COMPOSITIO MATHEMATICA

DANIEL S. KUBERT
STEPHEN LICHTENBAUM

# Jacobi-sum Hecke characters and Gauss-sum identities

*Compositio Mathematica*, tome 48, n° 1 (1983), p. 55-87
<http://www.numdam.org/item?id=CM_1983__48_1_55_0>

COMPOSITIO MATHEMATICA, Vol. 48, Fasc. 1, 1983, pag. 55–87


# JACOBI-SUM HECKE CHARACTERS AND GAUSS-SUM IDENTITIES

Daniel S. Kubert* and Stephen Lichtenbaum*

In this paper we study Jacobi-sum Hecke characters of mixed level. Jacobi-sum Hecke characters were introduced by Weil in his fundamental paper [1], where he only considered the case of a cyclotomic field. The definition was extended to arbitrary abelian fields by Weil [2] and Deligne [3], but always keeping the level fixed. Weil, in [2], gives necessary and sufficient conditions for a candidate for a Jacobi-sum Hecke character to actually be one (which amount to saying that the infinity-type is an element of the integral group ring). Deligne goes on to associate a product of values of the $\Gamma$-function to each Jacobi-sum Hecke character (or, more precisely, to each Jacobi-sum representation, since these may not be unique). In [4] he shows that if the infinity-type is a power of the norm, so the Hecke character is $\chi\mathbb{N}^k$, where $\chi$ is a Dirichlet character, then the above $\Gamma$-product, divided by $(2\pi i)^k$, is algebraic and transforms via $\chi$.

We extend the theorems of Weil and Deligne to the case of Jacobi-sum characters of mixed level. In [5], one of the authors extends the definition of Jacobi-sum Hecke character and the theorem of Weil still further, by allowing composition with the norm to smaller fields. Our work leads naturally to the introduction of new identities involving Gauss sums, generalizing those of Hasse–Davenport ([6]). These identities had previously been discovered and proved by Langlands in his work on Artin root numbers, but had never been published. We were unfortunately unaware of this. They follow here as easy consequence of our results and appear in Section 6.

The original motivation for this work was an investigation by one of the authors of the relationship between the value at zero of the $L$-function of a Jacobi-sum Hecke character of an imaginary quadratic

* Supported in part by NSF grants.

0010-437X/83/01/0055–33$0.20

field and its $\Gamma$-product ([7]). For such a relation to exist, the $\Gamma$-product of any representation of the trivial character over an imaginary quadratic field has to be rational, and this is an immediate consequence of our generalization of Deligne's theorem.

Our proofs rely on the original results of Weil and Deligne, but we do give an independent proof of Deligne's theorem if $K \subset \mathbb{Q}(\mu_p)$ for $p$ prime.

*Notations.*

$\mathbb{N}$: depending on the context, the Norm Hecke character, the norm in the group ring of a finite group, the norm relative to a finite field extension, or the norm of a prime ideal.

$\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$: The integers, rationals, reals and complexes.

$\langle x \rangle$: The unique real number $y$ such that $0 \leq y < 1$ and $y \equiv x \pmod{\mathbb{Z}}$.

$\langle y \rangle_N$: The remainder of the integer $y$ when divided by $N$.

$\# S$: The cardinality of the finite set $S$.

## §1. The statement of the theorem

Let $F$ be a finite field, $\chi$ and $\psi$ non-trivial multiplicative and additive characters of $F$ to $\mathbb{C}^x$, respectively. We define the (modified) Gauss sum $G(\chi, \psi)$ to be $-\sum_{x \in F^x} \chi^{(x)} \psi(x)$. If $F$ has characteristic $p$, we fix once and for all the additive character $\psi(x) = (e^{\frac{2\pi i}{p}})^{\mathrm{Tr}\, x}$, where Tr denotes the trace from $F$ to $\mathbb{Z}/p\mathbb{Z}$, and we write $G(\chi)$ for $G(\chi, \psi)$.

Let $\mu_N = e^{2\pi i/N}$ and, let $G_N = G(\mathbb{Q}(\mu_N)/\mathbb{Q})$, be identified with $(\mathbb{Z}/N\mathbb{Z})^x$ as usual. Let $\mathfrak{p}$ be a prime ideal of the ring of integers $\theta_N$ of $\mathbb{Q}(\mu_N)$ with residue field characteristic $p$ prime to $N$, and norm equal to $q$. Then we have the canonical multiplicative character $\chi_{\mathfrak{p},N}(x) = t(x^{q-1})^{/N})$. Here $t(y)$ denotes the unique lifting of the $N$–th root of unity $y$ to $\theta_N$. If a is in $\mathbb{Z}/N\mathbb{Z}$, define $J_N(a, \mathfrak{p})$ to be $G(\chi^a_{\mathfrak{p},N})$. We note that if $a = 0$, $J_N(a, \mathfrak{p}) = 1$.

Now let $k$ be an abelian extension of $Q$, and fix an embedding of $k$ into $\mathbb{C}$. Let $\{N_i\}$ for $i = 1, 2, \ldots, s$ be a collection of integers $\geq 2$, such that $k \subset \mathbb{Q}(\mu_{N_i})$ for all $i$. Let $\theta$ be a collection of maps

$$r_i : (\mathbb{Z}/N_i\mathbb{Z}) \to \mathbb{Z}. \text{ We write } \theta = \sum_i \sum_a r_i(a)[a]_{N_i}.$$

DEFINITION 1.1: We define the *infinity-type* $I(\theta)$ to be the element of the rational group-ring $\mathbb{Q}[G(k/\mathbb{Q})]$ given by

$$\sum_{\tau \in G(k/\mathbb{Q})} \sum_i \sum_a r_i(a) \sum_{b \in G_{N_i}} \left\langle -\frac{\tilde{a}\tilde{b}\tilde{\tau}}{N_i} \right\rangle \tau^{-1}.$$

Here $\tilde{\tau}$ is any lifting of $\tau$ to $G_{N_i}$, and then to $\mathbb{Z}$, $\tilde{a}$ and $\tilde{b}$ are any liftings of a and $b$ to $\mathbb{Z}$, and the definition is obviously independent of the choice of liftings.

PROPOSITION 1.2: *The following are equivalent:*

(i) $I(\theta)$ *is in* $\mathbb{Z}[G(k/\mathbb{Q})]$.

(ii) $\sum_i \sum_a r_i(a) \sum_{b \in G_{N_i}} \frac{ab}{N_i}$ *is integral.*

PROOF: It is clear that (i) $\Rightarrow$ (ii), since $\frac{-ab}{N_i} - \left\langle \frac{-\tilde{a}\tilde{b}}{N_i} \right\rangle \in \mathbb{Z}$, and (ii) $\Rightarrow$ (i) since $\sum_i \sum_a r_i(a) \sum_b \left\langle \frac{-\tilde{a}\tilde{b}\tilde{\tau}}{N_i} \right\rangle \equiv \tilde{\tau}\left( \sum_i \sum_a r_i(a) \left\langle \frac{-\tilde{a}\tilde{b}}{N_i} \right\rangle \right) \pmod{\mathbb{Z}}$.

DEFINITION 1.3: If $\theta$ satisfies the equivalent conditions of the above proposition, we say $\theta$ is of *Weil type.*

DEFINITION 1.4: We say that $\theta$ is of *Deligne type* if $I(\theta)$ is a multiple of the norm $\mathbb{N}$ in $\mathbb{Z}[G(k/\mathbb{Q})]$, and we define $n(\theta)$ by $I(0) = n(\theta)\mathbb{N}$.

Let $N = \prod_{i=1}^{s} N_i$ and let $S$ be the set of prime ideals of $k$ dividing $N$. Let $I_S$ be the group generated by the prime ideals $\mathfrak{p}$ of $k$ not in $S$. We define a function $J(\theta): I_S \to \mathbb{C}^x$

$$\text{by } J(\theta)(\mathfrak{p}) = \prod_{i=1}^{s} \prod_{a=1}^{N_i - 1} \prod_{\mathfrak{f} | \mathfrak{p}} J_{N_i}(a, \mathfrak{f})^{r_i(a)},$$

where the last product is taken over all $\mathfrak{f}$ in $\mathbb{Q}(\mu_{N_i})$ dividing $\mathfrak{p}$.

We wish to prove the following two theorems:

THEOREM 1.5 (Generalized Weil's Theorem): *If* $\theta$ *is of Weil type, then*

i) $J(\theta)$ *takes values in* $k$

ii) $J(\theta)$ *is a Hecke character with infinity-type* $I(\theta)$. *More precisely, there exists an integral ideal* $\mathfrak{f}$ *in* $k$ *such that if* $\alpha \equiv 1 \pmod{^x\ \mathfrak{f}}$, *then* $J(\theta)((\alpha)) = \alpha^{I(\theta)}$

iii) $\mathfrak{f}$ *divides some power of* $N$.

We remark that Weil proves this theorem in [2], for the case when $s = 1$ and all the $r_i(a)$'s are $\geq 0$, but the case when $s = 1$ and the $r_i(a)$'s are arbitrary is an immediate consequence.

Now define $\Gamma(\theta)$ to be

$$\prod_{i=1}^{s} \prod_{a \neq 0} \prod_{b \in G_{N_i}} \Gamma\left(\left\langle \frac{\tilde{a}\tilde{b}}{N_i} \right\rangle\right)^{r_i(a)},$$

and

$\Gamma^*(\theta)$ to be $\Gamma(\theta)(2\pi i)^{-n(\theta)}$.

THEOREM 1.6 (Generalized Deligne's Theorem): *If $\theta$ is of Deligne type, then*

(i) *$\Gamma^*(\theta)$ generates an abelian extension $K$ of $k$, which is Galois over $\mathbb{Q}$.*

(ii) *If we let $\chi(\theta) = J(\theta)\mathbb{N}^{-n(\theta)}$, then $\chi(\theta)$ is a character of $K/k$ and $\Gamma^*(\theta)$ transforms via $\chi(\theta)$ in the sense that if $\sigma$ is in $G(K/k)$, $\sigma\Gamma^*(\theta) = \chi(\sigma)\Gamma^*(\theta)$. If $s = 1$, then this becomes Deligne's Theorem* ([3], *p.* 339).

## §2. Some arithmetic lemmas

We start by fixing our terminology and notation. Let $p$ be a prime, let $f$ be a positive integer, and $q = p^f$. Given a in $\mathbb{Z}$ such that $0 \leq a < q$, write $a = \sum_{i=0}^{f-1} a_i p^i$, with $a_i \in \mathbb{Z}$ and $0 \leq a_i < p$. Let $\gamma(a) = \prod_{i=0}^{f-1} (a_i)!$, and let $s(a) = \sum_{i=0}^{f-1} a_i$. If $x$ *is in* $\mathbb{Z}_p$, let $r_q(x)$ be the unique integer such that $0 \leq r_q(x) < q$, and $r_q(x) \equiv x \pmod{q}$. If $l$ is prime, let $\left[\frac{y}{l}\right]$ denote the Legendre symbol modulo $l$.

LEMMA 2.1 (Gauss' Lemma): *If $l$ is an odd prime and $m$ is an integer prime to $l$, then $\left[\frac{m}{l}\right] = (-1)^\mu$, where $\mu$ is the number of members of the set $\{m, 2m, \ldots, \frac{1}{2}(l-1)m\}$ whose least positive residue* mod $l$ *is greater than $\frac{1}{2}l$.*

PROOF: By definition of $\mu$, we have

$$\prod_{j=1}^{(l-1)/2} (mj) = (-1)^\mu \prod_{j=1}^{(l-1)/2} j \pmod{l}.$$

So $\left[\frac{m}{l}\right] \equiv m^{(l-1)/2} \equiv (-1)^\mu \pmod{l}$, which implies $\left[\frac{m}{l}\right] = (-1)^\mu$.

LEMMA 2.2: *Let $l$ and $p$ be odd primes. Then*

$$(-1)^{\sum_{j=0}^{(l-1)/2} r_q(-j/l)} \equiv \left[\frac{q}{l}\right] \pmod{p}.$$

PROOF: Let $x = r_q(-j/l)$. We have $lx = yq - j$ for some $y \in \mathbb{Z}$. We see that $yq = lx + j$ and $0 \leq x < q$ together imply $0 \leq y \leq l$. Since $j < l$, $y < l$, so $0 \leq y \leq l - 1$. But $y \equiv jq^{-1} \pmod{l}$ implies that $y = r_l(j/q)$. So $(-1)^{\Sigma r_q(-j/l)} = (-1)^{l\Sigma r_q(-j/l)} = (-1)^{\Sigma(r_l(j/q)-j)}$, since $l$ and $q$ are both odd.

Now consider the set $\left\{r_l\left(\frac{j}{q}\right)\right\}$, for $j = 0, \ldots, (l-1)/2$. Since $x$ and $l - x$ cannot both occur in this set, exactly one must occur, and if we let $q^{-1} = m$ in Gauss' Lemma, $\mu$ becomes the number of times that $l - j$ occurs instead of $j$. Since $l$ is odd $(-1)^{\Sigma(r_l(j/q)-j)} = (-1)^{\mu} =$ (by Gauss' Lemma) $\left[\frac{q^{-1}}{l}\right] = \left[\frac{q}{l}\right]$.

LEMMA 2.3: *Let $\alpha$ be an integer, $0 < \alpha < p$. Then* $(\alpha!)(p - 1 - \alpha)! \equiv (-1)^{\alpha-1} \pmod{p}$.

PROOF: This follows immediately from Wilson's Theorem by induction.

LEMMA 2.4: *Let $l$ and $p$ be primes, and assume $l$ is odd. Then*

$$\prod_{j=0}^{l-1} \gamma(r_q(-j/l)) \equiv (-1)^{f\left(\frac{l-1}{2}\right)} \left[\frac{q}{l}\right] \pmod{p}.$$

PROOF: Since the lemma is obvious for $p = 2$, we may assume $p$ is odd. Let $x = \sum_{i=0}^{f} x_i p^i$ be an integer between 0 and $q - 1$ inclusive. Then $q - 1 - x = \sum(p - 1 - x_i)p^i$, and $\gamma(x)\gamma(q - 1 - x) = \prod(x_i)!(p - 1 - x_i)! \equiv (-1)^{f+\Sigma x_i}$, by Lemma 2.3. Also, $\sum x_i \equiv x \pmod{(p-1)}$, hence mod 2, so $\gamma(x)\gamma(q - 1 - x) \equiv (-1)^{f+x} \pmod{p}$. If we now let $y = -j/l$, and $x = r_q(y)$, then $q - 1 - x = r_q(-(l-j)/l)$,

hence $\prod_{j=0}^{l-1} \gamma(r_q(-j/l)) \equiv (-1)^{f\left(\frac{l-1}{2}\right)}(-1)^{\sum_{j=0}^{(l-1)/2} r_q(-j/l)}$

$\equiv (-1)^{f\left(\frac{l-1}{2}\right)} \left[\frac{q}{l}\right] \pmod{p}$ by Lemma 2.2.

PROPOSITION 2.5: *Let p be a prime, a an integer, and* $q = p^f$. *Let l be a positive integer prime to p. Let* $b(j,a)$ *be the unique integers such that* $0 \leq b(j,a) < q$, *and* $lb(j,a) \equiv a - j \pmod{q}$ *for* $j = 0, 1, \ldots, l-1$. Then

i) $f(a) = l^a(\prod_{j=0}^{l-1} \gamma(b(j,a)))/\gamma(a)$ *is independent of a* $\pmod{p}$.

ii) $g(a) = \sum_{j=0}^{l-1} s(b(j,a)) - s(a)$ *is independent of a.*

iii) *If p is prime and l is an odd prime, then*

$$f(a) \equiv (-1)^{f\left(\frac{l-1}{2}\right)} \begin{bmatrix} q \\ l \end{bmatrix} \pmod{p}.$$

PROOF: We will prove by induction on a that $f(a) \equiv f(0) \pmod{p}$ and $g(a) = g(0)$. This is clear if $a = 0$. Now suppose we know these relations for $a - 1$. Since the collections $\{b(j,a)\}$ and $\{b(j,a-1)\}$ agree except for their first and last elements, we must prove that $l\gamma(b(0,a))/\gamma(a) \equiv \gamma(b(l-1,a-1))/\gamma(a-1) \pmod{p}$ and $s(b(0,a)) - s(a) = s(b(l-1,a-1)) - s(a-1)$. These are immediately equivalent to: $l\gamma(b)/\gamma(b-1) \equiv \gamma(a)/\gamma(a-1) \pmod{p}$ and $s(b) - s(b-1) = s(a) - s(a-1)$, where $b = b(0,a)$.

Let $a' = a_j$ be the first non-zero coefficient in the $p$-adic expansion of $a$. Then by Wilson's theorem $\gamma(a)/\gamma(a-1) \equiv a'(-1)^j \pmod{p}$. If $b = \sum_{i=0}^{f-1} b_i p^i$ and if $b' = b_i$ is the first nonzero coefficient in the $p$-adic expansion of $b$, then we must have $i = j$ and $lb' \equiv a' \pmod{p}$, since $(l,p) = 1$ and $lb \equiv a \pmod{q}$. Since $\gamma(b)/\gamma(b-1) \equiv b'(-1)^j \pmod{p}$, (i) follows. Also, $s(a-1) - s(a) = j(p-1) - 1 = i(p-1) - 1 = s(b-1) - s(b)$, so (ii) follows.

To see (iii), we observe that $f(0) = \prod_{j=0}^{l-1} \gamma(b(j,0)) = \prod_{j=0}^{l-1} \gamma(r_q(-j/l))$, and use Lemma 2.4.

PROPOSITION 2.6: *Let l be an odd prime, p a prime different from l, and* $q = p^f$, *f an integer* $> 1$. *Then*

$$l^{\frac{1}{2}(q-1)}(-1)^{\left(\frac{l-1}{2}\right)\left(\frac{q-1}{2}\right)} \equiv \begin{bmatrix} q \\ l \end{bmatrix} \pmod{p}.$$

PROOF:

$$l^{\frac{1}{2}(q-1)} = (l^{\frac{1}{2}(p-1)})^{\frac{(q-1)}{(p-1)}} \equiv \begin{bmatrix} l \\ p \end{bmatrix}^{(q-1)/(p-1)}$$

$$= \left(\begin{bmatrix} p \\ l \end{bmatrix} (-1)^{\left(\frac{p-1}{2}\right)\left(\frac{l-1}{2}\right)}\right)^{(q-1)/(p-1)}$$

by quadratic reciprocity. This in turn equals $\begin{bmatrix} p \\ l \end{bmatrix}^f (-1)^{\left(\frac{q-1}{p-1}\right)\left(\frac{p-1}{2}\right)\left(\frac{l-1}{2}\right)}$ (since $(q-1)/(p-1) \equiv f \pmod 2$) which obviously is the same as

$$\begin{bmatrix} q \\ l \end{bmatrix}(-1)^{\left(\frac{l-1}{2}\right)\left(\frac{q-1}{2}\right)}.$$

PROPOSITION 2.7: *Let $\pi = \zeta - 1$, where p is a prime and $\zeta$ is a primitive p-th root of unity. Then $p/\pi^{p-1} \equiv (-1) (\operatorname{mod} \pi)$.*

PROOF: We may assume $p$ is odd. We know that $\mathbb{N}\pi = p$, where $\mathbb{N}$ is the norm from $\mathbb{Q}(\zeta)$ to $\mathbb{Q}$. $\mathbb{N}\pi = \prod_{\sigma \in (\mathbb{Z}/p\mathbb{Z})^\times}(\sigma\pi)$, so $p/\pi^{p-1} = \prod_\sigma (\pi^\sigma/\pi)$. But if $\sigma = \sigma_b$, then $\pi^\sigma = 1 - \zeta^b$ and $\pi^\sigma/\pi = (1 - \zeta^b)/(1 - \zeta) = 1 + \zeta + \ldots + \zeta^{b-1} \equiv b \pmod{\pi}$, since $\zeta \equiv 1 \pmod{\pi}$. The result then follows immediately from Wilson's Theorem.

PROPOSITION 2.8: *Let p be a prime and l be an odd prime, M an integer $> 1$, and assume that $(p, M) = (l, M) = 1$. Set $N = lM$. Let q be minimal such that q is a power of p and M divides $q - 1$. Let g be minimal such that N divides $q^g - 1$. Assume $g > 1$. Let $0 \leq a < N$ and let $0 \leq b < N$ be such that $b \equiv 0 \pmod{l}$ and $b \equiv a \pmod{M}$. Then $l\langle b(q^g - 1)/N\rangle_q \equiv a(q-1)/M \pmod{(q-1)}$.*

PROOF: We know that $b$ is the unique integer $\leq 0$ and $< N$ such that $b \equiv 0 \pmod{l}$ and $b \equiv a \pmod{M}$. Let $x$ be such that $0 \leq x < q - 1$ and $lx \equiv a(q-1)/M \pmod{(q-1)}$. Then $x$ is unique since $l \nmid q - 1$ by assumption. Then $lx = b'(q-1)/M$ with $0 \leq b' < N$. Thus $b'(q-1) \equiv 0 \pmod{l}$ which implies $b' \equiv 0 \pmod{l}$ which implies that $b' = b$ since $b' \equiv a \pmod{M}$. Then $x \equiv b(q^g - 1)/N \pmod{q}$ so $x = \langle b(q^g - 1)/N\rangle_q$ which proves the proposition.

PROPOSITION 2.9: (*Gauss multiplication formula*)

$$(2\pi)^{(n-1)/2}\Gamma(z) = n^{z-1/2}\Gamma\left(\frac{z}{n}\right)\Gamma\left(\frac{z+1}{n}\right)\ldots\Gamma\left(\frac{z+n-1}{n}\right).$$

PROOF: See ([8], p. 162).

Let $F$ be a finite field, $\chi$ a character of $F^\times$ of order $l$, $\psi$ a character of $F^\times$. Then:

PROPOSITION 2.10: (*Hasse–Davenport distribution formula*)

$$\prod_{i=0}^{l-1} G(\chi^i\psi) = \psi^{-1}(l^l)G(\psi^l)\prod_{j=0}^{l-1} G(\chi^j).$$

PROOF: This is essentially $(0.9_1)$ of Hasse–Davenport ([6], p. 172).

COROLLARY 2.11: *Let* $k = \mathbb{Q}(\mu_N)$ *and* $l|N$, $M = N/l > 1$. *Then, in the notation of* 1, *if* $\mathfrak{p}$ *is a prime of* $k$ *prime to* $N$, *we have:*

$$\prod_{i=0}^{l-1} J_N(a+iM,\mathfrak{p}) = \chi_{\mathfrak{p},N}(l)^{-la}J_N(la,\mathfrak{p})\prod_{j=0}^{l-1} J_N(iM,\mathfrak{p}).$$

PROOF: This follows immediately from Proposition 2.10, with $\chi = \chi_{\mathfrak{p},N}^M$ and $\psi = \chi_{\mathfrak{p},N}^a$.

Let $E$ be a finite extension of $F$ of degree $r$, and let $\chi_E$ be the character of $E^x$ defined by $\chi_E = \chi\circ\mathbb{N}_{E/F}$. Then we have

PROPOSITION 2.12: (*Hasse–Davenport theorem*)

$$G(\chi_E) = G(\chi)^r.$$

PROOF: This is (0.8) of Hasse–Davenport ([6], p. 172).

PROPOSITION 2.13: (*Stickelberger's Theorem*) *Let* $F = \mathbb{Q}(\mu_M) \subset \mathbb{C}$ *and let* $\mathfrak{p}$ *be a prime ideal of* $\theta_F$ *of characteristic* $p$ *prime to* $M$. *Let* $q = \mathbb{N}\mathfrak{p}$, $k(\mathfrak{p})$ *be the residue field at* $\mathfrak{p}$, *and let* $t$ *be the natural lifting from the* $M$*-th roots of unity in* $k(\mathfrak{p})$ *to* $M$*-th roots of unity in* $F$. *Given* $a$ *in* $\mathbb{Z}/M\mathbb{Z}$, *let* $\chi_a$ *be the complex-valued character of* $k(\mathfrak{p})$ *defined by* $\chi_a(x) = t(x^{-a(\frac{q-1}{M})})$. *Let* $\psi$ *be the additive character of* $k(\mathfrak{p})$ *defined by* $\psi(x) = e^{\frac{2\pi i\,Tr(x)}{p}}$, *and let* $G(\chi_a)$ *be the (modified) Gauss sum* $-\sum_x \chi_a(x)\psi(x)$. *Let* $\mathfrak{f}$ *be the unique prime lying over* $\mathfrak{p}$ *in* $\mathbb{Q}(\mu_{pM})$. *Let* $a_M = \dfrac{\langle a\rangle_M(q-1)}{M}$, *where* $\langle a\rangle_M$ *is the residue of* $a$ mod $M$. *Then*

$$\frac{G(\chi_a)}{(\zeta_p - 1)^{s(a_M)}} \equiv \frac{1}{\gamma(a_M)} \pmod{\mathfrak{f}},$$

*where* $\zeta_p = e^{2\pi i/p}$.

PROOF: See ([9], p. 94).

## §3. Proof of the generalized Weil and Deligne theorems in special cases

PROPOSITION 3.1: *If* $\theta = \sum_i \sum_a r_i(a)[a]_{N_i}$ *is of Weil type, then* $J(\theta)$ *takes values in* $k$.

PROOF: It clearly suffices to prove that $J(\theta)(\mathfrak{p})$ belongs to $k$ where $\mathfrak{p}$ is prime. The first point to note is that $J_N(a, \mathfrak{p})$ belongs to $k(\mu_p)$. This follows from the fact that $J_N(a, \mathfrak{p})$ is the product $J_N(a, \mathfrak{p}_i)$ over $\mathfrak{p}_i | \mathfrak{p}$ in $\mathbb{Q}(\mu_N)$. We know that each $J_N(a, \mathfrak{p}_i)$ is in $\mathbb{Q}(\mu_{pN})$ and, if $\sigma = \sigma_b \in G(\mathbb{Q}(\mu_N)/\mathbb{Q})$, $J_N(a, \mathfrak{p}_i)^\sigma = J_N(ab, \mathfrak{p}_i) = J_N(a, \mathfrak{p}_i^\sigma)$.

Next we determine the action of $(\mathbb{Z}/p\mathbb{Z})^\times$ on $J(\theta)(\mathfrak{p})$. We have for $c \in (\mathbb{Z}/p\mathbb{Z})^\times$ and $\tau = \tau_c$, $J_N(a, \mathfrak{p})^\tau = t(c^{-a\left(\frac{q-1}{N}\right)} J_N(a, \mathfrak{p}))$. It follows immediately that $(J(\theta)(\mathfrak{p}))^\tau = t(c^{-r}) J(\theta)(\mathfrak{p})$, where $r \in \mathbb{Z}/(p-1)\mathbb{Z}$ equals $\sum_i \sum_a r_i(a) \sum_{G_i/D_i} b\left(\frac{q_i - 1}{N_i}\right)$, where $D_i$ is the decomposition group of a prime $\mathfrak{p}_i$ in $\mathbb{Q}(\mu_{N_i})$ lying over $\mathfrak{p}$, $q_i$ is the norm of $\mathfrak{p}_i$ and $b$ runs through $G_i/D_i$. Now

$$r = \sum_i \sum_a r_i(a) \sum_{G_i/D_i} \left((q_i - 1)/(q-1) \frac{ab}{N_i}\right)(q-1)$$

$$= \sum_i \sum_a r_i(a) \sum_{G_i} \frac{ac}{N_i}(q-1),$$

where $c$ now runs through $G_i$. (Note that

$$\sum_{G_i} c = \sum_{b \in G_i/D_i} \sum_{c \to b} c = \sum_{b \in G_i/D_i} \sum_{j=0}^{f-1} bq^j = \sum_b b\left(\frac{q^f - 1}{q-1}\right) = \sum_b b\left(\frac{q_i - 1}{q-1}\right)\Bigg).$$

But by definition of Weil type, $r$ is an integer divisible by $(q-1)$, hence by $(p-1)$. Thus $c^{-r} = 1$, which completes the proof.

LEMMA 3.2: *Let* $\theta$ *be of Deligne type. Then*

i) $n(\theta) = \frac{1}{2} \sum_i \sum_{a \neq 0} r_i(a) \# G_{N_i}$

ii) $\chi(\theta) = J(\theta)\mathbb{N}^{-n(\theta)}$ *takes values in roots of unity in* $k$ *on ideals* $\mathfrak{a}$ *prime to* $\prod N_i$.

PROOF: (i) We have $n(\theta) = \sum_i \sum_a r_i(a) \sum_b \left\langle \frac{-\tilde{a}\tilde{b}\tilde{\tau}_i}{N_i} \right\rangle$, for any $\tau \in G(k/Q)$. Summing over $\tau$, we have:

$$\# G(k/\mathbb{Q})n(\theta) = \sum_i \sum_a r_i(a) \sum_b \sum_\tau \left\langle \frac{-\tilde{a}\tilde{b}\tilde{\tau}_i}{N_i} \right\rangle.$$

Since we may choose $\tilde{\tau}_i$ so that both $\tilde{\tau}_i$ and $N_i - \tilde{\tau}_i$ are in the set of $\tilde{\tau}$'s, and $\left\langle \frac{-\tilde{a}\tilde{b}\tilde{\tau}_i}{N_i} \right\rangle + \left\langle \frac{-\tilde{a}b(N_i - \tilde{\tau}_i)}{N_i} \right\rangle$ is equal to 1 unless $a = 0$, we obtain:

$$\# G(k/\mathbb{Q})n(\theta) = \tfrac{1}{2} \sum_i \sum_a r_i(a) \# G_{N_i} \# G(k/Q),$$

which gives (i).

(ii): We know by Proposition 3.1 that $\chi(\theta)$ takes values in $k$. We may clearly assume that $\mathfrak{a}$ is a prime ideal $\mathfrak{p}$ not dividing $\prod N_i$, and that $r_i(0) = 0$, for all $i$. By Stickelberger's theorem (Proposition 2.13) we have $(J(\theta)(\mathfrak{p})) = \mathfrak{p}^{S(\theta)}$, where $S(\theta) = \sum_i \sum_a r_i(a) \sum_{b \in G_{N_i}} \left\langle \frac{-\tilde{a}\tilde{b}\tilde{\tau}_i}{N_i} \right\rangle \tau^{-1}$. We wish to show first that $\chi(\theta)(\mathfrak{p})$ is a unit. Clearly the only primes which divide $J(\theta)(\mathfrak{p})$ are the conjugates of $\mathfrak{p}$. Also the exponent of $\tau^{-1}\mathfrak{p}$ in $J(\theta)(\mathfrak{p})$ is given by $\sum_i \sum_a r_i(a) \sum_{b \in G_{N_i}} \left\langle \frac{-\tilde{a}\tilde{b}\tilde{\tau}_i}{N_i} \right\rangle \# D_p$, where $D_p$ is the decomposition group of $p$. By definition of Deligne type, this is $n(\theta) \# D_p$. Since $p$ is unramified in $k$, the norm of $\tau^{-1}\mathfrak{p}$ is $p^{\# D_p}$, so $\chi(\theta)(\mathfrak{p}) = J(\theta)(\mathfrak{p})\mathbb{N}^{-n(\theta)}(\mathfrak{p})$ is a unit at $\tau^{-1}\mathfrak{p}$ and hence a unit.

Since the absolute value of a Gauss sum over a finite field with $q$ elements is $q^{1/2}$, we compute $|J(\theta)(\mathfrak{p})| = \prod_i \prod_a (\mathbb{N}\mathfrak{p})^{\frac{1}{2} \# G_{N_i} r_i(a)}$, or $(\mathbb{N}\mathfrak{p})^{n(\theta)}$, (by part (i)) for any absolute value. Hence $|\chi(\theta)(\mathfrak{p})| = 1$ for any absolute value, and $\chi(\theta)(\mathfrak{p})$ is a root of unity by the Dirichlet unit theorem.

PROPOSITION 3.3: *Let $\theta$ be of Deligne type. Assume that:*

i) *$K = k(\Gamma^*(\theta))$ is an abelian extension of $k$.*

ii) *$\Gamma^*(\theta)^{w(k)} \in k$, where $w(k)$ is the number of roots of unity in $k$.*

iii) *$k(\Gamma^*(\theta))/k$ is unramified at every finite prime not dividing $N = \prod N_i$.*

iv) *For all $\mathfrak{p}$ prime to $N$, $\chi(\theta)(\mathfrak{p}) \equiv (\Gamma^*(\theta))^{q-1} \pmod{\mathfrak{f}}$, where $q = \mathbb{N}\mathfrak{p}$ and $\mathfrak{f}$ is any prime dividing $\mathfrak{p}$ in $K$. Then the generalized Weil and Deligne theorems are true for $\theta$; that is, $J(\theta)$ is a Hecke character with values in $k$, $\chi(\theta)$ is a character of finite order, and $\chi(\theta)(\mathfrak{p})(\Gamma^*(\theta)) = \sigma_\mathfrak{p}\Gamma^*(\theta)$ for all $\mathfrak{p}$ prime to $N$. (Moreover, $\chi(\theta)$ is unramified outside of $N$, so the finite part of the conductor of $J(\theta)$ divides a power of $N$.)*

PROOF: First assume $q$ is odd. Let $\sigma_\mathfrak{p}$ be the Frobenius at $\mathfrak{p}$ for the extension $K/k$, so by definition $\sigma_\mathfrak{p}\Gamma^*(\theta) \equiv \Gamma^*(\theta)^q$ (mod $\mathfrak{f}$) for any $\mathfrak{f}$ lying over $\mathfrak{p}$. Since $q > 1$ and $\Gamma^*(\theta)^{q-1}$ is congruent to a unit mod $\mathfrak{p}$, $\Gamma^*(\theta)$ is a unit at $\mathfrak{f}$. Since $\Gamma^*(\theta)^{w(k)}$ lies in $k$, $\sigma_{\mathfrak{p}}\Gamma^*(\theta)/\Gamma^*(\theta)$ is a root of unity of order prime to $\mathfrak{p}$, lying in $k$. Now $\sigma_{\mathfrak{p}}\Gamma^*(\theta)/\Gamma^*(\theta) \equiv (\Gamma^*(\theta))^{q-1}$ (mod $\mathfrak{f}$). So $\chi(\theta)(\mathfrak{p}) \equiv \sigma_{\mathfrak{p}}\Gamma^*(\theta)/\Gamma^*(\theta)$ (mod $\mathfrak{f}$) and since these are both roots of unity of order prime to $\mathfrak{p}$, we obtain $\chi(\theta)(\mathfrak{p})\Gamma^*(\theta) = \sigma_{\mathfrak{p}}\Gamma^*(\theta)$.

Now consider the case when $\mathfrak{p}$ divides 2. Since $\mathfrak{p}$ is prime to $N$, $N$ is odd. Then $w(k)$ only divides $2N$, and not necessarily $N$, so we can only conclude that $\chi(\theta)(\mathfrak{p})(\Gamma^*(\theta)) = \pm\sigma_{\mathfrak{p}}\Gamma^*(\theta)$, or that $\chi(\theta)(\mathfrak{p}) = \pm(\Gamma^*(\theta)\sigma^{\mathfrak{p}-1})$.

On the other hand, by Weil's theorem in the case of unmixed level $N$, $\mathfrak{p} \mapsto \chi^N(\theta)(\mathfrak{p})$ defines a Hecke character for all $\mathfrak{p}$ prime to $N$, as does $\mathfrak{p} \mapsto (\Gamma^*(\theta))^{N(\sigma\mathfrak{p}-1)}$ by class field theory. Since these are both Dirichlet characters which agree on all primes not dividing $2N$, they must also agree on $\mathfrak{p}$, so $\chi^N(\theta)(\mathfrak{p}) = (\Gamma^*(\theta)^{(\sigma\mathfrak{p}-1)})^N$. Since $N$ is odd, we conclude that $\chi(\theta)(\mathfrak{p}) = \Gamma^*(\theta)^{\sigma\mathfrak{p}-1}$ rather than $-\Gamma^*(\theta)^{\sigma\mathfrak{p}-1}$.

Clearly $\chi(\theta)(\mathfrak{p}) = 1$ if $\sigma_{\mathfrak{p}} = 1$ on $K$, hence $\chi(\theta)$ is a Dirichlet character of $K/k$ and $J(\theta) = \chi(\theta)\mathbb{N}^{n(\theta)}$ is a Hecke character. Since $K/k$ is unramified outside of $N$, the rest of the proposition follows.

It also follows readily that $K$ is Galois over $\mathbb{Q}$: We have already remarked in the first paragraph of the proof of Proposition 3.1 that $J(\theta)$ is Galois-equivariant, i.e., that $J(\theta)(\mathfrak{p}^\sigma) = \sigma(J(\theta)(\mathfrak{p}))$. Since $\mathbb{N}$ is Galois-equivariant, so is $\chi$. If we then, for any $\tau$ in $G(\bar{\mathbb{Q}}/\mathbb{Q})$ define $\chi^\tau$ by $\chi^\tau(\sigma) = \tau(\chi(\tau\sigma\tau^{-1}))$, it is a series of straightforward computations, using only the formal properties of the Artin symbol, to verify first, that if $\chi$ is Galois equivariant $\chi = \chi^\tau$, second, that if $G = \operatorname{Ker}\chi$, the kernel of $\chi^\tau$ is $G^\tau = \{\tau^{-1}\sigma\tau : \sigma \in G\}$, and third, that the fixed field of $G^\tau$ is $K^{\tau^{-1}}$. These three facts immediately yield that $K$ is Galois over $\mathbb{Q}$.

THEOREM 3.4: *Let $N = lM$, with $l$ prime. Let $a$ be any element of $\mathbb{Z}/N\mathbb{Z}$. Then the generalized Weil and Deligne theorems are true for the following $\theta$'s, and $k = \mathbb{Q}(\mu_M)$. Also, the conductor of $J(\theta)$ divides a power of $N$.*

1) $l = 2$, *$M$ odd, $a$ even:* $\theta = [a]_N - [a/2]_M$
2) $l = 2$, *$M$ even, $a$ even:* $\theta = [a]_N - 2[a/2]_M$
3) *$l$ is odd,* $l|M, l|a : \theta = [a]_N - l[a/l]_M$
4) *$l$ is odd,* $l \nmid M$, $l|a : \theta = [a]_N + (1-l)[a/l]_M$
5) $l = 2$, *$M$ odd, $a$ odd*$: \theta = [a]_N - [M]_N - [a]_M + [2^{-1}a]_M$
6) $l = 2$, *even, $a$ odd*$: \theta = [a]_N - [M/2]_M - [a]_M$
7) *$l$ odd,* $l|M$, $l \nmid a : \theta = [a]_N - [a]_M$
8) *$l$ odd,* $l \nmid M$, $l \nmid a : \theta = [a]_N - [a]_M + [l^{-1}a]_M$
9) $l = 2$, *$M$ odd*$: \theta = 2[M]_N$.

PROOF: We check immediately that all of these $\theta$'s are of Deligne type, with $n(\theta) = 0$ in Cases 1–6, $\left(\frac{l-1}{2}\right)$ in Cases 7) and 8), and [1] in Case 9.

Case 1): Since $J_N(a, \mathfrak{p}) = J_M(a/2, \mathfrak{p})$ for all $\mathfrak{p}$ prime in $k$, we obviously have $J(\theta) = 1$. Clearly $\Gamma^*(\theta) = 1$ also, and the Weil and Deligne theorems are immediate.

Case 2): Let $\mathfrak{q}$ be a prime in $\mathbb{Q}(\mu_M)$. Suppose that $\mathfrak{q}$ splits in $\mathbb{Q}(\mu_N)$ into $\mathfrak{q}_1\mathfrak{q}_2$. Then $J_N(a, \mathfrak{q}_1) = J_N(a, \mathfrak{q}_2) = J_M(a/2, \mathfrak{q})$, so $J(\theta) = 1$. If $\mathfrak{q}^1 = \mathfrak{q} \circ N$ is prime, then by the Hasse–Davenport Theorem (Proposition 2.12), we have $J_N(a, \mathfrak{q}^1) = J_M(a/2, \mathfrak{q})^2$, so again $J(\theta) = 1$. An immediate computation also shows that $\Gamma^*(\theta) = 1$ in $\mathbb{R}^x/\mathbb{Q}^x$.

Case 3): The argument here, using the Hasse–Davenport theorem, is identical to that just used in Case 2).

Case 4): Let $\mathfrak{q}$ be a prime in $\mathbb{Q}(\mu_M)$ which is unramified in $\mathbb{Q}(\mu^N)$. Let $\mathfrak{q}^1$ be a prime in $\mathbb{Q}(\mu_N)$ lying above $\mathfrak{q}$ and $D$ the decomposition group of $\mathfrak{q}^1$. Let $f = \# D$, so that $\mathbb{N}(\mathfrak{q}^1) = \mathbb{N}(\mathfrak{q})^f$. Then $J_N(a, \mathfrak{q}, k)$ = (by Hasse–Davenport) $J_M(a/l, \mathfrak{q}, k)^{l-1}$, since $l - 1 = [\mathbb{Q}(\mu_N) : \mathbb{Q}(\mu_M)]$ and $\frac{ab}{N} \equiv \frac{a}{N}$ (mod $\mathbb{Z}$) for $b \in G(\mathbb{Q}(\mu_N)/\mathbb{Q}(\mu_M))$. It follows that $J(\theta) = 1$. A simple calculation also shows that $\Gamma^*(\theta) = 1$ in $\mathbb{R}^x/\mathbb{Q}^x$.

Case 5): Let $\mathfrak{q}$ be a prime ideal of $k$, prime to $N$, and let $2b \equiv a$ (mod $M$). Then $J(\theta)(\mathfrak{q}) = J_N(a, \mathfrak{q})J_M(b, \mathfrak{q})/J_M(a, \mathfrak{q})J_N(M, \mathfrak{q})$. But $J_M(a, \mathfrak{q}) = J_N(2a, \mathfrak{q})$, and $J_M(b, \mathfrak{q}) = J_N(a + M, \mathfrak{q})$. So applying the Hasse–Davenport distribution formula (Proposition 2.11) we obtain $J(\theta)(\mathfrak{q}) = \chi_{\mathfrak{q},N}(2)^{-2a} = \chi_{\mathfrak{q},M}(2)^{-a}$.

We have $\Gamma(\theta) = \Gamma(a/N)\Gamma(a + M/N)/\Gamma(a/M)\Gamma(1/2)$, which is equal by the Gauss multiplication formula (Proposition 2.9) to $2^{\frac{1}{2} - a/M}\sqrt{2\pi}/\sqrt{\pi} = 2^{1 - a/M}$. Since $\Gamma^*(\theta) = \Gamma(\theta)$, we clearly have that $\Gamma^*(\theta)$ generates an abelian extension $K$ of $k$, unramified outside $N$, and $\Gamma^*(\theta)^M \in k$. Applying Proposition 3.3, we need only prove that $J(\theta)(\mathfrak{q}) \equiv \Gamma(\theta)^{q-1}$ (mod $\mathfrak{q}^1$) where $\mathfrak{q}^1$ is a prime lying above $\mathfrak{q}$ in $K$. This amounts to showing that $\chi_{\mathfrak{q},M}(2)^{-a} \equiv 2^{-a(q-1)/M}$ (mod $\mathfrak{q}^1$), which is immediate from the definition of $\chi_{\mathfrak{q},M}$.

Case 6): Again let $\mathfrak{q}$ be a prime ideal in $k$, and $\mathbb{N}\mathfrak{q} = q = p^f$. We first consider the case when $\mathfrak{q}$ splits in $\mathbb{Q}(\mu_N)$. Recalling that in this case $\theta = [a]_N - [M/2]_M - [a]_M$, we have $J(\theta)(\mathfrak{q}) = J_N(a, \mathfrak{q}^1)J_N(a + N, \mathfrak{q}^1)/J_M(M/2, \mathfrak{q})J_M(a, \mathfrak{q})$, where $\mathfrak{q}^1$ is either prime lying above $\mathfrak{q}$. But $J_M(M/2, \mathfrak{q}) = J_N(M, \mathfrak{q}^1)$ and $J_M(a, \mathfrak{q}) = J_N(2a, \mathfrak{q}^1)$, so $J(\theta)(\mathfrak{q}) = J_N(a, \mathfrak{q}^1)J_N(a + N, \mathfrak{q}^1)/J_N(M, \mathfrak{q}^1)J_N(2a, \mathfrak{q}^1)$. Applying the Hasse–Davenport distribution formula, we obtain $J(\theta)(\mathfrak{q}) = \chi_{\mathfrak{q}^1,N}(2)^{-2a} = \chi_{\mathfrak{q},M}(2)^{-a}$.

Now suppose that $\mathfrak{q}$ remains prime in $\mathbb{Q}(\mu_N)$. Let $\mathfrak{q}^1$ be the unique prime of $\mathbb{Q}(\mu_{Np})$ lying above q. By Stickelberger's Theorem (Proposition 2.13), and replacing $a$ by $-a$, we have

$$J(\theta)(\mathfrak{q}) \equiv \pi^{S_N(a)}\gamma_M(a)\gamma_M(M/2)/\pi^{S_M(a)}\pi^{S_M(M/2)}\gamma_N(a) \pmod{\mathfrak{q}^1}$$

where $\pi = \mu_p - 1$.

We first claim that $S_N(a) = S_M(a) + S_M(M/2)$. By definition:

i) $S_N(a) = \sum_{i=0}^{2f-1} a_i(N)$, where

$$\langle a\rangle_N\left(\frac{q^2-1}{N}\right) = \sum_{i=0}^{2f-1} a_i(N)p^i.$$

ii) $S_M(a) = \sum_{i=0}^{f-1} a_i(M)$, where

$$\langle a\rangle_M\left(\frac{q-1}{M}\right) = \sum_{i=0}^{f-1} a_i(M)p^i.$$

iii) $S_M(M/2) = \sum_{i=0}^{(f-1)} \frac{(p-1)}{2} = f\left(\frac{p-1}{2}\right)$. Let $a' = \langle a\rangle_N(q^2-1)/N$ and $a'' = \langle a+M\rangle_N(q^2-1)/N$. Either $\langle a\rangle_N = \langle a\rangle_M$ or $\langle a\rangle_N = \langle a\rangle_M + M$. In the first case

$$2a' \equiv -\langle a\rangle_N/M \equiv -\langle a\rangle_M/M \equiv \langle a\rangle_M(q-1)/M \pmod{q}.$$

In the second case

$$2a'' \equiv -\langle a+M\rangle_N/M \equiv -\langle a\rangle_M/M \equiv \langle a\rangle_M(q-1)/M \pmod{q}.$$

In this paragraph we will show that the last $f$ digits of $a'$ are the same as the first $f$ digits of $a''$. These last $f$ digits of $a'$ are the first $f$ digits of $\langle a'q\rangle_{q^2-1}$. Now $a'' = a' \pm (q^2-1)/2$, so $a'' \equiv a' + \left(\frac{q^2-1}{2}\right)$ (mod $(q^2-1)$). On the other hand, $a'q = a' + a'(q-1)$, while $a'(q-1) = \frac{\langle a\rangle_N(q-1)}{M}\left(\frac{q^2-1}{2}\right) \equiv \left(\frac{q^2-1}{2}\right)$ (mod $q^2-1$) since $\frac{\langle a\rangle_N(q-1)}{M}$ is odd because q remains prime in $\mathbb{Q}(\mu_N)$. So $a'' \equiv a'q$ mod $(q^2-1)$, and $\langle a''\rangle_{q^2-1} = \langle a'q\rangle_{q^2-1}$. But since $a'' < q^2-1$, $a'' = \langle a''\rangle_{q^2-1}$, and we are done.

So the collection $\{a_i(N)\}$ consists of the digits of $\langle a'\rangle_q$ and of $\langle a''\rangle_q$. Since $a'' = a' \pm (q^2-1)/2$, $2a'' \equiv 2a' \mp 1 \pmod{q}$. If $\langle a\rangle_N = \langle a\rangle_M$, $2a' \equiv \langle a\rangle_M(q-1)/M \pmod{q}$ and $2a'' \equiv 2a' - 1 \pmod{q}$ so the set

$\{\langle a'\rangle_q, \langle a''\rangle_q\}$ consists of $b_0$ and $b_1$ where $2b_0 \equiv \langle a\rangle_M(q-1)/M \pmod q$ and $2b_1 \equiv (\langle a\rangle_M(q-1)/M - 1) \pmod q$. Similarly, the same holds if $\langle a\rangle_N = \langle a\rangle_M + M$.

We are now in a position to apply Proposition 2.5, with $l = 2$ and $a$ replaced by $\langle a\rangle_M(q-1)/M$. Part ii) of this proposition then shows that

$$s(b_0) + s(b_1) - s(\langle a\rangle_M(q-1)/M) = s(-1/2).$$

But $s_N(a) = s(\langle a'\rangle_q) + s(\langle a''\rangle_q) = s(b_0) + s(b_1)$. So $s_N(a) - s_M(a) = = s(-1/2) = s\left(\frac{q-1}{2}\right) = f\left(\frac{p-1}{2}\right)$, and we have proved our original claim.

It now follows that

$$J(\theta)(\mathfrak{q}) \equiv \gamma_M(a)\gamma_M(M/2)/\gamma_N(a) \pmod{\mathfrak{q}'},$$

and hence mod $\mathfrak{q}$, since both sides are in $k$.

The above argument also shows that $\gamma(b_0)\gamma(b_1) = \gamma_N(a)$. From the first part of Proposition 2.5 we obtain

$$2^c\gamma(b_0)\gamma(b_1)/\gamma(c) = \gamma(-1/2);$$

where $c = \langle a\rangle_M\left(\frac{q-1}{M}\right)$. Since $\gamma_M(M/2) = \gamma(q-1)/2 = \gamma(-1/2)$, we conclude that $J(\theta)(\mathfrak{q}) \equiv 2^{\langle a\rangle_M(q-1)/M} \pmod{\mathfrak{q}}$. Switching a back to $-a$, we obtain

$$J(\theta)(\mathfrak{q}) \equiv 2^{-\langle a\rangle_M(q-1)/M} \pmod{\mathfrak{q}}.$$

We now compute $\Gamma(\theta)$. By definition, this is $(\Gamma(a/N)\Gamma(a+M)/N)/(\Gamma(a/M)\Gamma(\frac{1}{2}))$, which is equal by the Gauss multiplication formula to $2^{\frac{1}{2}-aM}(2\pi)^{1/2}/\pi^{1/2} = 2^{1-a/M}$. Since $n(\theta) = 0$, we have $\chi(\theta) = \mathrm{J}(\theta)$ and $\Gamma^*(\theta) = \Gamma(\theta)$. But since $2^{q-1} \equiv 1 \pmod{\mathfrak{q}}$, we have $\chi(\theta) \equiv \Gamma(\theta)^{q-1} \pmod{\mathfrak{q}}$, and, arguing as in Case 5), the hypotheses of Proposition 3.3 are satisfied and the Weil and Deligne theorems are true for $\theta$, with $J(\theta) = = \chi(\theta)$ so $J(\theta)(\mathfrak{q}) = \chi_{\mathfrak{q},M}(2)^{-a}$.

Case 7): Again $\mathfrak{q}$ is a prime ideal in $k$, and $\mathbb{N}\mathfrak{q} = q = p^f$. We have $\theta = [a]_N - [a]_M$, so $J(\theta)(\mathfrak{q}) = J_N(a, \mathfrak{q})/J_M(a, \mathfrak{q})$. We compute $J(\theta)(\mathfrak{q})$ first in the case when $\mathfrak{q}$ splits completely in $\mathbb{Q}(\mu_N)$. Then $J(\theta)(\mathfrak{q}) = = \prod_{i=0}^{l-1} J_N(a + iM, \mathfrak{q}')/J_N(la, \mathfrak{q}')$, where $\mathfrak{q}'$ is any prime lying over $\mathfrak{q}$ in $\mathbb{Q}(\mu_N)$. Using the Hasse–Davenport distribution formula, we see that

$J(\theta)(\mathfrak{q}) = \prod_{i=0}^{l-1} J_N(iM, \mathfrak{q}')\chi_{\mathfrak{q}',N}(l)^{-la}$. Since $n(\theta) = \dfrac{l-1}{2}$, $\chi(\theta) = J(\theta)\mathbb{N}^{-\left(\frac{l-1}{2}\right)}$. But now $J_N(iM, \mathfrak{q}')J_N(-iM, \mathfrak{q}') = \chi_{\mathfrak{q}',N}(-1)^{iM} \cdot \mathbb{N}\mathfrak{q}$, and $\chi_{\mathfrak{q}',N}(-1)^{iM} = (-1)^{i\left(\frac{q-1}{l}\right)} = 1$ since $q-1$ is even and $l$ is odd. So $\prod_{i=0}^{l-1} J_N(iM, \mathfrak{q}') = (\mathbb{N}\mathfrak{q})^{(l-1)/2}$, and

$$\chi(\theta)(\mathfrak{q}) = \chi_{\mathfrak{q}',N}(l)^{-la} = \chi_{\mathfrak{q},M}(l)^{-a}.$$

Now consider the case when $\mathfrak{q}$ does not split in $\mathbb{Q}(\mu_N)$. $\pi = e^{2\pi i/p} - 1$, and $\mathfrak{q}^1$ be a prime lying over $\mathfrak{q}$ in $\mathbb{Q}(\mu_{Np})$. Replacing $a$ by $-a$, and using Stickelberger's theorem, we obtain

$$J(\theta)(\mathfrak{q})\pi^{S_M(a) - S_N(a)} \equiv \gamma_M(a)/\gamma_N(a) \pmod{\mathfrak{q}^1}$$

We proceed as in Case 6). Let $a_N = \langle a \rangle_N(q^l - 1)/N$ and $a_M = = \langle a \rangle_M(q-1)/M$. Let $a_N(i) = \langle a + iM \rangle_N(q^l - 1)/N$ for $i = 0, \ldots, l-1$. We stop to prove:

LEMMA 3.5: *The digits in the p-adic expansion of $a_N$ are the same as the disjoint union of the digits in the p-adic expansions of $\langle a_N(i) \rangle_q$ for $i = 0, 1, \ldots, l-1$.*

PROOF: The digits of $a_N$ can be divided naturally into $l$ parts each digits of $(\langle a_N q^{i-1} \rangle_{q^l - 1})_q$. So we need only show that the collection $\{a_N q^{i-1}\} \bmod q^l - 1$ is the same as the collection $\{\langle a + iM \rangle_N (q^l - 1)/N\}$. Now since $\mathfrak{q}$ remains prime in $\mathbb{Q}(\mu_N)$, $q$ generates $G(\mathbb{Q}(\mu_N)/\mathbb{Q}(\mu_M))$. Thus $\{aq^{i-1}\}$ mod $N$ consists of elements $b_i$ mod $N$ such that $b_i \equiv a \pmod{M}$. So the collection $\{a_N q^{i-1}\}$ mod $(q^l - 1)$ consists of elements $c_i$ mod $(q^l - 1)$ such that $c_i = b_i(q^l - 1)/N$, $b_i \equiv a$ (mod $M$). But this last collection is clearly the same as $\{\langle a + iM \rangle_N (q^l - 1)/N\}$, which proves the lemma.

We now wish to relate these digits to the digits of $a_M$.

LEMMA 3.6: *The collection $\{\langle a_N(i) \rangle_q\}$ is the same as the collection $\{b(j, a_M)\}$ as in Proposition 2.5.*

PROOF: There exists a unique $i$ such that $\langle a + iM \rangle_N < M$. Replacing $a$ by $a + iM$, we may assume that $\langle a \rangle_N < M$, i.e., that $a < M$. Then $\langle a + iM \rangle_N = a + iM$ and $\langle a_N(i) \rangle_q \equiv a_M/l - i/l$ (mod ${}^q$). So $l\langle a_N(i) \rangle_q \equiv a_M - i$, and $\langle a_N(i) \rangle_q = b(i, a_M)$.

COROLLARY 3.7: $s_N(a) - s_M(a) = (p-1)f\left(\frac{l-1}{2}\right)$.

PROOF: We have just seen that $s_N(a) = \sum_{j=0}^{l-1} s(b(j, a_M))$. Hence by Proposition 2.5, $s_N(a) - s_M(a) = \sum_{j=0}^{l-1} s(b(j,0)) - s(0)$. Now $b(j,0) = \left(\frac{q-1}{l}\right)j$. So, combining the terms of $j$ and $l-j$, $s\left(\frac{q-1}{l}\right)j + s\left(\frac{q-1}{l}(l-j)\right) = s(q-1) = (p-1)f$, hence $s_N(a) - s_M(a) = (p-1)f\left(\frac{l-1}{2}\right)$.

So we have now

$$J(\theta)(\mathfrak{q})\pi^{(1-p)f\left(\frac{l-1}{2}\right)} \equiv \gamma_M(a)/\gamma_N(a) \pmod{\mathfrak{q}^1}$$

COROLLARY 3.8: $\chi(\theta)(\mathfrak{q}) \equiv (-1)^{f(l-1)/2}\gamma_M(a)/\gamma_N(a) \pmod{\mathfrak{q}}$.

PROOF: $\chi(\theta)(\mathfrak{q}) = J(\theta)(\mathfrak{q})/(\mathbb{N}\mathfrak{q})^{(l-1)/2} = J(\theta)(\mathfrak{q})q^{(1-l)/2} = J(\theta)(\mathfrak{q})p^{f(1-l)/2}$.
But by Proposition 2.7, $\pi^{p-1}/p \equiv -1 \pmod{\pi}$, hence mod $\mathfrak{q}^1$ so the desired congruence holds mod $\mathfrak{q}^1$, and hence mod $\mathfrak{q}$.

LEMMA 3.9: $\gamma_M(a)/\gamma_N(a) \equiv (-1)^{f(l-1)/2}\left[\frac{q}{l}\right] l^{\langle a\rangle_M} \pmod{\mathfrak{q}}$.

PROOF: It follows from Lemma 3.6 that $\gamma_M(a)/\gamma_N(a) = \gamma(\langle a\rangle_M)/\prod_{j=0}^{l-1}\gamma(b(j,\langle a\rangle_M))$. By Proposition 2.5, this equals $(\gamma(0)/\prod_{j=0}^{l-1}\gamma(-j))l^{\langle a\rangle_M} \pmod{\mathfrak{q}}$. Using Lemma 2.4 we get $\gamma_M(a)/\gamma_N(a) \equiv (-1)^{f(l-1)/2}\left[\frac{q}{l}\right] l^{\langle a\rangle_M} \pmod{\mathfrak{q}}$, which is the lemma.

Reversing $a$ and $-a$ again we obtain: $\chi(\theta)(\mathfrak{q}) \equiv \left[\frac{q}{l}\right] l^{-\langle a\rangle_M} \pmod{\mathfrak{q}}$.
Now since $l\,|\,M$, $l\,|\,(q-1)$, so $q \equiv 1 \pmod{l}$.

Hence again $\chi(\theta)(\mathfrak{q}) \equiv \chi_{\mathfrak{q},M}(l)^{-a} \pmod{\mathfrak{q}}$. We now compute $\Gamma(\theta)$. Choosing $0 < a < N$,

$$\Gamma(\theta) = \prod_{i=0}^{l-1}\Gamma\left(\frac{a+iM}{N}\right)\Big/\Gamma\left(\frac{a}{M}\right) = l^{\frac{1}{2}-a/M}(2\pi)^{(l-1)/2}$$

by the Gauss multiplication formula. So

$$\Gamma^*(\theta) = \Gamma(\theta)/(2\pi i)^{(l-1)/2} = (-i)^{(l-1)/2} l^{\frac{1}{2}-aM}.$$

Thus

$$
\begin{aligned}
(\Gamma^*(\theta))^{q-1} &= ((-i)^{(l-1)/2} l^{\frac{1}{2}-\frac{a}{M}})^{q-1} \\
&= ((-1)^{\left(\frac{l-1}{2}\right)\left(\frac{q-1}{2}\right)} l^{\frac{q-1}{2}}) l^{-\frac{a}{M}(q-1)} \\
&\equiv \left[\frac{q}{l}\right] l^{-\frac{a}{M}(q-1)} (\text{mod } \mathfrak{q}) \text{ by Proposition 2.6} \\
&\equiv l^{-\frac{a}{M}(q-1)} (\text{mod } \mathfrak{q}) \text{ since } \left[\frac{q}{l}\right] = 1 \text{ as } l \mid M.
\end{aligned}
$$

Clearly $\Gamma^*(\theta)$ generates an abelian extension of $k$, and $(\Gamma^*(\theta))^{w(k)}$ lies in $k$. Now $K \subset k(l^{-1/M}, l^{\frac{1}{2}} i^{(l-1)/2})$. It is immediate that $k(l^{\frac{1}{M}})$ is unramified outside $N$, and $k(l^{\frac{1}{2}} i^{(l-1)/2}) = k(\sqrt{l})$ if $l \equiv 1 \pmod 4$ and $k(\sqrt{-l})$ if $l \equiv 3 \pmod 4$, so unramified over $k$ outside $l$ in either case. We again conclude, using Proposition 3.3, that the Weil and Deligne Theorems hold for $\theta$.

Case 8): Again $\mathfrak{q}$ is a prime ideal in $k$, and $\mathbb{N}\mathfrak{q} = q = p^f$. In this case $\theta = [a]_N - [a]_M + [l^{-1}a]_M$. So for $\mathfrak{q}$ prime to $N$ we have $J(\theta)(\mathfrak{q}) = J_N(a, \mathfrak{q}) J_M(l^{-1}a, \mathfrak{q}) / J_M(a, \mathfrak{q})$ and $\chi(\theta)(\mathfrak{q}) = J(\theta)(\mathfrak{q}) q^{-(l-1)/2}$.

We first consider the case when $\mathfrak{q}$ splits completely in $\mathbb{Q}(\mu_N)$, and let $\mathfrak{q}'$ lie over $\mathfrak{q}$. Then $J(\theta)(\mathfrak{q}) = \prod_i J_N(a + iM, \mathfrak{q}') J_M(l^{-1}a, \mathfrak{q}) / J_M(a, \mathfrak{q})$, where in the product $0 \le i \le l-1$ and $l \nmid a + iM$. But then $\prod_i J_N(a + iM, \mathfrak{q}') J_M(l^{-1}a, \mathfrak{q}) = \prod_{i=0}^{l-1} J_N(a + iM, \mathfrak{q}')$. Applying the Hasse–Davenport distribution formula, we get:

$$
J(\theta)(\mathfrak{q}) = \prod_{i=0}^{l-1} J_N(iM, \mathfrak{q}) \chi_{\mathfrak{q}', N}(l)^{-la}.
$$

Hence $\chi(\theta)(\mathfrak{q}) = \chi_{\mathfrak{q}', N}(l)^{-la} \prod_{i=0}^{l-1} J_N(iM, \mathfrak{q}) q^{-(l-1)/2}$. But exactly as in Case 7, we have

$$
\prod_{i=0}^{l-1} J_N(iM, \mathfrak{q}) q^{-(l-1)/2} = 1,
$$

so $\chi(\theta)(\mathfrak{q}) = \chi_{\mathfrak{q}', N}(l)^{-la} = \chi_{\mathfrak{q}, M}(l)^{-a}$.

We next consider the case when $\mathfrak{q}$ does not split completely in $\mathbb{Q}(\mu_N)$. Let $D_\mathfrak{q}$ be the decomposition group of $\mathfrak{q}$, and let $g > 1$ be the degree of the residue field extension over $\mathfrak{q}$. So $g \mid (l-1)$. Let $\mathfrak{q}'$ be a prime lying over $\mathfrak{q}$. Then $J(\theta)(\mathfrak{q}) = \prod_i J_N(a + iM, \mathfrak{q}') J_M(l^{-1}a, \mathfrak{q}) / J_M(a, \mathfrak{q})$ where $i$ runs over a set $I$ maximal with the following properties:

1) $0 \in I$

2) $l \not| a + iM$

3) $a + iM$ and $a + jM$ belong to distinct orbits of the action of $D_{\mathfrak{q}}$ on $(\mathbb{Z}/N\mathbb{Z})$ if $i \neq j$.

So in particular $I$ has cardinality $(l-1)/g$. Let $a_M = \langle a \rangle_M(q-1)/M$, $a_N = \langle a_N \rangle (q^g - 1)/N$, and $a_N(i) = \langle a + iM \rangle_N(q^g - 1)/N$, $i = 0, \ldots, l-1$.

Lemma 3.10: *Fix $i \in I$. The digits in the p-adic expansion of $a_N(i)$ are the same as the disjoint union of the digits in the p-adic expansion of $\{\langle a_N(j) \rangle_q\}$ as $j$ ranges over a maximal set such that $a + iM$ and $a + jM$ belong to the same orbit of $D_{\mathfrak{p}}$.*

Proof: The proof is similar to the proof of Lemma 3.5 and is left to the reader.

Lemma 3.11: *The collection $\{\langle a_N(j) \rangle_q\}$ for $j = 0, \ldots, l-1$ is equal to the collection $b(j, a_M)$ as in Proposition 2.5.*

Proof: $a_N(j) = \langle a + jM \rangle_N(q^g - 1)/N$. We may assume $0 < a < N$. Let $k$ be such that $a + jM < N$ for $j = 0, \ldots, k$ and $2N > a + jM \geq N$ for $j = k+1, \ldots, l-1$. Then $a_N(j) \equiv a_N - j/l \pmod{q}$ if $j \leq k$ and $a_N(j) \equiv a_N - j/l + 1 \pmod{q}$ if $j \leq k$. It follows that the $a_N(j)$ are the collection $b(j, la_N + l - 1 - k)$. But we see easily that $la_N + l - 1 - k \equiv a_M \pmod{q}$, which proves the lemma.

Set $(l^{-1}a)_M = \langle l^{-1}a \rangle_M(q-1)/M$.

Lemma 3.12: *Let $j$ be such that $\langle a + jM \rangle_N$ is divisible by $l$. Then $\langle a_N(j) \rangle_q = (l^{-1}a)_M$.*

Proof: The above equality is equivalent to $l\langle a_N(j) \rangle_q \equiv a_M$ (mod $(q-1)$). (Since $l \not| M$, and since $\mathfrak{q}$ does not split completely in $\mathbb{Q}(\mu_N)$, $q \not\equiv 1 \pmod{l}$ and $l$ is prime to $q - 1$.) Now

$$a_M \equiv \langle a \rangle_N(q-1)/M \qquad (\mathrm{mod}\,(q-1)),$$

and $0 \leq \langle a + jM \rangle_N < N$, $l | \langle a + jM \rangle_N$ and $\langle a + jM \rangle_N \equiv \langle a \rangle_M \pmod{M}$. Thus we may apply Proposition 2.8 with $a = \langle a \rangle_M$ and $b = \langle a + jM \rangle_N$ to deduce the result.

It now follows as before from Stickelberger's theorem, (switching $a$ to $-a$) that:

$$J(\theta)(\mathfrak{q})\pi^{-\Sigma s_N(a+iM)-s_M(l^{-1}a)+s_M(a)}$$
$$\equiv \gamma_M(a)/(\gamma_M(l^{-1}a)\prod \gamma_N(a+iM)) \pmod{\mathfrak{q}''},$$

where $\mathfrak{q}''$ is the unique prime of $\mathbb{Q}(\mu_{Np})$ lying over $\mathfrak{q}'$. Using the above lemmas, we see that

$$\sum_I s_N(a+iM) + s_M(l^{-1}a) - s_M(a) = \sum_{j=0}^{l-1} s(b(j,a_M) - s(a_M)$$
$$= \sum_{j=0}^{l-1} s(b,0)) \quad \text{by Proposition 2.5.}$$

Suppose that $x = b(j,0)$ so $lx \equiv -j \pmod{q}$. Then $l(q-1-x) \equiv -(l-j) \pmod{q}$ so $b(j,0) + b(l-j,0) = q-l$, and it follows that

$$\sum_{j=0}^{l-1} s(b(j,0)) = (p-1)f(l-1)/2.$$

So

$$J(\theta)(\mathfrak{q})\pi^{-(p-1)f(l-1)/2} \equiv \gamma_M(a)/\gamma_M(l^{-1}a)\prod_I \gamma_N(a+iM) \pmod{\mathfrak{q}''}.$$

Since $\chi(\theta)(\mathfrak{q}) = J(\theta)(\mathfrak{q})q^{-(l-1)/2}$ we have, using Proposition 2.7,

$$\chi(\theta)(\mathfrak{q}) \equiv (-1)^{f(l-1)/2}\gamma_M(a)/\gamma_M(l^{-1}a)\prod_I \gamma_N(a+iM) \pmod{\mathfrak{q}''}$$

and hence mod $\mathfrak{q}$. Now using Lemmas 3.8, 3.9, 3.10 and Proposition 2.5, we obtain:

$$\chi(\theta)(\mathfrak{q}) \equiv (-1)^{f(l-1)/2}\gamma(a_M)/\prod_{j=0}^{l-1}\gamma(b(j,a_M)) \pmod{\mathfrak{q}}$$
$$\equiv (-1)^{f(l-1)/2} l^{a_M}/\prod_{j=0}^{l-1}\gamma(b(j,0)) \pmod{\mathfrak{q}}$$
$$\equiv \begin{bmatrix} q \\ l \end{bmatrix} l^{a_M} \pmod{\mathfrak{q}} \text{ by Lemma 2.4.}$$

Switching back from $a$ to $-a$ we conclude that

$$\chi(\theta)(\mathfrak{q}) \equiv \chi_{\mathfrak{q},M}(l)^{-a}\begin{bmatrix} q \\ l \end{bmatrix} \pmod{\mathfrak{q}}.$$

We now compute $\Gamma(\theta)$. Choosing $a$ such that $0 < a < N$, $\Gamma(\theta) = \prod_i \Gamma((a + iM)/N)\Gamma((a + jM)/N)\Gamma(a/M)$, where $i$ runs over the set of integers between 0 and $l - 1$ such that $l \nmid a + iM$ and $j$ is such that $l \mid a + jM$. So

$$\Gamma(\theta) = \prod_{i=0}^{l-1} \Gamma\left(\frac{a}{N} + \frac{i}{l}\right) \Big/ \Gamma\left(\frac{a}{M}\right) = l^{\frac{1}{2} - \frac{a}{M}}(2\pi)^{\frac{1}{2}(l-1)}$$

by the Gauss Multiplication Formula. So

$$\Gamma^*(\theta) = (-i)^{(l-1)/2} l^{\frac{1}{2} - \frac{a}{M}}.$$

Therefore

$$\Gamma^*(\theta)^{q-1} = l^{-\frac{a}{M}(q-1)} l^{\frac{q-1}{2}} (-i)^{(l-1)(q-1)/2}$$

$$\Gamma^*(\theta)^{q-1} \equiv l^{-\frac{a}{M}(q-1)} \left[\frac{q}{l}\right] (\text{mod } \mathfrak{q}) \text{ by Proposition 2.6.}$$

So $\Gamma^*(\theta)^{q-1} \equiv \chi(\theta)$ (mod $\mathfrak{q}$) and, as in Case 7 by Proposition 3.3, Weil's and Deligne's Theorems hold for $\theta$.

If the reader has successfully struggled through Cases 1–8, he should have no problem with Case 9.

It remains to prove the statement about the conductor. It follows immediately from Proposition 3.3 that in every case, the finite part of the conductor divides a power of $N$, so we need only show that $J(\theta)$ is unramified at $\infty$. For cases 1–6, $n(\theta) = 0$, and $\Gamma^*(\theta) = \Gamma(\theta)$ is real, so $\chi(\theta)$ is unramified at $\infty$, and we are done. In case 7, $k = \mathbb{Q}(\mu_M)$ must be imaginary, since $M \geq l \geq 3$. In case 8, we may assume $M = 1$ or 2, i.e., $k = \mathbb{Q}$. If $l \equiv 1$ (mod 4), then $n(\theta)$ is even and $\chi(\theta)$ corresponds to $\mathbb{Q}(\sqrt{l})$ so $J(\theta)$ is unramified at $\infty$. If $l \equiv 3$ (mod 4), $n(\theta)$ is odd and $\chi(\theta)$ corresponds to $\mathbb{Q}(\sqrt{-l})$, so again $J(\theta)$ is unramified at $\infty$. In case 9, $n(\theta)$ is 1 and $\chi(\theta)$ corresponds to $\mathbb{Q}(\sqrt{-1})$, so again $J(\theta)$ is unramified at $\infty$.

## §4. Proof of the generalized Weil and Deligne theorems

We begin by proving the generalized Weil and Deligne theorems for the special $\theta$'s of the last section, but where we let $k$ be any subfield of $Q(\mu_M)$. Throughout this section $G$ will denote $G(\mathbb{Q}(\mu_M)/k) \subset (\mathbb{Z}/M\mathbb{Z})^x$. In cases 1–4, it is easy to verify that $\chi(\theta) = J(\theta) = 1$ and $\Gamma^*(\theta) = \Gamma(\theta) = 1$ in $\mathbb{R}^x/\mathbb{Q}^x$, so we confine our attention to cases 5–8. We begin by proving.

LEMMA 4.1: *$\Gamma^*(\theta)$ generates an abelian extension of $k$, unramified outside $N$, and $\Gamma^*(\theta)^{w(k)}$ lies in $k$.*

PROOF: We begin by showing that $\Gamma^*(\theta)$ generates an abelian extension of $k$. Let $G = G(\mathbb{Q}(\mu_M)/k)$. In cases 5 and 6, we have $\Gamma^*(\theta) = 2^{[\mathbb{Q}(\mu_M):k]}2^{-\sum_{b\in G} ab/M}$. In cases 7 and 8

$$\Gamma^*(\theta) = ((-i)^{(l-1)/2}l^{\frac{1}{2}})^{[\mathbb{Q}(\mu_M):k]}l^{-\sum_{b\in G} ab/M}.$$

Since $i$ and $l^{\frac{1}{2}}$ generate abelian extensions of $k$, we are immediately reduced to showing that $l^{\sum_{b\in G} ab/M}$ generates an abelian extension of $k$. Let $e$ in $\mathbb{Z}/M\mathbb{Z}$ be defined by $e = \sum_{b\in G} b$. Then $k(l^{\Sigma ab/M})/k$ is abelian exactly when $k$ contains the $(M/e)$-th-roots of unity. Let $\zeta$ be a primitive $M$-th root of unity. Then $\zeta^e = \mathbb{N}_{Q(\mu_M)/k}(\zeta)$ is in $k$ and is a primitive $(M/e)$-th root of unity, so $k(\Gamma^*(\theta)$ is abelian over $k$. To see that $\Gamma^*(\theta)^{w(k)}$ lies in $k$, since $w(k)$ is even it is enough to verify that $(l^{ea/M})^{M/e}$ is in $k$, which is clear.

We have immediately that $k(\Gamma^*(\theta))/k$ is unramified over $k$ outside of $2N$, but since $k((-i^{(l-1)/2}l^{\frac{1}{2}}) = k(\sqrt{l})$ if $l \equiv 1 \pmod 4$ and $k(\sqrt{-l})$ if $l \equiv -1 \pmod 4$ we see that if $2 \nmid N$ $k(\Gamma^*(\theta)/k)$ is unramified at 2.

THEOREM 4.2: *The Generalized Weil and Deligne theorems are true for the $\theta$'s of the last section, and any $k \subset \mathbb{Q}(\mu_M)$, and the conductor of $J(\theta)$ divides a power of $N$.*

PROOF: Let $\mathfrak{q}$ be a prime ideal of $k$, with $\mathbb{N}\mathfrak{q} = q$. We have only to prove that $\Gamma^*(\theta)^{q-1} \equiv \chi(\theta)(\mathfrak{q}) \pmod{\mathfrak{q}}$. If we write $\theta = \theta(a, k)$, it is immediate that $\Gamma^*(\theta(a, k)) = \prod_{b\in G} \Gamma^*(\theta(ab, \mathbb{Q}(\mu_M))$ so

$$\Gamma^*(\theta)^{q-1} = \prod_b \Gamma^*(\theta(ab, \mathbb{Q}(\mu_M))^{q-1}.$$

Let us first consider the cases when $l$ is odd. Then

$$\Gamma^*(\theta(a, \mathbb{Q}(\mu_M)) = (-i)^{(l-1)/2}l^{\frac{1}{2}-\frac{a}{M}}$$

So

$$\Gamma^*(\theta(a, k)) = ((-i)^{(l-1)/2}l^{\frac{1}{2}})^{\# G}l^{-\sum_{b\in G}\frac{ab}{M}}$$

Thus

$$\Gamma^*(\theta(a,k)^{q-1} = (-1^{(l-1)/2} l^{\frac{1}{2}})^{\# G(q-1)} l^{-\sum_{b\in G} \frac{ab(q-1)}{M}}$$

By Proposition 2.6, we have

$$((-i)^{(l-1)/2} l^{\frac{1}{2}})^{(q-1)\# G_M} \equiv \begin{bmatrix} q \\ l \end{bmatrix}^{\# G} \pmod{\mathfrak{q}}$$

Hence

$$\Gamma^*(\theta(a,k))^{q-1} \equiv \begin{bmatrix} q \\ l \end{bmatrix}^{\# G} l^{-\Sigma \frac{ab(q-1)}{M}} \pmod{\mathfrak{q}}.$$

Let us now compute $\chi(\theta)(\mathfrak{q})$. Analogously to the above, we have:

$$\chi(\theta(a,k))(\mathfrak{q}) = \prod_{b\in G/D} \chi(\theta(ab, \mathbb{Q}(\mu_M))(\mathfrak{q}^*),$$

where $\mathfrak{q}^*$ is a prime in $\mathbb{Q}(\mu_M)$ lying above $\mathfrak{q}$ and $D$ is the decomposition group of $\mathfrak{q}$ in $G$. Then we have previously seen that

$$\chi(\theta(ab, \mathbb{Q}(\mu_M))(\mathfrak{q}^*) \equiv \begin{bmatrix} q^g \\ l \end{bmatrix} l^{-ab(q^g-1)/M} \pmod{\mathfrak{q}^*}$$

where $q^g = \mathbb{N}\mathfrak{q}^*$.

$$\text{So } \chi(\theta(a,k))(\mathfrak{q}) \equiv \begin{bmatrix} \mathfrak{q} \\ 1 \end{bmatrix}^{\# G} \prod_{b\in G/D} l^{-ab(q^g-1)/M} \pmod{\mathfrak{q}^*}$$

$$\equiv \begin{bmatrix} q \\ l \end{bmatrix}^{\# G} \prod_{b\in G} l^{-ab(q-1)/M} \pmod{\mathfrak{q}^*},$$

since $\sum_{b\in D} b = 1 + q + \ldots + q^{g-1} = (q^g - 1)/(q-1)$.

Since both sides of the congruence lie in $k$, the congruence holds modulo $\mathfrak{q}$ as well as $\mathfrak{q}^*$, and $\Gamma^*(\theta)^{q-1} \equiv \chi(\theta) \pmod{\mathfrak{q}}$, Hence by Proposition 3.3, and Lemma 4.1, Weil's and Deligne's theorems are true for $\theta$, and the finite part of the conductor of $J(\theta)$ divides a power of $N$.

It remains to check once again that $J(\theta)$ is unramified at $\infty$. In cases 1–4, $n(\theta) = 0$ and $\Gamma^*(\theta) = 1$, so there is no problem. For cases 5–9, we may clearly assume $k$ is real. Since $n(\theta) = 0$ in Cases 5 and 6, $\dfrac{l-1}{2}[K_M:k]$ in Cases 7 and 8, and $[K_M:k]$ in Case 9, $n(\theta)$ is always even unless $K_M = \mathbb{Q}$, when $k$ must be $K_M$. But we have treated this case in the last section, so we may assume $n(\theta)$ is even, and show that $k(\Gamma^*(\theta))/k$ is unramified at $\infty$.

Using the notation in the proof of Lemma 4.1, since $k$ is real, $M/e$ must be 1 or 2 and $[K_M:k]$ is even. Hence, up to a rational number, $\Gamma^*(\theta) = 1$ or $\sqrt{l}$, and $k(\Gamma^*(\theta))$ is still totally real, so we are done.

The cases when $l = 2$ are similar to the above and left to the reader.

REMARK 4.3: We have proved that, for all of our special $\theta$'s, and for any $k \subset \mathbb{Q}(\mu_M)$, the function on ideals prime to $N$ defined by $\mathfrak{p} \mapsto J(\theta)(\mathfrak{p})$ is a Hecke character of conductor dividing a power of $N$, of the form $\chi(\theta)\mathbb{N}^{n(\theta)}$, and that for $\mathfrak{p}$ prime to $N$, $(\chi(\theta)(\mathfrak{p}))(\Gamma^*(\theta)) = \sigma_{\mathfrak{p}}(\Gamma^*(\theta))$.

We now are ready to complete the proof of Theorems 1.5 and 1.6 (the generalized Weil and Deligne theorems).

PROOF OF THEOREMS 1.5 AND 1.6: Let $\theta_0 = \sum_{i=1}^{s} \sum_a r_i(a)[a]_{N_i}$ be of Weil type, with respect to $k \subset K_{N_i}$ for all $i$. Let $K_f$ be the minimal cyclotomic field containing $k$, so that $K_f \subseteq K_{N_i}$ for all $i$. If all the $N_i$ are odd, we may assume that $f$ is odd, and if any $N_i$ is even, we may assume that $f$ is even. If $f$ is even, and some $N_i$ is odd, we may replace $N_i$ by $2N_i$, since $J(\sum_a r_i(a)[a]_{N_i} - \sum_a r_i(a)[2a]_{2N_i})$ is the trivial character and $\Gamma^*(\sum_a r_i(a)[a]_{N_i} - \sum_a r_i(a)[2a]_{2N_i}) = 1$. So we may assume that $f$ divides each $N_i$.

We proceed by induction on the number $t$ of $N_i$'s $\neq f$. If $t = 0$, all $N_i$'s are equal to $f$, and we are in the case already proved by Weil. If $t \neq 0$, we induct on the number of prime factors of any $N_i/f \neq 1$. So let $\theta_0 = \theta_1 + \theta_2$ where $\theta_1 = \sum_{i=1}^{s-1} \sum_a r_i(a)[a]_{N_i}$ and $\theta_2 = \sum_a r(a)[a]_{N_s}$, $N_s$, $N_s = lM$, $f|M$. But using Theorem 4.2, we may always write $\theta_2$ as $\theta_3 + \theta_4$,
where $\theta_3 = \sum_a r'(a)[a]_M$ and $\theta_4$ is an integral multiple of one of the relations in Theorem 4.3, involving only $M$ and $N_s$. Since $\theta_4$ is of Weil type, $\theta_1 + \theta_3$ is of Weil type. By the induction hypothesis, Weil's theorem is true for $\theta_1 + \theta_3$, and by Theorem 4.2 it is true for $\theta_4$. Since $J(\theta)$, $\chi(\theta)$ and $\Gamma^*(\theta)$ are all multiplicative in $\theta$, Weil's theorem is true for $\theta_0$. If we assume that $\theta_0$ is of Deligne type, then the above argument also shows that Deligne's theorem is true for $\theta$.

## §5. Deligne's theorem for $k \subset \mathbb{Q}(\mu_p)$

In this section we show how the methods of this section yield a proof of Deligne's theorem *ab* initio in the case when $k \subset \mathbb{Q}(\mu_p)$.

We begin with some notation. If $\theta = \sum_a s(a)[a]_p$, let $\tilde{\theta} = \sum_a \sum_b s(a)[ab]_p$, where $b$ runs through $G = G(\mathbb{Q}(\mu_p)/k) \subset (\mathbb{Z}/p\mathbb{Z})^x$. We may write $\tilde{\theta} = \sum_a r_a[a]_p$, where $r_a = \sum_{b \in G} s(ab^{-1})$ has a constant value $r(O)$ on fixed orbit $O$ of $G$. So we may also write $\tilde{\theta} = \sum_O r(O) \sum_{\gamma \in O} [\gamma]_p$, where $r_a = r(O)$ if $a \in O$.

Lemma 5.1: *Deligne's theorem is true for $k \subset \mathbb{Q}(\mu_p)$ and $N = p$.*

Proof: We first claim that if $\theta$ is of Deligne type, $r_a = r_{p-a}$ for $1 \leq a \leq p-1$.

If $k$ is real, $-1$ is in $G$, and so automatically $r_a = r_{p-a}$. So we may assume $k$ is imaginary. By definition of Deligne type, $\sum_O r(O) \sum_{\gamma \in O} \left\langle \dfrac{-\gamma c}{p} \right\rangle$ is an integer independent of $c$, where $O$ runs through the orbits of $G$. Let $W$ be the space of $\sum_a r_a[a]_p$ such that $r_a$ is complex and constant on $G$-orbits. So $\theta \in W \Rightarrow \theta = \sum_O r(O) \sum_{\gamma \in O} [\gamma]_p$. Let $R \subseteq W$ be the subspace consisting of all $\theta$'s such that $\sum_O r(O) \sum_{\gamma \in O} \left\langle \dfrac{-\gamma c}{p} \right\rangle$ is independent of $c$.

We define a linear map $\phi : W \to W$ by $\phi(\sum_O r \sum_{\gamma \in O} [\gamma]_p) = \sum_c \sum_O r(O) \sum_{\gamma \in O} \left\langle \dfrac{-\gamma c}{p} \right\rangle [c]$.

If we let $\Delta \subset W$ be generated by $\sum_a [a]_p$, then $R$ is exactly $\phi^{-1}(\Delta)$. Let $\chi$ be a character of $G(k/\mathbb{Q})$, viewed as a character on $(\mathbb{Z}/p\mathbb{Z})^x$ which is invariant under the action of $G$. Let $A_\chi$ be the vector $\sum_a \chi(a)[a]_p = \sum_O \chi(O) \sum_{\gamma \in O} [\gamma]_p$, clearly $A_\chi$ lies in $W$. If $\chi$ is non-trivial,

$$\phi(A_\chi) = \sum_c \left( \sum_O \chi(O) \sum_{\gamma \in O} \left\langle \frac{-\gamma c}{p} \right\rangle [c] \right) = \sum_c \left( \sum_a \chi(a) \left\langle \frac{-ac}{p} \right\rangle \right) [c]$$
$$= \sum_c \bar{\chi}(c) \left( \sum_a \frac{-\chi(a)a}{p} \right) [c] = L(\chi, 0) (\sum_c \bar{\chi}(c)[c]).$$

If $\chi$ is trivial, $\phi(A_\chi) = \dfrac{(p-1)}{2} \sum_c [c]$. So, by the theorem on linear independence of characters, we have $\dim(\operatorname{Im} \phi) \geq 1 + \frac{1}{2}[k:Q]$. Since $\dim W = [k:\mathbb{Q}]$, and $\operatorname{Im} \phi \supset \Delta$, $\dim R \leq \frac{1}{2}[k:\mathbb{Q}]$.

For $1 \leq a \leq \dfrac{p-1}{2}$. Let $V_a$ be the vector $\sum r_b[b]_p$ in $W$, where $r_b = 1$ if $b$ is in the same $G$-orbit as a or $p-a$ and 0 otherwise. It is immediate that there are $\frac{1}{2}$-$[k:\mathbb{Q}]$ distinct $V_a$'s, and that these are linearly independent and lie in $R$. Hence they span $R$. and if $\theta = \sum r_a[a]_p$ is any vector in $R$, we must have $r_a = r_{p-a}$. If $\theta$ is of Deligne type $\theta$ is in $R$, and we have demonstrated our claim.

It is also immediate that the $V_a$'s are in fact of Deligne type, and hence any $\theta$ of Deligne type is a linear combination of the $V_a$'s with integral coefficients. So to complete the proof, we need only show that Deligne's theorem holds for $V_a$.

Now

$$\Gamma(V_a) = \prod_{b\in G} \Gamma\left(\frac{ab}{p}\right)\Gamma\left(\frac{(p-a)b}{p}\right) = \prod_{b\in G} \Gamma\left(\frac{ab}{p}\right)\Gamma\left(1-\frac{ab}{p}\right)$$

in $\mathbb{C}^x/\mathbb{Q}^x$. Since

$$\Gamma(z)\Gamma(1-z) = \frac{\pi}{\sin \pi z,}\Gamma(V_a) = \pi^{\#G}/\prod_{b\in G}\sin\left(\frac{\pi ab}{p}\right).$$

If we let $\eta_a = e^{\frac{\pi i a}{p}} - e^{\frac{-\pi i a}{p}}$ in $\mathbb{Q}(\mu_p)$ then

$$\prod_{b\in G} \sin\left(\frac{\pi ab}{p}\right) = \mathbb{N}_{\mathbb{Q}(\mu_p)/k}(\eta)(2i)^{-\#G}.$$

Hence $\Gamma^*(V_a) = (2\pi i)^{-\#G}\Gamma(V_a) = \mathbb{N}_{\mathbb{Q}(\mu_p)/k}(\eta_a)$ lies in $k$.

To check Deligne's theorem, we need only show that $\chi(\theta)$ is trivial. But $\chi(\theta) = J(\theta)\mathbb{N}^{-\#G}$, and since $J(a,\mathfrak{f})J(p-a,\mathfrak{f}) = \mathbb{N}\mathfrak{f}$ for any prime ideal $\mathfrak{f}$ of $\mathbb{Q}(\mu_p)$, it follows easily that $J(\theta) = \mathbb{N}^{\#G}$ and $\chi(\theta)$ is trivial.

LEMMA 5.2: Deligne's theorem is true for $k \subseteq \mathbb{Q}(\mu_p)$ and $N = 2p$.

PROOF: let $\theta = \sum_a r(a)[a]_{2p}$ be of Deligne-type. Then

$$\begin{aligned}\theta = &\sum_{a\,\text{even}} r(a)([a]_{2p} - [a/2]_p) + \sum_{a\,\text{even}} r(a)[a/2]_p \\ &+ \sum_{a\,\text{odd}} r(a)([a]_{2p} - [p]_{2p} - [a]_p + [2^{-1}a]_p) \\ &+ \sum_{a\,\text{odd}} r(a)([a]_p - [2^{-1}a]_p) + (\sum_{a\,\text{odd}} r(a)[p]_{2p}),\end{aligned}$$

which we may write as $\theta = \theta_1 + \theta_2 + \theta_3 + \theta_4 + \theta_5$. Now $\theta_1$ and $\theta_3$ are of Deligne type and Deligne's theorem is true for them by Theorem 3.4.

Since $\theta$ is of Weil type, $\sum_a r(a)\sum_b \frac{ab}{2p} \in \mathbb{Z}$, where $b$ runs through $G(Q(\mu_{2p}(k)) \subset (\mathbb{Z}/2p)^x$. Hence $\sum_a r(a)\sum_b ab \equiv 0 \pmod 2$, which implies $\sum_{a\,\text{odd}} r(a)\sum_b b \equiv 0 \pmod 2$. But since all the $b$'s are odd, $\sum_b b \equiv \#G \pmod 2$, and $\sum_{a\,\text{odd}} r(a)\#G$ is even. By Theorem 3.4, case 9, $\theta_5$ is of Deligne type and Deligne's theorem is true for it. Hence $\theta_2 + \theta_4$ is of Deligne type. But by Lemma 5.1, Deligne's theorem is true for $\theta_2 + \theta_4$, hence Deligne's theorem is true for $\theta$.

THEOREM 5.3: *Deligne's theorem is true for* $k \subseteq \mathbb{Q}(\mu_p)$ *and any* $\theta$.

PROOF: The proof of Theorems 1.5 and 1.6 in §4 immediately reduces the general Deligne's theorem for $k$ to Theorems 5.1 and 5.2.

## §6. The Gauss sum identities of Langlands

In this section we show that the Gauss-sum identities of Langlands [10] may be derived from the main theorem of this paper. We begin by stating the first Langlands identity:

THEOREM 6.1 (Langlands): *Let $F_1$ and $F_2$ be two finite fields, $F_2$ containing $F_1$. Let $F_1$ have $q$ elements and $F_2$ have $q^f$ elements, and let $l$ be a prime with $(l, q) = 1$ such that the order of $q$ mod $l$ is equal to $f$. Let $T$ be a set of representatives for the orbits of non-trivial characters of $F_2^x$ of order $l$ under the Galois group $G(F_2/F_1)$. Let $\rho$ be a character of $F_1^x$. Then:*

$$G(\rho^l)\prod_{\mu\in T} G(\mu) = \rho(l^l)G(\rho)\prod_{\mu\in T} G(\mu(\sigma\circ\mathbb{N})).$$

(*Here $\mathbb{N}$ denotes the norm from $F_2$ to $F_1$*).

REMARK 6.2: If $f = 1$, this reduces to the Hasse–Davenport distribution formula (Proposition 2.10). This is always the case when $l = 2$.

REMARK 6.3: In Langlands' statement, the "$\sigma(l^l)$" is on the other side of the equation; this is because he calls $G(\rho)$ what we call $G(\rho^{-1})$.

PROOF OF THEOREM 6.1: We may assume that $f > 1$, since we are taking the Hasse–Davenport distribution formula as known. (The methods of this paper also yield a new proof of the distribution formula, which we leave to the reader.) Let $M = q - 1$, and $N = lM$. Since $f > 1$,

$l \nmid M$. We may clearly identify our field $F_1$ with a residue field of the ring of integers in $\mathbb{Q}(\mu_M)$ at a prime $\mathfrak{p}$, and our character $\rho$ with $\chi_{\mathfrak{p}}^a = \chi_{\mathfrak{p}}^{a(q-1)/M}$ for a suitable $a$ in $(\mathbb{Z}/M\mathbb{Z})^x$. Choose $b \in \mathbb{Z}/N\mathbb{Z}$ such that $l \nmid b$ and $b \equiv la \pmod{M}$. We may assume by Remark 6.2 that $l$ is odd, and we let $k = \mathbb{Q}(\mu_M)$, and $\theta = [b]_N - [b]_M + [l^{-1}b]_M - [M]_N$.
By case 8 of Theorem 3.4 with $a = M$, we see that $\theta' = [M]_N$ is of Deligne type, with $n(\theta') = (l-1)/2$, and Deligne's theorem is true for it. Hence, again by case 8 of Theorem 3.4, Deligne's theorem is true for $\theta$, and $n(\theta) = 0$, $\Gamma^*(\theta) = \Gamma(\theta)$. Deligne's theorem for $\theta$, at the prime $\mathfrak{p}$, translates into:

$$\Gamma(\theta)^{\sigma_{\mathfrak{p}}} = \chi(\theta)(\mathfrak{p})\Gamma(\theta),$$

where

$$\chi(\theta)(\mathfrak{p}) = \prod_{\mu \in T} (G(\rho \circ \mathbb{N})\mu) G(\rho) (\prod_{\mu \in T} G(\mu))^{-1} (G(\rho^l))^{-1}.$$

On the other hand, using the proof of case 8 of Theorem 3.4, $\Gamma(\theta)$ is immediately computed to be $l^{-b/M} \in \mathbb{R}^x/\mathbb{Q}^x$, while Langlands' result asserts that $\chi(\theta)(\mathfrak{p}) = \rho^{-1}(l^l) = \chi_{\mathfrak{p}}^{-a}(l^l) = \chi_{\mathfrak{p}}^{-b}(l)$. Since $M$ is prime to $q$, it is enough to check that $\sigma_{\mathfrak{p}}(l^{-b/M}) \equiv \chi_{\mathfrak{p}}^{-b}(l)^{-b/M} \pmod{\mathfrak{p}}$ or that $l^{(q-1)(-b/M)} \equiv \chi_{\mathfrak{p}}^{-b}(l) \pmod{\mathfrak{p}}$. Since $M = q-1$, this is clear.

We now come to the second Langlands identity:

THEOREM 6.4 (Langlands): *Let $F_1$ be a finite field with $q$ elements and let $F_2$ be an extension of $F_1$ of degree $l$ where $l$ is a prime dividing $q-1$. Suppose $\rho$ is a character of $F_1^x$ whose restriction to the $l$-th roots of unity is non-trivial and $\psi$ is a character of $F_2^x$ such that $\psi^l = \rho \circ \mathbb{N}$. If $T$ is the set of non-trivial characters of $F_1^x$ of order $l$, then*

$$G(\rho) \prod_{\mu \in T} G(\mu) = \rho(l) G(\psi).$$

PROOF: We start with the following lemma:

LEMMA 6.5: *Let $l \mid M$ and $\theta = \sum_{i=1}^{l-1} [iM/l]_M$. Then $\theta$ is of Deligne type, $n(\theta) = \dfrac{l-1}{2}$, $\Gamma(\theta) = (2\pi)^{(l-1)/2} l^{-1/2}$, and Deligne's theorem is true for $\theta$.*

PROOF OF LEMMA: We may rewrite $\theta$ as $\sum_{i=1}^{(l-1)/2} ([iM/l]_M + [(l - - i)M/l]_M)$. These are all expressions of the type $[a]_M + [M-a]_M$,

$a \neq 0$, so we may assume $\theta$ has this form. Then immediate calculations yield first that $\theta$ is of Deligne type with $n(\theta) = 1$ and next that $\Gamma^*(\theta) = (\sin(\pi a/M))^{-1}$. Note that we may write $(\sin(\pi a/M))^{-1}$ as $ce^{-\pi i a/M}$ where $c$ is a non-zero element of $k = \mathbb{Q}(\mu_M)$, and a unit away from primes dividing $M$.

On the other hand, $J(\theta)(\mathfrak{p}) = G(\chi_{\mathfrak{p}}^a)G(\chi_{\mathfrak{p}}^{-a}) = \chi_{\mathfrak{p}}(-1)^a \mathbb{N}\mathfrak{p}$, by standard properties of Gauss sums. So $\chi(\theta)(\mathfrak{p}) = (-1)^{a(q-1)/M}$, where $q = \mathbb{N}\mathfrak{p}$. Since $c^{q-1} \equiv 1 \pmod{\mathfrak{p}}$ $\Gamma^*(\theta)^{q-1} \equiv e^{-\pi i a(q-1)/M} \equiv (-1)^{a(q-1)/M} \pmod{\mathfrak{p}}$, so an application of Proposition 3.3 completes the proof.

REMARK: This result has also been demonstrated by Gross and Koblitz [11] but we give a proof here for the sake of completeness.

We now resume the proof of the theorem. We proceed as in Theorem 6.3. Let $M = q - 1$, $N = lM$, $\rho = \chi_{\mathfrak{p}}^a = \chi_{\mathfrak{p}}^{a(q-1)/M}$, and $\theta = [a]_N - [a]_M - \sum_{i=1}^{l-1} [iM/l]_M$. By Lemma 6.5 and Case 7 of Theorem 3.4, Deligne's theorem is true for $\theta$, and we see that $n(\theta) = 0$, $\Gamma^*(\theta) = \Gamma(\theta)$, and $\Gamma(\theta) = l^{1-a/M}$. Theorem 6.4 can now be restated as $J(\theta) = \rho^{-1}(l)$. Since both sides are roots of unity, it suffices to verify this mod $\mathfrak{p}$. But by Deligne's theorem. $J(\theta) \equiv l^{\frac{-a(q-1)}{M}} = l^{-a/M} \pmod{\mathfrak{p}}$ and $\rho^{-1}(l) \equiv l^{-a/M} \pmod{\mathfrak{p}}$ by definition, so we are done.

## Appendix – by Daniel S. Kubert

### *Generalized Gauss Sum Identities*

We now show how *Proposition* 2.10 and the two Langlands' identities may be viewed as special cases of a more general identity on Gauss sums. Conversely it seems likely that this generalized identity may be obtained from the three identities above and possibly also *Proposition* 2.12 but an inductive proof does not appear to be straightforward.

Let $M, m \in Z$, $M > 1$, $m > 1$. Let $a \in Z/MZ - (0)$. We construct a $\theta$ of Deligne type such that the corresponding $\Gamma$-factor is

$$\prod_{b \in Q/Z} \Gamma(\langle b \rangle) \Big/ \Gamma\left(\left\langle \frac{a}{M} \right\rangle\right) \prod_{\substack{c \in Q/Z \\ mc = 0 \\ c \neq 0}} \Gamma(\langle c \rangle)$$

For each $b$ let $N(b)$ be minimal such that

1) $bN(b) \in Z$

2) $M$ divides $N(b)$

We define $N(c)$ in the same manner.

Suppose $\sigma \in \mathrm{Gal}(Q(\mu(N))/Q(\mu(M)))$. Then $m\sigma b = a$ since $\sigma \equiv 1(M)$ and clearly $N(\sigma b) = N(b)$. We wish to show that the set of $b$'s with fixed $N(b)$ can be written as a disjoint union of sets of the form $\{\sigma b, \sigma \in Q(\mu(N(b))/Q(\mu(M))\}$. We require the following lemma.

LEMMA: *Let $\sigma \in \mathrm{Gal}\, Q(\mu(N(b)))/Q(\mu(M)))$ such that $\sigma b \equiv b \bmod Z$. Then $\sigma$ is trivial.*

PROOF: By assumption $M$ divides $\sigma - 1$, and we wish to show that $N(b)$ divides $\sigma - 1$. Now $(\sigma - 1)b \in Z$ by assumption, so $\sigma - 1$ satisfies properties 1), 2) above and is therefore divisible by $N(b)$ by definition. Thus $\sigma$ is trivial.

We now construct a $\theta$ with the desired properties.

For each $N$ which is divisible by $M$ we consider the set $B(N) = = \left\{ b \in Q/Z,\ mb = \frac{a}{M}, N(b) = N \right\}$. For most $N$, $B(N)$ will be empty. If not we partition it into sets of the form $\{\sigma b_i,\ \sigma \in \mathrm{Gal}\, Q(\mu(N))/Q(\mu(M))\}$ where $i$ ranges over an index set $I_1(N)$. We also create sets $C(N) = = \{c \in Q/Z - O,\ mc = 0,\ N(c) = N\}$ and partition them over $I_2(N)$ as above. We then define $\theta$ by

$$\theta = \sum_N \sum_{I_1(N)} (b_i N)_N - (a)_M - \sum_N \sum_{I_2(N)} (c_j N)_N$$

where $\theta$ is considered with respect to the field $Q(\mu_M)$. Then we claim

PROPOSITION: (i) *$\theta$ if of Deligne type with $n(\theta) = 0$*

$$\text{(ii) } \Gamma(\theta) = \prod_{\substack{b \in Q/Z \\ mb = \frac{a}{M}}} \Gamma(\langle b \rangle) \Big/ \Gamma\left(\left\langle \frac{a}{M} \right\rangle\right) \prod_{\substack{c \in Q/Z \\ c \neq 0 \\ cm = 0}} \Gamma(\langle c \rangle)$$

PROOF: Part (ii) of the proposition is clear from construction. Part (i) is also easy. We first show that

$$\sum_{\substack{b \in Q/Z \\ mb = \frac{a}{M}}} b - \frac{a}{M} - \sum_{\substack{c \neq 0 \\ c \in Q/Z \\ mc = 0}} c \in Z$$

$$\text{Now } \sum b = \sum_{\substack{c \in Q/Z \\ mc = 0}} \frac{a}{mM} + c$$

Therefore the above sum equals $m \frac{a}{mM} - \frac{a}{M} \in Z$.

To complete the proof of the proposition we must show that $n(\theta) = 0$. Now

$$n(\theta) = \sum_b (B_1(\langle b \rangle) + \tfrac{1}{2}) - \left(B_1\left\langle \frac{a}{M} \right\rangle + \tfrac{1}{2}\right)$$

$$- \sum_c (B_1(\langle c \rangle) + \tfrac{1}{2})$$

and since $\sum_b (b) - \left(\frac{a}{M}\right)$ and $\sum_c (c)$ are distribution relations we get

$$n(\theta) = (m-1)/2 - (m-1)/2 = 0.$$

We now may prove the generalized Gauss sum identity.

Let $m \in Z, m \geq 1$. Let $p$ be a rational prime $(p, m) = 1$ and $q$ a power of $p$. Let $\phi$ be a character on $F_q^*$. Let $\psi$ be a character on $F_{q'}^*$, $q' = q^r$, such that $\psi^m = \phi \circ N_{q'/q}$ where $N_{q'/q}$ is the norm from $F_{q'}$ to $F_q$. Moreover let $\psi$ be primitive in the sense that $\psi \neq \psi_1 \circ N_{q'/q''}$ where $q'' = q^s$, $s|r$ and $\psi_1$ is a character on $F_{q''}^*$. If $\psi$ satisfies $\psi^m = \phi \circ N_{q'/q}$ we can always find a primitive character $\psi_1$ associated to it. For if $\psi = \psi_1 \circ N_{q'/q''}$ where $q'' \neq q'$ then $\psi_1^m = \phi \circ N_{q''/q}$ since the norm map is onto and $N_{q'/q} = N_{q'/q''} \circ N_{q''/q}$. So there are $m$ primitive characters $\psi$ such that $\psi^m = \phi \circ N_{q'/q}$. Let $\sigma \in \mathrm{Gal}(F_{q'}/F_q)$. Then if $\psi$ is primitive, so is $\psi^\sigma$ and we consider $\psi$ and $\psi^\sigma$ to be conjugate characters. In the case when $\phi$ is the trivial character on $F_q^*$, we write $\chi$ instead of $\psi$. Then we have

THEOREM (generalized Gauss-sum identity):

$$G(\phi) \prod_{\substack{\chi \neq 1 \\ \chi^m = 1}} G(\chi) = \phi(m) \prod_{\psi} G(\psi)$$

*In the above formula $\chi$ and $\psi$ range over primitive characters in the above sense. Moreover only one character in each orbit of Galois conjugates is taken.*

PROOF: In the case when $\phi = 1$, $G(\phi) = 1$, $\phi(m) = 1$, and the equality is clear. So suppose $\phi \neq 1$. Set $M = q - 1$. Let $\mathfrak{p}$ be a prime in $Q(\mu(M))$ lying above $p \in Q$. Then $\phi = \omega^{a/M(q-1)}$ for some $a \in Z/MZ - (0)$. We now apply the *Generalized Deligne's Theorem, Theorem* 1.6, to the $\theta$ constructed above at the prime $\mathfrak{p}$. We first calculate $\Gamma(\theta)$ using *Proposition* 2.9, the Gauss multiplication formula.

$$\Gamma(\theta) = \prod_{\substack{b \in Q/Z \\ mb = a/M}} \Gamma(\langle b \rangle) \Big/ \Gamma\left(\left\langle \frac{a}{M} \right\rangle\right) \prod_{\substack{c \in Q/Z \\ c \neq 0\ mc = 0}} \Gamma(\langle c \rangle)$$

$$= m^{-(B_1\langle a/M\rangle + \frac{1}{2})} = m^{-\langle a/M \rangle}.$$

We must now calculate $J(\theta)$. Given $b$ such that $mb = a/M$, consider $J_{N(b)}(bN(b), \mathfrak{p})$. Let $D$ be the decomposition group of a prime $\mathfrak{p}'$ of $Q(\mu(N(b)))$ over $\mathfrak{p}$ in $Q(\mu(M))$. Let $q'$ be the

reduction

$$\begin{array}{ccc} Z(\mu(N(b))) & \to & F_{q'} \\ {\scriptstyle G}| & & {\scriptstyle D}| \\ Z(\mu(M)) & \to & F_q \end{array}$$

norm of $\mathfrak{p}'$. Let $\{\sigma\}$ be a set of coset representatives for $G/D$ where $G = \operatorname{Gal} Q(\mu(N(b)))/Q(\mu(M))$. Then $J_{N(b)}(bN(b), \mathfrak{p})$ equals $\prod_\sigma J_{N(b)}(\sigma bN(b), \mathfrak{p}')$.

We first must show that each term $J_{N(b)}(\sigma bN(b), \mathfrak{p}')$ equals $G(\psi)$ where $\psi: F_{q'}^* \to C$ and $\psi$ is primitive, $\psi^m = \phi \circ N_{q'/q}$. We may clearly suppose that $\sigma = 1$ for this. If $\omega$ is the Teichmuller character associated to $\mathfrak{p}'$ then $\psi = \omega^{b(q'-1)}$. Suppose then that $\psi$ is not primitive, $\psi = \psi_1 \circ N_{q'/q''}$ where $q'' = q^s$, $q' = q^r$, $s|r$. Now $q'$ is minimal such that $N(b)|q'-1$. Suppose $\psi_1 = \omega_1{}^{b_1(q''-1)}$ where $b_1(q''-1) \in Z$. Then $\psi = \omega^{b_1(q'-1)}$. Thus $b \equiv b_1 \pmod{Z}$. Thus $b(q''-1) \in Z$, $M|q''-1$ since $M = q-1$. Hence $N(b)|q''-1$ since $N(b)$ is minimal satisfying (1) and (2) above. Hence $q'' = q'$ and $\psi$ is primitive as claimed. Finally $\psi^m = \omega^{mb(q'-1)} = \omega^{a/M(q'-1)} = \phi \circ N_{q'/q}$.

Next we show that the map $\psi: (b, \sigma) \to \psi$ is injective into primitive characters mod Galois conjugation by $D$. We first show that, if $N(b_1)$ and $N(b_2)$ are distinct then the images of $b_1$ and $b_2$ are distinct under $\psi$: For if $N(b_1)$ and $N(b_2)$ are distinct the denominators of $b_1$ and $b_2$ are distinct. But $\psi(b_i, \sigma_i)$ has order equal to the denominator of $b_i$. Therefore the two characters are not in the same orbit under the action of $D$. Hence we may assume that $N(b_1) = N(b_2)$. It clearly suffices also to assume that $\sigma_i = 1$ for $i = 1, 2$. We must show that if $\psi(b_1)$ and $\psi(b_2)$ belong to the same $D$ orbit then $b_1$ and $b_2$ belong to the same $D$ orbit. Let $q'$ be minimal as above such that $N(b_1) = N(b_2)$ divides $q'-1$. Then $\psi(b_i) = \omega^{b_i(q'-1)}$. $\psi(b_1)$ and $\psi(b_2)$ belong to the same $D$ orbit if and only if $\exists t \in Z$ s.t. $(q^t b_1 - b_2)(q'-1) \equiv 0(q'-1)$. But this is equivalent to $q^t b_1 = b_2 \pmod{Z}$. Hence $b_1$ and $b_2$ belong to the same $D$-orbit and $\psi$ is injective. Finally we must show that $\psi$ is onto. Suppose we are given $\psi = \omega^{b(q'-1)}$ with $b \in Q/Z$ and $q' = q^r$ such that $\psi$ is primitive. This means that $q'$ is minimal such that $q'$ is a power of $q$ and $b(q'-1) \in Z$. Then we may choose $N(b)$ minimal such that $M|N(b)$ and $bN(b) \in Z$ as before.

Then $N(b)|q' - 1$ since $M|q' - 1$ and $b(q' - 1) \in Z$. Then $q'$ is the minimal power of $q$ such that $N(b)|q' - 1$ since $bN(b) \in Z$. Hence $\psi(b, 1) = \psi$ which proves that $\psi$ is onto.

In the above argument if a happened to be 0 we would get a map $\chi: (c, \sigma) \to \chi$ which is 1–1 and onto and where $\chi$ is primitive such that $\chi^m = 1$.

We now may calculate $J(\theta)$. By definition

$$J(\theta) = \prod_N \prod_{I_1(N)} J_N(b_i N, \mathfrak{p}) \Big/ J_M(a, \mathfrak{p}) \prod_N \prod_{I_2(N)} J_N(c_i N, \mathfrak{p}).$$

Now by choice of $a$, $J_M(a, \mathfrak{p})$ equals $G(\phi)$. By the above discussion

$$\prod_N \prod_{I_1(N)} J_N(b_i N, \mathfrak{p}) = \prod_\psi G(\psi)$$

$$\prod_N \prod_{I_2(N)} J_N(c_i N, \mathfrak{p}) = \prod_\chi G(\chi)$$

where $\chi$ can be considered to range either over the set $\chi^m = 1$ or the set $\chi^m = 1$, $\chi \neq 1$ since $G(1) = 1$. Hence

$$J(\theta) = \prod_\psi G(\psi) \Big/ G(\phi) \prod_\chi G(\chi).$$

Now applying the generalized Deligne's Theorem we know that $J(\theta)$ equals $\Gamma(\theta)^{\mathrm{Frob}(\mathfrak{p})}/\Gamma(\theta)$.

Now $\Gamma(\theta) = m^{-\langle \frac{a}{M} \rangle}$. So

$$\Gamma(\theta)^{\mathrm{Frob}(\mathfrak{p})}/\Gamma(\theta) = m^{-\frac{a}{M}(N(\mathfrak{p}) - 1)} = m^{-\frac{a}{M}(q - 1)}.$$

But this equals $\phi^{-1}(m)$ by the definition of $\phi$. Hence $J(\theta) = \phi^{-1}(m)$ which completes the proof of the theorem.

Finally we note that this generalized identity has been independently discovered by Greg Anderson in the case that the rational prime $p$ is not 2. His unpublished proof is based directly on Stickelberger's Theorem. Moreover recently Evans has produced some generalizations of Langlands' identities. These are easily seen to be special cases of the generalized identity above as are the Langlands' identities themselves.

For in conclusion we note when $m = l$ a prime, $(l, p) = 1$ we recover the Langlands' identities or the Hasse–Davenport distribution identity with $l$ prime depending on whether $l$ divides $q - 1$ and $\phi$ has order divisible by $l$ in which case we get the Hasse–Davenport distribution identity, or $l$ divides $q - 1$ and $\phi$ does not have order divisible by $l$ in which case we get Langlands' second identity or $l$ does not divide $q - 1$ in which case we get Langlands' first identity.

## REFERENCES


[1] A. WEIL: Jacobi sums as "Grössencharaktere". *Trans. Amer. Math. Soc. 75* (1952) 487–495.

[2] A. WEIL: Sommes de Jacobi et caractères de Hecke. *Nachrich. der Akad. Göttingen* (1974) 1–14.

[3] P. DELIGNE: Valeurs de fonctions L et périodes d'intégrales. *Proceedings of Symposia in Pure Mathematics 33* (1979) 313–346.

[4] P. DELIGNE: Cycles de Hodge sur les varietes abeliennes, preprint.

[5] D. KUBERT: Jacobi sums and Hecke characters, to appear.

[6] H. DAVENPORT and H. HASSE: Die Nullstellen der Kongruenz-zeta funktionen in gewissen zyklischen Fallen. *J. reine angew Math. 172* (1935) 151–182.

[7] S. LICHTENBAUM: Jacobi-sum Hecke characters of imaginary quadratic fields, preprint.

[8] L. AHLFORS: *Complex analysis.* McGraw-Hill, 1953.

[9] S. LANG: *Algebraic number theory.* Addison-Wesley, 1970.

[10] R. LANGLANDS: unpublished manuscript.

[11] B. GROSS and N. KOBLITZ: Gauss sums and the $p$-adic $\Gamma$-function. *Ann. of Math. 109* (1979) 569–581.

[12] G.H. HARDY and E.M. WRIGHT: *An introduction to the theory of numbers*, 4th ed. Oxford University Press, 1960.

[13] I. IWASAWA: Some remarks on Hecke characters. *International Symposium on Algebraic Number Theory*, Kyoto, 1976. S. Iyanaga, ed.

[14] R.J. EVANS: Identities for products of Gauss sums over finite fields. To appear in *L'Enseignement Math.*


(Oblatum 6-I-1982)


D.S. Kubert
Department of Mathematics
University of Pennsylvania
Philadelphia, PA 19104
U.S.A.

S. Lichtenbaum
Department of Mathematics
Cornell University
Ithaca, NY 14853
U.S.A.