation and we have a decomposition

$$\otimes\, \tau = \sum_{\tau\in\hat{G}} a(\tau)\tau\,,$$

where the $a(\tau)$ are positive integers and $a(\tau) = 0$ for all but a finite number of τ. The integer $a(\tau)$ is the multiplicity with which the representation τ appears in $\rho \otimes \tau$. If α is a unitary representation of G and β is an irreducible unitary representation of G we denote by $[\alpha : \beta]$ the multiplicity with which β appears in the decomposition of α into irreducible components. Since the character of a unitary representation uniquely determines the class of the unitary representation, we have by the orthogonality relations for the characters that

$$\begin{aligned} [\rho \otimes \sigma : \tau] &= a(\tau) \\ &= \int_G \left(\sum a(t)\chi_\tau(g)\right)\bar{\chi}_\tau(g)d\mu \\ &= \int_G \chi_{\rho\otimes\sigma}(g)\bar{\chi}_\tau(g)d\mu \\ &= \int_G \chi_\rho(g)\chi_\sigma(g)\bar{\chi}_\tau(g)d\mu\,. \end{aligned}$$

A simple combinatorial exercise, using the Maclaurin expansion of $\log(1-T)$, gives for $\rho, \tau \in \hat{G}$ and $H(T, \rho, g) = \det(I - \rho(g)T)$ that

1) $$\frac{H'}{H}(T, \rho, g) = \sum_{n=0}^{\infty} \chi_\rho(g^n)T^n$$

2) $$\frac{H'}{H}(T, \rho \oplus \tau, g) = \sum_{n=0}^{\infty} (\chi_\rho(g^n) + \chi_\tau(g^n))T^n$$

3) $$\frac{H'}{H}(T, \rho \otimes \tau, g) = \sum_{n=0}^{\infty} \chi_\rho(g^n)\chi_\tau(g^n)T^n\,.$$

It is a formal consequence of the Peter-Weyl Theorem, that the character χ_ρ determines ρ up to isomorphism. In particular the map $\rho \to \chi_\rho$ sets a one-to-one correspondence between the family of irreducible unitary finite dimensional representations of G and the set of characters of irreducible representations.

Remark. The Peter-Weyl Theorem together with Weyl's character formula and Cartan's Theorem about the highest weight constitute the fundamentals of the representation theory of compact Lie groups.

As a special case of the Peter-Weyl Theorem, we have that the collection $\{\chi_\rho\}_{\rho\in\hat{G}}$ forms an orthonormal basis for the space $L_c^2(G)$ of square integrable central functions on G. For our purposes the following result will suffice; a proof of it can easily be obtained from the Stone-Weierstrass approximation theorem.

Weyl's Approximation Theorem. On a compact group every continuous central complex valued function f can be uniformly approximated by finite linear combinations with complex coefficients of the characters $\{\chi_\rho\}_{\rho\in\hat{G}}$.

Remark. The above theorem means that for every continuous central function $f : G \to \mathbf{C}$ and for every $\varepsilon > 0$, there is a finite linear combination

$$f' = \sum_{\rho \in \hat{G}} c(\rho)\chi_\rho ,$$

where $c(\rho) \in \mathbf{C}$ and $c(\rho) = 0$ for all but a finite number of ρ, such that $| f(x) - f'(x) | < \varepsilon$ for all $x \in G$.

Existence of Invariant Symmetric Neighborhoods: On a compact topological group there exist arbitrarily small invariant symmetric neighborhoods of the identity, i.e. a neighborhood N of the identity such that

1) (Symmetric) $N^{-1} = N$

2) (Invariant) $x^{-1}Nx = N$ for all $x \in G$.

To establish this result recall that the unique topology carried by the topological group G is defined by a base $\mathscr{B}(e)$ for the filter of neighborhoods of the identity. $\mathscr{B}(e)$ satisfies the following properties

(i) For every $x \in G$ and $A \in \mathscr{B}(e)$, there is a B in $\mathscr{B}(e)$ such that $B \subseteq x^{-1}Ax$.

(ii) For every pair of sets A, B in $\mathscr{B}(e)$, there is a C in $\mathscr{B}(e)$ such that $C \subseteq A \cap B$.

(iii) The identity belongs to every set A of $\mathscr{B}(e)$.

(iv) For every A in $\mathscr{B}(e)$ there is a $B \in \mathscr{B}(e)$ such that $B^{-1} \subseteq A$.

(v) For every $A \in \mathscr{B}(e)$ there is a $\mathscr{B}$ in $\mathscr{B}(e)$ such that $B^2 \subseteq A$.

Now let N_e be an arbitrary neighborhood of the identity. By (ii), (iv) and (v) there is a neighborhood B of e such that $B = B^{-1}$ and $B^3 \subseteq N_e$. The family of interiors $xB^i(x \in G)$ cover G so by the compactness of G there is a finite set $x_1, \ldots, x_n$ in G such that $x_1B^i, \ldots, x_nB^i$ cover G. By (i) and (ii) there is a neighborhood C of e such that $x_k^{-1}Cx_k \subseteq B$ for each k. Now given any $g \in G$, we have $g \in x_kB$ for some k and so $g^{-1}Cg \subseteq Bx_k^{-1}Cx_kB \subseteq B^3 \subseteq N_e$. Now let W be the union of all $g^{-1}Cg$, with $g \in G$. This is clearly contained in N_e. By (ii) there is a symmetric neighborhood U in $\mathscr{B}(e)$ such that $U \subseteq W \cap W^{-1}$. Clearly $U \subseteq N_e$. This proves the result.

§2.1. THE BEGINNING OF THE PROOF OF THE MAIN LEMMA. We fix $\varepsilon > 0$ and a finite subset $\Lambda \subset \hat{G}$, which contains the trivial representation. Now choose a symmetric invariant neighborhood U of the identity which satisfies

$$| \chi_\lambda(g) - \dim \lambda | \leqslant \varepsilon$$

for all $g \in U$ and all $\lambda \in \Lambda$. Let us first prove an

Auxiliary Lemma. If U is a symmetric, invariant neighborhood of e, then there is a continuous function

$$f : G \to \mathbf{R}_+$$

which satisfies

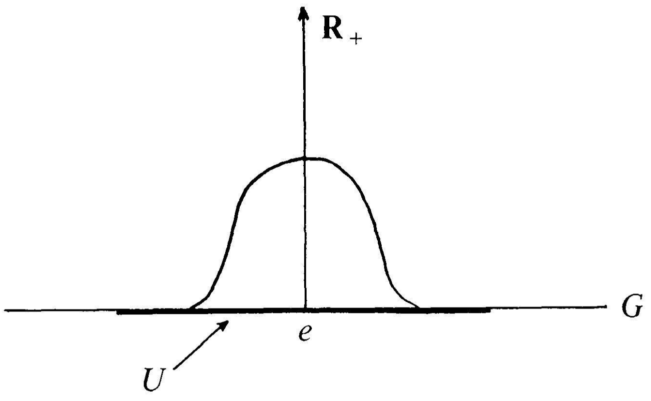
(i) $f(g) = f(g^{-1})$

(ii) $f(aga^{-1}) = f(g)$, for every $a \in G$

(iii) the support of f is contained in U

(iv) $f(e) > 0$.

Remark. The graph of such a function would have the following shape



To prove the existence of f we proceed as follows. As in the proof of the existence of the symmetric invariant neighborhood U, we can find a neighborhood A of e such that $A^2 \subseteq U$; we may also suppose that the measure of A satisfies $\mu(A) > 0$. Let χ_A be the characteristic function of A and let $h(x)$ be the convolution of χ_A with itself

$$h(x) = \chi_A{}^*\chi_A(x) = \int_G \chi_A(y)\chi(x^{-1}y)dy\,.$$

$h(x)$ is a continuous function of x and satisfies $h(e) = \mu(A) > 0$. The support of h is clearly contained in $A^2 \subseteq U$. Now define a function

$$f(x) = \int_G h(g^{-1}xg)d\mu(g)$$

clearly $f(e) = h(e) > 0$ and $f(x)$ is central. Since U is invariant we see that if $x \notin U$, then $g^{-1}xg \notin U$ for all $g \in G$; therefore the support of f is contained in U. If necessary we may replace $f(g)$ by $(f(g) + f(g^{-1}))/2$ to obtain a function f which satisfies $f(g) = f(g^{-1})$. This proves the Auxiliary Lemma.

Claim 1. The real part of the integral

$$\int_G f(g)^2\,(\chi_\lambda(g) - \dim\lambda + 2\varepsilon)d\mu$$

is >0 for all $\lambda \in \Lambda$.

Proof. Observe that the integral is equal to

$$\int_U f(g)^2\,(\chi_\lambda(g) - \dim\lambda + 2\varepsilon)d\mu$$

and that on U

$$|\,\chi_\lambda(g) - \dim\lambda + 2\varepsilon\,| > \varepsilon$$

for all $\lambda \in \Lambda$. The claim is now clear.

We now want to replace f by a function f_0 which approximates it and has the form

$$(*) \qquad f_0(g) = \sum_{\mu\in\hat{G}} n(\mu)\chi_\mu(g)\,,$$

where $n(\mu) = n(\bar{\mu}) \in \mathbf{Z}$ and almost all $n(\mu)$ are 0. We first use Weyl's Approximation Theorem to obtain an ordinary approximation to f of the form (*) with the $n(\mu)$'s complex numbers. Secondly since $f(g) = f(g^{-1})$ and $\chi_{\bar{\mu}}(g) = \chi_\mu(g^{-1})$, we observe that $\bar{f_0}$ is also a good approximation to f; thus if necessary we may replace f_0 by $\frac{1}{2}(f_0 + \bar{f_0})$ in order to obtain a function f_0 of the form (*) with $n(\mu) = n(\bar{\mu})$. Thirdly, since f is real valued, we may replace the $n(\mu)$'s by their real parts $R(n(\mu))$; this gives a function f_0 of the form (*) with $n(\mu)$'s real numbers. We then approximate the $n(\mu)$ by rational numbers so that we may suppose that our original function f is sufficiently close to a function of the form (*) with the $n(\mu) = n(\bar{\mu}) \in \mathbf{Q}$. If this is the case, then the inequality in Claim 1 still remains true when f is replaced by f_0:

$$(**) \qquad Re \int_G f_0(g)^2\,(\chi_\lambda(g) - \dim\lambda + 2\varepsilon)d\mu \geqslant 0\,, \qquad \text{for all } \lambda \in \Lambda\,.$$

Since this inequality is "homogeneous" in f_0 we may multiply it by the square of a large positive integer which is a multiple of all the denominators of the $n(\mu)$'s. In this way we obtain a function f_0 in (*) with $n(\mu) = n(\bar{\mu}) \in \mathbf{Z}$ and which satisfies (**).

Let us put $f_0 = f_0^+ - f_0^-$ with

$$f_0^+ = \sum_{n(\mu)>0} n(\mu)\chi_\mu \quad \text{and} \quad f_0^- = \sum_{n(\mu)<0} - n(\mu)\chi_\mu\,.$$

f_0^+ and f_0^- are the characters of two unitary representations which we denote by ρ^+ and ρ^-. It should be pointed out that the representations ρ^+ and ρ^- have no component in common, i.e. $\int_G f_0^+ \cdot f_0^-\,d\mu = 0$.

Claim 2. The real part of

$$\int_G (f_0^+ + f_0^-)^2 (\chi_\lambda(g) - \dim \lambda + 2\varepsilon) d\mu$$

is positive for all $\lambda \in \Lambda$.

Proof. The integral is equal to

$$\int_G (f_0^+ - f_0^-)^2 (\chi_\lambda(g) - \dim \lambda + 2\varepsilon) d\mu + \int_G 4 f_0^+ \cdot f_0^- \chi_\lambda(g) d\mu + (-\dim \lambda + 2\varepsilon) \int_G 4 f_0^+ f_0^- d\mu .$$

The third integral is clearly 0. The second integral is a positive integer, because it is the multiplicity with which the irreducible unitary representation $\bar{\lambda}$ appears in the tensor product $\rho^+ \otimes \rho^-$. The first integral has positive real part as follows from the inequality in Claim 1 (**).

Consider now the representation $\rho = \rho^+ + \rho^-$; clearly $\chi_\rho = f_0^+ + f_0^-$. In our context the representation ρ plays the role of the regular representation. Let us observe that the inequality in Claim 2 can be written in the form

$$Re \int_G \chi_{\rho\otimes\bar{\rho}}(g) \chi_\lambda(g) d\mu \geqslant \{Re \int_G \chi_{\rho\otimes\bar{\rho}}(g) d\mu\} (\dim \lambda - 2\varepsilon) ;$$

both of the integrals appearing here are real numbers and hence the integrals themselves satisfy the inequality, i.e.

$$\int_G \chi_{\rho\otimes\bar{\rho}}(g) \chi_\lambda(g) d\mu \geqslant (\dim \lambda - 2\varepsilon) \int_G \chi_{\rho\otimes\bar{\rho}}(g) d\mu .$$

The integral on the left hand side represents the multiplicity with which the representation $\bar{\lambda}$ appears in the representation $\rho \otimes \bar{\rho}$:

$$[\rho \otimes \bar{\rho} : \bar{\lambda}] = \int_G \chi_{\rho\otimes\bar{\rho}}(g) \chi_\lambda(g) d\mu ;$$

similarly, the integral on the right hand side represents the multiplicity with which the trivial representation $\tau = 1$ appears in $\rho \otimes \bar{\rho}$:

$$[\rho \otimes \bar{\rho} : 1] = \int_G \chi_{\rho\otimes\bar{\rho}}(g) d\mu .$$

With the above notation, the last inequality can be written in the form

$$(***) \qquad [\rho \otimes \bar{\rho} : \lambda] \geqslant [\rho \otimes \bar{\rho} : 1] (\dim \lambda - 2\varepsilon) , \qquad \text{for all } \lambda \in \Lambda .$$

§2.2. Conclusion of the Proof of the Main Lemma. We first decompose the representation $\rho \otimes \bar{\rho}$

$$\rho \otimes \bar{\rho} = \sum_{\mu \in \hat{G}} [\rho \otimes \bar{\rho} : \mu] \mu, \; [\rho \otimes \bar{\rho} : \mu] = \int_G \chi_{\rho\otimes\bar{\rho}}(g) \chi_\mu(g) dg ;$$

we then use the additivity property of the order function ν and its positive definiteness to obtain that

$$0 \leqslant \nu(\rho\otimes\bar{\rho}) = [\rho \otimes \bar{\rho} : 1]\nu(1) + \sum_{\substack{\mu\in\hat{G} \\ \mu\neq 1}} [\rho \otimes \bar{\rho} : \mu]\nu(\mu) .$$

Now since the sum is nonpositive the inequality remains true if we restrict the summation to those $\mu \in \Lambda$, $\mu \neq 1$:

$$0 \leqslant [\rho \otimes \bar{\rho} : 1]\nu(1) + \sum_{\substack{\lambda\in\Lambda \\ \lambda\neq 1}} [\rho \otimes \bar{\rho} : \lambda]\nu(\lambda) ;$$

from the inequality (***) we then obtain

$$0 \leqslant [\rho \otimes \bar{\rho} : 1]\nu(1) + \sum_{\substack{\lambda\in\Lambda \\ \lambda\neq 1}} [\rho \otimes \bar{\rho} : 1] (\dim \lambda - 2\varepsilon)\nu(\lambda) ;$$

hence

$$0 \leqslant [\rho \otimes \bar{\rho} : 1] \{\nu(1) + \sum_{\substack{\lambda\in\Lambda \\ \lambda\neq 1}} (\dim \lambda - 2\varepsilon)\nu(\lambda)\} .$$

Letting $\varepsilon \to 0$ and observing that $[\rho \otimes \bar{\rho} : 1] \geqslant 1$ we obtain finally that

$$0 \leqslant \sum_{\lambda\in\Lambda} (\dim \lambda)\nu(\lambda)$$

for any finite set $\Lambda \subset \hat{G}$ which contains the trivial representation. The Main Lemma now follows from the last inequality by observing that besides the term $\nu(1) = 1$, there can occur at most one other non-zero term with $\nu(\tau) = -1$ and $\dim \tau = 1$. Thus $\tau_0 = \bar{\tau}_0$ must be of order 2. This completes the proof of the Main Lemma and hence also of Deligne's Theorem.

§3.1. CONDITIONS UNDER WHICH $L(\tau) \neq 0$ FOR ALL τ WITH $R(\tau) = 1$. The question still remains whether the exceptional representation τ_0 in the main theorem actually exists. We now want to show that axioms A and B and the assumptions which appear in the statement of the theorem are not enough to imply the non-existence of τ_0. In fact we construct a set of data $\{G, (x_v)_{v\in\Sigma}, \omega_1\}$ and exhibit the particular character τ_0 for which $L(\tau_0) = 0$. We then propose a condition, called Axiom C, which is quite natural from the point of view of the applications to number theory and algebraic geometry and which can be incorporated into the statement of the theorem so as to guarantee that $L(\tau) \neq 0$ for all τ with $R(\tau) = 1$.

Let us recall that the first instance of a calculation implying the non-vanishing of an L-function associated with a quadratic character seems to be the representation obtained by Leibniz of $\frac{\pi}{4}$ as an infinite series

$$\frac{\pi}{4} = 1 - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} + \ldots$$

In fact the series above is simply the value at $s = 1$ of the L-function

$$L(s, \chi) = \prod_p \frac{1}{1 - \chi(p)p^{-s}},$$

where $\chi(p) = 1$ if $p \equiv 1 \bmod 4$ and $\chi(p) = -1$ if $p \equiv 3 \bmod 4$, i.e. χ is the character which corresponds by class field theory to the Gaussian field $\mathbf{Q}(i)$. These ideas were fully developed by Dirichlet who proved that an ordinary L-function $L(s, \chi)$ associated with a character χ of the second order never vanishes at $s = 1$; this he did by explicitly evaluating $L(1, \chi)$ as a non-zero number. It is unfortunate that in the generality in which we want to work, the ideas of Dirichlet do not seem to apply directly to the L-functions $L(\tau)$. In searching for an appropriate variant of Dirichlet's argument which could be applied to $L(\tau)$ we are lead to the method introduced by Merten in 1897 to show that $L(1, \chi) \neq 0$ for any real character χ without explicitly evaluating the L-function. Merten's idea consists in 1.) exploiting boundedness of the partial sums of the values of χ: if χ is a character of conductor f, then

$$\sum_{N \leqslant n \leqslant m} \chi(n) = O(f)$$

and 2.) observing that for χ a character of order 2, the function

$$a(n) = \sum_{d|n} \chi(d)$$

satisfies $a(n) \geqslant 0$ for all n and $a(n^2) \geqslant 1$ (see [8], p. 133).

A careful analysis of Merten's proof and a translation of Dirichlet's theorem on primes in arithmetic progressions into a statement about the distribution of conjugacy classes of the Galois groups of cyclotomic extensions already reveals what could go wrong in the more general situation dealt with in the Main Theorem; it also shows what makes possible the existence of a character τ_0 with $L(\tau_0) = 0$. In this respect, Weber's proof of the Prime Ideal Theorem and Beurling's analysis of the distribution of generalized prime numbers [2] are also of some relevance.

§3.2. An example of a representation τ_0 with $L(\tau_0) = 0$. Consider the extension

$$0 \to \overset{\circ}{G} \to G \to \mathbf{R} \to 0$$

with $G = \overset{\circ}{G} \times \mathbf{R}$ the direct product of the reals $\mathbf{R}$ with $\overset{\circ}{G} = \mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$ the Galois group of the separable closure of the rationals $\bar{Q}$. For each rational prime p we let F_p denote the Frobenius conjugacy class in $\overset{\circ}{G}$. For Σ we take the set of all rational primes $p \equiv 3 \bmod 4$. For each $p \in \Sigma$ we consider the conjugacy class of G

$$x_p = \left\{F_p, -\log \frac{P}{2}\right\}.$$

The set $(x_p)_{p\in\Sigma}$ will play the role of the countably infinite family of conjugacy classes in G. The quasi-character $\omega_1 : \mathbf{R} \to \mathbf{R}_+^*$ is $\omega_1(r) = e^r$. Similarly $\omega_s : G \to \mathbf{C}^*$ is given by composing the projection map $G \to \mathbf{R}$ with ω_1^s. In particular we have $\omega_s(x_p) = \left(\frac{2}{p}\right)^s$. Axiom A is clearly satisfied. As for Axiom B we certainly have $\omega_{-1}(x_p) = \frac{p}{2} > 1$ and if $s \in \mathbf{C}$ satisfies $R(s) > 1$, then the Euler product

$$L(\omega_s) = \prod_{p\in\Sigma} \frac{1}{1 - \omega_s(x_p)} = \prod_{p\equiv 3 \bmod 4} \frac{1}{1 - \left(\frac{2}{p}\right)^s}$$

converges absolutely. In fact if $\sigma > 1$, then $L(\omega_\sigma)$ can be compared with $\zeta(\sigma)^{2^\sigma}$. Now let τ_0 be the character of G corresponding to the quadratic extension $\mathbf{Q}(i)/\mathbf{Q}$. From elementary number theory we know that

$$\tau_0(F_p) = \begin{cases} 1 & \text{if} \quad p \equiv 1 \bmod 4 \\ -1 & \text{if} \quad p \equiv 3 \bmod 4 \end{cases}.$$

Thus we have $\tau_0(F_p) = -1$ for all $p \in \Sigma$. We want to show that the L-function

$$L(\tau_0\omega_s) = \prod_{p\in\Sigma} \frac{1}{1 - \tau_0\omega_s(F_p)}$$

has a zero at $s = 1$. In fact we observe that

$$L(\tau_0\omega_s) = \prod_{p\in\Sigma} \frac{1}{1 - \tau_0(F_p)\left(\frac{p}{2}\right)^{-s}} = \prod_{p\equiv 3 \bmod 4} \frac{1}{1 + \left(\frac{2}{p}\right)^s};$$

if we multiply $L(\tau_0\omega_s)$ by

$$L(\omega_s) = \prod_{p\in\Sigma} \frac{1}{1 - \omega_s(F_p)}$$

we obtain

$$L(\omega_s)L(\tau_0\omega_s) = \prod_{p\equiv 3 \bmod 4} \frac{1}{1 - \left(\frac{2}{p}\right)^{2s}},$$

which is a function holomorphic and free of zeros in the region $R(s) > \frac{1}{2}$. Therefore to show that $L(\tau_0\omega_s)$ has a zero at $s = 1$, it suffices to show that $L(\omega_s)$ has a simple pole at $s = 1$ and otherwise is holomorphic and free of zeros in the region $R(s) \geqslant 1$. This information is a simple consequence of Beurling's theory of generalized prime systems [2]; it can also be obtained more directly by using the prime number theorem for arithmetic progressions to obtain the asymptotic law

$$\# \left\{\frac{p}{2} \leqslant x \mid p \equiv 3 \bmod 4\right\} \sim \frac{x}{\log x}.$$

A still simpler approach consists in using the identity

$$L(\omega_s) = f_1(s)f_2(s)f_3(s)\frac{\zeta(s)}{L(s, \tau_0)},$$

where $\zeta(s)$ is the Riemann zeta function, $L(s, \tau_0)$ is the ordinary Dirichlet series associated with the character τ_0, and whose value at $s = 1$ is given by the Leibniz series, and

$$f_1(s) = \prod\left(1 - \frac{2}{p^s}\right)\left(1 - \left(\frac{2}{p}\right)^s\right)^{-1}$$

$$f_2(s) = \prod\left(1 - \frac{1}{p^s}\right)^2\left(1 - \frac{2}{p^s}\right)^{-1}$$

$$f_3(s) = \prod\left(1 + \frac{1}{p^{2s}}\right)^{-1}$$

where each product is taken over all the prime $p \equiv 3 \bmod 4$. All the functions $f_i(s)$ are well defined and distinct from 0 at $s = 1$; $L(1, \tau_0) = \frac{\pi}{4}$. Therefore $L(\omega_s)$ has a simple pole at $s = 1$ and $L(\tau_0\omega_s)$ has a simple zero at $s = 1$. Let us also observe that the other hypothesis in the Main Theorem are satisfied. All the L-functions $L(\tau\omega_s)$ associated with finite dimensional representations $\tau\omega_s$ of G, where τ are representations of the Galois group $\overset{\circ}{G}$ distinct from τ_0 and the trivial representation are holomorphic in the region $R(s) \geqslant 1$. This can be shown by an argument similar to that given above for $L(\tau_0\omega_s)$. We prefer to use estimates like those which enter into the proof of the Chebotarev density theorem. For these purposes it is enough to verify that

$$\sum_{p \in \Sigma} \chi_\tau(F_p) = O\left(\frac{x}{(\log x)^m}\right), \qquad \text{some } m > 0\,,$$

(χ_τ = Trace τ). But this is clear because

$$\begin{aligned}\sum_{p \in \Sigma} \chi_\tau(F_p) &= \sum_{p \leqslant x} \frac{1}{2}(1 - \tau_0(F_p))\chi_\tau(F_p) \\ &= \frac{1}{2}\sum_{p \leqslant x} \chi_\tau(F_p) - \frac{1}{2}\sum_{p \leqslant x} \tau_0\chi_\tau(F_p) \\ &= O\left(\frac{x}{(\log x)^m}\right),\end{aligned}$$

where the last estimate results because the ordinary Artin L-functions $L(s, \tau)$ and $L(s, \tau_0\tau)$ are holomorphic and free of zeros in the region $R(s) \geqslant 1$.

Remark. It should now be possible for the reader to construct infinitely many other examples like the one given above by considering polynomials other than $x^2 + 1$. Similar examples in the geometric case $\Gamma \simeq \mathbf{Z}$ are also possible.

§3.3. Axiom C and an addendum to Deligne's Theorem. In order to remove the possibility of the existence of a representation like τ_0 we now formulate a condition that guarantees a certain amount of equi-distribution of the conjugacy classes $(x_v)_{v \in \Sigma}$ when restricted to subgroups of finite index in G. The guiding requirements are i) to postulate that the given family of conjugacy classes $(x_v)_{v \in \Sigma}$ is not completely outside a certain subgroup of index 2 and ii) to postulate that the data $\{G, (x_v)_{v \in \Sigma}, \omega_1\}$ behaves properly under *base change.* More precisely, we suppose that we are given data $\{G, (x_v)_{v \in \Sigma}, \omega_1\}$ as in Part II, §2. Now consider a subgroup G' of G of finite index in G. A conjugacy class x_v in G can be thought of as an orbit

$$x_v = \{gag^{-1} \mid g \in G\}\,.$$

If we let $G = \bigcup_j G'\sigma_j$ be a left coset decomposition of G modulo G'. Then we can split x_v into the disjoint union of orbits under G':

$$x_v = \bigcup_j \{g(\sigma_j a \sigma_j^{-1})g^{-1} \mid g \in G'\}\,;$$

some of these orbits will belong to G' others will lie outside. We denote by

$$s(v) = (x_w)_{w|v}$$

the collection of conjugacy classes in G' contained in x_v and say that the index w divides v; the set $s(v)$ may possibly be empty. Given a subgroup G' of finite index in G it is often convenient to think of the countable family $\{s(v)\}_{v\in\Sigma}$ of conjugacy classes in G' as a covering of the family $(x_v)_{v\in\Sigma}$. For a given v, we attach an integer $d(w)$ to each divisor w of v. This should be done coherently so that $\sum_{w|v} d(w) = [G : G']$. At any rate, the choice $d(w) = [G : G']/\# s(v)$ will suffice when G' is normal in G. In order to obtain a coherent system of norms which fits well with the commutative diagram

$$\begin{tikzcd}
0 \arrow[r] & G'^{\circ} \arrow[r] \arrow[d] & G' \arrow[r] \arrow[d] & \Gamma' \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & G^{\circ} \arrow[r] & G \arrow[r] & \Gamma \arrow[r] & 0
\end{tikzcd}$$

we now extend the quasi character $\omega_1 : \Gamma \to \mathbf{R}_+^*$ to a quasi-character

$$\omega_1' : \Gamma' \to \mathbf{R}_+^*$$

so that

$$\omega_1'(x_w) = \omega_1(x_v)^{d(w)},$$

whenever the conjugacy class x_w is contained in x_v. With the above notations we can now make the following definition.

Definition. For a subgroup G' of finite index in G, the data $\{G', (x_w)_{w\in\Sigma'}, \omega_1'\}$ is called the *base-change* of $\{G, (x_v)_{v\in\Sigma}, \omega_1\}$ to G'.

If G' is a normal subgroup of G, then a combinatorial argument of a rather simple nature ([7], page 248) shows that if the L-function of a representation τ' of G' is defined by

$$L(\tau', G') = \prod_{w\in\Sigma'} \frac{1}{\det\left(I - \tau'(x_w)\right)},$$

then we have

$$L(\tau', G') = \prod_{\sigma} L(\tau'\otimes\sigma, G)^{n(\sigma)},$$

where

$$r = \sum_{\sigma} n(\sigma)\sigma$$

is the decomposition of the regular representation of the finite group G/G' and $L(\tau'\otimes\sigma, G)$ is a twisted L-function defined on $\{G, (x_v)_{v\in\Sigma}, \omega_1\}$ as in [7], page 248. We now state the third requirement that the L-functions $L(\tau)$ must satisfy.

Axiom C. Let G' be a subgroup of G of index 2. For the principal L-function $L(\omega'_s)$ associated to the quadratic base-change $\{G', (x_w)_{w \in \Sigma'}, \omega'_1\}$ we have a decomposition

$$L(\omega'_s) = L(\omega_s)L(\tau_0\omega_s),$$

where $\tau_0 : G \to \mathbf{C}^*$ is the real character of order 2 with $\mathrm{Ker}(\tau_0) = G'$.

We can now add to the main result of Deligne the following statement.

THEOREM. *With the hypothesis and notation as in the Main Theorem (Part II, §3), suppose furthermore that the principal L-function* $L(\omega'_s)$ *associated to any quadratic base change* $\{G', (x_w)_{w \in \Sigma'}, \omega'_1\}$ *satisfies Axiom C and has a simple pole at* ω'_1, *then the exceptional character* τ_0 *does not exist and* $L(\tau) \neq 0$ *for all* τ *with* $R(\tau) = 1$.

The proof is clear, since if $L(\tau_0\omega_s)$ has a zero at $s = 1$, then the pole of $L(\omega_s)$ would be cancelled and $L(\omega'_s)$ would be regular at $s = 1$.

BIBLIOGRAPHY

[1] ARTIN, E. Quadratische Körper im Gebiet der hoheren Kongruenzen I, II. *Math. Zeitschrift 19* (1924), 153-246.

[2] BATEMAN, P. T. and H. DIAMOND. Asymptotic distribution of Beurling's generalized prime numbers. *Studies in Number Theory, M.A.A. Studies Vol. 6* (1969), 152-210.

[3] DELIGNE, P. La conjecture de Weil II. *Publ. Math. I.H.E.S., No. 52* (1980).

[4] DAVENPORT, H. und H. HASSE. Die Nullstellen der Kongruenz zetafunktion in gewissen zyklyschen Fällen. *Crelle's Journ. Vol. 172* (1934), 151-182.

[5] KATZ, N. *Deligne's second proof of the Riemann Hypothesis.* (Notes by A. Adolphson, Princeton 1979.)

[6] MESSING, W. Short sketch of Deligne's proof of the Hard Lefschetz Theorem. *Proc. Symposia Pure Math., Vol. 29* (1975), 563-580.

[7] MORENO, C. Kunneth formula for *L*-functions. *Number Theory Carbondale* (Editor: M. B. Nathanson), *L.N. Math. Vol. 751* (1979), 253-255. Springer-Verlag.

[8] RADEMACHER, H. *Lectures on Elementary Number Theory.* Blaisdell Publ. Co., New York, 1964.

[9] SERRE, J.-P. *Abelian l-adic Representations and Elliptic Curves.* W. A. Benjamin, Inc., New York, 1968.

[10] SMITH, R. A. On *n*-dimensional Kloosterman sums. *C.R. Math. Rep. Acad. Sci. Canada, Vol. 1, No. 3* (1979), 173-176.

[11] WEIL, A. *L'integration dans les groupes topologiques et ses applications.* Hermann, Paris, 1965.

[12] YOSHIDA, H. On an analogue of the Sato Conjecture. *Inventiones Math. Vol. 19* (1973), 261-277.

(Reçu le 30 septembre 1982)

Carlos J. Moreno

Department of Mathematics
University of Illinois at Urbana
Urbana, Illinois 61801