Part III: Proof of the Main 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:

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

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

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

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 $x_1, ..., x_n$ in G such that $x_1B^i, ..., x_nB^i$ 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

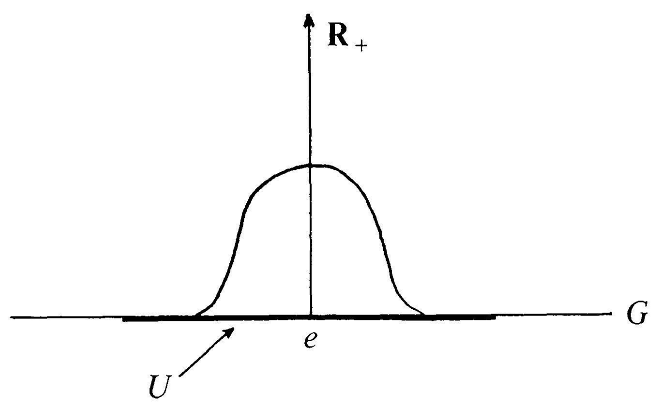
(i) $f(g) = f(g^{-1})$

(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

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

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

$$\begin{array}{ccccccccc} 0 & \to & G'^{\circ} & \to & G' & \to & \Gamma' & \to & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \to & G^{\circ} & \to & G & \to & \Gamma & \to & 0 \end{array}$$

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 $s = 1$.