COMPOSITIO MATHEMATICA

JAN BRINKHUIS

On a comparison of Gauss sums with products of Lagrange resolvents

Compositio Mathematica, tome 93, n° 2 (1994), p. 155-170

<http://www.numdam.org/item?id=CM_1994__93_2_155_0>

Compositio Mathematica **93**: 155–170, 1994.

On a comparison of Gauss sums with products of Lagrange resolvents

JAN BRINKHUIS

Erasmus Universiteit, Econometrisch Instituut, Postbus 1738, 3000 DR Rotterdam, Netherlands

Received 13 February 1991; accepted in final form 3 August 1993

Introduction

Kronecker's classical determination of the quadratic Gauss sum

$$\sum_{x=1}^{p-1} \left(\frac{x}{p}\right) e^{2\pi i x/p}$$

proceeds by comparison with the expression $\Pi_s(e^{2\pi is/p} - e^{-2\pi is/p})$ where s runs over all odd natural numbers $< p$. The relation is simple: the two numbers are equal. More generally, for a Gauss sum of a character modulo p of order n, there is a natural generalization for the expression above; it is the product of certain cyclotomic integers which arise as Lagrange resolvents. This product is called a norm resolvent. Here the relation is not so simple. A. Fröhlich has found an interpretation for this lack of simplicity: he discovered a connection between the quotients of norm resolvents and Gauss sums, and the relative Galois module structure of the ring of algebraic integers in the cyclotomic field $\mathbb{Q}(e^{2\pi i/p})$ over the subfield K over which $\mathbb{Q}(e^{2\pi i/p})$ has degree n.

In this paper we bring a new object onto the scene and relate it to these quotients and to this Galois module. It is an element of the integral group ring R of a cyclic group of order n, the coefficients of which count certain transversals of the subgroup of order n in the cyclic group $\mathbb{F}_p^*$ or, equivalently, the number of points on certain varieties over the finite field $\mathbb{F}_p$. We fix n and let p vary over all prime numbers $\equiv 1 \bmod n$. If we take this point of view the new object gives an element in the group ring R for each prime $\mathfrak{p}$ of $\mathbb{Q}(e^{2\pi i/n})$ of absolute degree one. This suggests to search for a global object which 'glues them together'. We have made a first step in this direction by defining group ring elements for arbitrary prime ideals in

$\mathbb{Q}(e^{2\pi i/n})$ which are relatively prime to $2n$. Moreover we relate these elements to appropriately defined quotients of 'generalized norm resolvents' and Gauss sums.

A further problem which we consider is whether the quotients of norm resolvents and Gauss sums can sometimes be algebraic units. This problem is suggested by the connection with Galois module structure. Finally we mention that by now there is an extensive literature on the quotients under consideration (for example [F], [G], [H] and [L]) and that for some known results we provide direct proofs.

A. Fröhlich introduced me to these intriguing quotients many years ago. My work on them did not appear in print, but they have been a source of inspiration to me ever since and this has led (sometimes indirectly) to a number of other results which have been published in various papers. It is a great pleasure to thank Ali Fröhlich for all his help, for many stimulating 'Covent Garden discussions' and specially for his non-abating insistence throughout the years that a write-up should be produced. Also I would like to acknowledge many conversations on Galois modules with Adrian Nelson and the helpful comments of Colin Bushnell who read an early draft of this paper.

1. Three objects of study

In this section the three objects of study of this paper are introduced. Let $n \in \mathbb{N}$ be given. Let $\mathbb{Q}^c$ be an algebraic closure of $\mathbb{Q}$, the field of rationals. For each integer d let μ_d be the group of d-th roots of unity in $\mathbb{Q}^c$. Let $\mathfrak{p}$ be a prime of $\mathbb{Q}(\mu_n)$ with $\mathfrak{p} \nmid n$.

1.1 The relation between norm resolvends and Gauss sum elements

Let $Y = \mathbb{Z}[\mu_n]/\mathfrak{p}$ be the residue field of $\mathfrak{p}$. The natural surjection from $\mathbb{Z}[\mu_n]$ to Y maps μ_n injectively to Y. We view μ_n as a subgroup of Y^*, the multiplicative group of Y. The symbols S and T will be used to denote transversals of μ_n in Y^*, that is, S resp. T is a complete set of coset representatives in Y^* of the quotient group Y^*/μ_n. Let $p \in \mathbb{N}$ be the rational prime with $\mathfrak{p} \mid p$. Let $m = \#(Y^*/\mu_n)$, that is, more explicitly, $m = (p^{f(\mathfrak{p}|p)} - 1)/n$ where $f(\mathfrak{p} \mid p)$ is the absolute residue class degree of $\mathfrak{p}$. Let ψ be a canonical additive character on Y, that is, ψ is the composition of the trace map Tr from Y to $\mathbb{Z}/p$ and some isomorphism j from $\mathbb{Z}/p$ to μ_p.

(1.2) Explicitly, if write $\zeta = j(1)$, then $\psi(y) = \zeta^{Try}$ for all $y \in Y$. Let $Z = \mathbb{Z}[\mu_{np}]/\mathfrak{p}\mathbb{Z}[\mu_{np}]$. Again we may view μ_{np} as a subgroup of Z^*, the multiplicative group of Z. For each finite abelian group A and each

commutative ring $\mathscr{R}$ we let $\mathscr{R}A$ denote the group ring of A over $\mathscr{R}$. All group ring elements to be considered in this paper will be inside the ring $\mathbb{Q}^c G$ where $G = T^*$. To begin with, we define the following group ring elements.

$$\tau = \sum_{y \in Y^*} y^{-m} \psi(y)$$

$$\mathscr{N}_S = \prod_{s \in S} \sum_{x \in \mu_n} x^{-1} \psi(sx) \tag{1.3}$$

As elements of μ_{np} belong both to $\mathbb{Q}^c$ and to Z^*, we have to stipulate how these formulas are meant to be read: $y^{-m}\psi(y)$ and $x^{-1}\psi(sx)$ are meant to be elements of Z^*.

We call $\mathscr{N}_S$ a generalized norm resolvend and τ a Gauss sum element for reasons to be explained in Section 2. The relation between $\mathscr{N}_S$ and τ is the first object of study.

1.4 Transversal of μ_n in Y^*.

For each transversal S we let $s(S) \in Y$ be the sum of the elements of S. Let $p(S) \in Y$ be the product of the elements of S. We define the following element in $\mathbb{Z}G$.

$$B = \sum_{\substack{S \\ s(S)=1}} p(S)^{-1} \tag{1.5}$$

For simplicity we do not indicate the dependence of B on the prime p in the notation.

(1.6) Let R be the subring $\mathbb{Z}\mu_n$ of $\mathbb{Q}^c G$. So R is the group ring of μ_n over $\mathbb{Z}$, not to be confused with $\mathbb{Z}[\mu_n]$, the ring of algebraic integers in the cyclotomic field $\mathbb{Q}(\mu_n)$. Clearly, for T a transversal the product $p(T) \cdot B$ lies in R and it does only depend on the choice of T up to a factor from μ_n. This element $p(T) \cdot B$ is the second object of study.

(1.7) REMARKS. Let $T = \{t_1, \ldots, t_m\}$ be a transversal of μ_n in Y^*. The coefficients of B essentially count the number of points on varieties over finite fields. Namely, if we write

$$p(T) \cdot B = \sum_{\xi \in \mu_n} b_\xi \xi^{-1}$$

with $b_\xi \in \mathbb{Z}$ for all $\xi \in \mu_n$, then for each ξ one has, by definition of B, that b_ξ is the number of transversals of μ_n in Y^* with sum 1 and product ξ; that is, it equals n^{-m} times the number of points over the finite field Y of the

affine variety which is defined by the following pair of equations.

$$t_1 X_1^m + \cdots + t_m X_m^m = 1$$
$$X_1^m . \cdots . X_m^m = \xi$$

1.8. Galois modules associated to certain relative cyclotomic field extensions

In the rest of this section we assume moreover that the absolute residue class degree $f(\mathfrak{p} \mid p)$ of $\mathfrak{p}$ equals 1.

Then $m = p - 1/n$. We define the relative extension of number fields N/K by $N = \mathbb{Q}(\zeta)$ with ζ as defined in (1.2) and $[N:K] = n$. Let σ be the isomorphism from $(\mathbb{Z}/p)^*$ to $\mathrm{Gal}(N/\mathbb{Q})$ which is defined by $\zeta^{\sigma(x)} = \zeta^x$ for all $x \in (\mathbb{Z}/p)^*$. We identify μ_n with the Galois group of N/K by the following composition of homomorphisms

$$\mu_n \hookrightarrow Y^* = (\mathbb{Z}/p)^* \xrightarrow{\sigma} \mathrm{Gal}(N/\mathbb{Q}).$$

For each number field F let $\mathcal{O}_F$ be its ring of integers. Now $\mathcal{O}_N$ and its subgroup $\mathcal{O}_K \mu . \zeta$ are by Galois action $\mathbb{Z}\mu_n$-modules and so is the quotient $\mathcal{O}_N/\mathcal{O}_K \mu_n . \zeta$. Its structure is the third object of study. The isomorphism class of this module can be viewed as an element of the Grothendieck group $K_o T(\mathbb{Z}\mu_n)$ of the category of locally freely presented $\mathbb{Z}\mu_n$-modules. This is the category of those modules M for which there exists an exact sequence of $\mathbb{Z}\mu_n$-modules $0 \to P \to Q \to M \to 0$ with P and Q finitely generated, locally free $\mathbb{Z}\mu_n$-modules of the same rank (then M is finite). Details about the functor $K_0 T$ can be found in [T].

2. The relation of $\mathcal{O}_N/\mathcal{O}_K \mu_n . \zeta$ with $\mathcal{N}_S$ and τ

In this section we recall some general fundamental Galois module results from [F] for the special extensions of number fields N/K which we are considering in this paper. We refer in particular to §1(b) of Chapter VI of [F]. In this section we assume, as in (1.8), that the absolute residue class degree of $\mathfrak{p}$ equals 1. Let $V_{\mathbb{Q}}$ be the ring of adeles of $\mathbb{Q}$. Let $A_{\mathbb{Q}}$ be the ring of integral adeles of $\mathbb{Q}$. The inclusion map from μ_p into $\mathbb{Q}^c$ induces a morphism of rings i from $\mathbb{Q}\mu_{np}$ to $\mathbb{Q}^c \mu_n$. For each number $\omega \in N$ we define the element $\mathcal{N}_S^\omega \in \mathbb{Q}^c \mu_n$ by the following expression.

$$\mathcal{N}_S^\omega = \prod_{s \in S} \sum_{x \in \mu_n} \omega^{\sigma(sx)} x^{-1}.$$

We observe that $\mathscr{N}_S^\zeta = i(\mathscr{N}_S)$ with $\mathscr{N}_S$ as defined in (1.3). Let $\hat{\mu}_n$ be the group of all characters of μ_n; we extend each $\chi \in \hat{\mu}_n$ by $\mathbb{Q}$-linearity to a morphism of rings from the group ring $\mathbb{Q}\mu_n$ to the cyclotomic field $\mathbb{Q}(\mu_n)$; we denote this morphism also by χ.

(2.1) THEOREM. (i) *There is a canonical isomorphism* π *from* $K_0T(\mathbb{Z}\mu_n)$ *to the factor group* $(V_{\mathbb{Q}}\mu_n)^*/(A_{\mathbb{Q}}\mu_n)^*$.

(ii) *The element* $i(\tau)$ *is invertible in the ring* $\mathbb{Q}^c\mu_n$ *and for each* ω *in* $\mathcal{O}_N$ *the element* $\mathscr{N}_S^\omega i(\tau)^{-1}$ *is contained in the maximal* $\mathbb{Z}$*-order in the* $\mathbb{Q}$*-algebra* $\mathbb{Q}\mu_n$.

(iii) *For each* $\omega \in \mathcal{O}_N$ *one has that the* $\mathcal{O}_K\mu_n$*-submodule of* $\mathcal{O}_N$ *generated by* ω *is a free module with finite index in* $\mathcal{O}_N$ *iff* $N = K\mu_n.\omega$. *Then this index equals the product of the algebraic integers* $\chi(\mathscr{N}_S^\omega i(\tau)^{-1})$ *where* χ *runs over* $\hat{\mu}_n$. *That is,*

$$\#(\mathcal{O}_N/\mathcal{O}_K\mu_n.\omega) = \prod_{\chi\in\hat{\mu}_n} \chi(\mathscr{N}_S^\omega i(\tau)^{-1}).$$

(iv) *For each* $\omega \in \mathcal{O}_N$ *one has that* $\mathcal{O}_N = \mathcal{O}_K\mu_n.\omega$ *iff* $\mathscr{N}_S^\omega i(\tau)^{-1}$ *is a unit in the maximal order of the* $\mathbb{Q}$*-algebra* $\mathbb{Q}\mu_n$.

(v) *For each* $\omega \in \mathcal{O}_N$ *with* $N = K(\mu_n).\omega$ *the class of the* $\mathbb{Z}\mu_n$*-module* $\mathcal{O}_N/\mathcal{O}_K\mu_n.\omega$ *in* $K_0T(\mathbb{Z}\mu_n)$ *corresponds under the isomorphism* π *of* (i) *to the inverse of the class of the element* $\mathscr{N}_S^\omega i(\tau)^{-1}$ *in* $(V_{\mathbb{Q}}\mu_n)^*/(A_{\mathbb{Q}}\mu_n)^*$.

(2.2) REMARKS. (i) Later we will give a direct proof for (2.1)(ii): see Remark (4.3).

(ii) If $n = 2$, then $\mathcal{O}_N = \mathcal{O}_K\mu_n.\zeta$. See [F] Ch. VI, §1(b) for this and for the relation between this fact and the classical sign determination of the quadratic Gauss sum by Kronecker. For the latter we refer to [B-S] Ch. 5, Sec. 4.3.

(iii) It has been shown that $\mathcal{O}_N \ncong \mathcal{O}_K\mu_n$ as $\mathcal{O}_K\mu_n$-modules if n is an odd prime (see [B] and [Co]). Using the theorem above gives that the element $\mathscr{N}_S^\omega i(\tau)^{-1}$ is not invertible in the maximal $\mathbb{Z}$-order of $\mathbb{Q}\mu_n$.

(iv) The case $n = 4$ will be studied in Section 8.

(v) Our terminology norm resolvend and Gauss sum element for $\mathscr{N}_S$ and τ is inspired by the one generally used in the literature on Galois module theory (see [F1]). One can first apply the map i to these elements and then a character $\chi \in \hat{\mu}_n$. The resulting algebraic number $\chi(i(\mathscr{N}_S)) = \chi(\mathscr{N}_S^\zeta)$ resp. $\chi(i(\tau))$ is precisely the norm resolvent of ω, resp. the Galois Gauss sum, associated to the Galois character on $\mathrm{Gal}(N/K)$ which is defined as the composition of the isomorphism $\mathrm{Gal}(N/K) \simeq \mu_n$ from (1.7) and the character χ. The verification of this fact is straightforward but would take too much space to justify inclusion of it in this paper.

3. On the question whether periods can be algebraic units

In this section we assume again that the residue class degree $f(\mathfrak{p} \mid p)$ equals 1. The trivial character $\varepsilon \in \hat{\mu}_n$ extends by linearity to the augmentation morphism ε from $\mathbb{Z}\mu_n$ to $\mathbb{Z}$. Fröhlich has raised the question whether the rational integer $\varepsilon(i(\mathcal{N}_S)i(\tau)^{-1})$ can be invertible, that is, whether it can be equal to ± 1. We observe that in (2.2)(ii) we have mentioned that the element $i(\mathcal{N}_S)i(\tau)^{-1}$ itself is not invertible in the ring $\mathbb{Z}\mu_n$ if n is an odd prime number. The sum $\Sigma_x \zeta^x$ where x runs over $\mu_n(\mathbb{F}_p)$, the set of n-th roots of unity in the field $\mathbb{F}_p$, is usually called a *period*. The question above amounts to the question whether periods can be algebraic units. Indeed $\Sigma_x \zeta^x = \mathrm{Trace}_{N/K}\zeta$ and

$$\varepsilon(i(\mathcal{N}_S)i(\tau)^{-1}) = \mathrm{Norm}_{K/\mathbb{Q}}\mathrm{Trace}_{N/K}\zeta, \tag{3.1}$$

as is readily verified from the definitions. Now we state our result.

(3.2) THEOREM. *Assume that n is odd.*

(i) *For each prime divisor q of* $\varepsilon(i(\mathcal{N}_S)i(\tau)^{-1})$, *one has* $q \neq p$ *and the least common multiple of n and* $f(q)$, *the order of q* mod *p in* $\mathbb{F}_p^*$, *is a proper divisor of* $p - 1$.

(ii) *There is at least one prime divisor q of* $\varepsilon(i(\mathcal{N}_S)i(\tau)^{-1})$ *for which the class of q* mod *p has odd order in* $\mathbb{F}_p^*$.

In particular $\varepsilon(i(\mathcal{N}_S)i(\tau)^{-1})$ *never equals* ± 1.

Proof. (i) Let q be a prime number dividing $\varepsilon(i(\mathcal{N}_S)i(\tau)^{-1})$. It suffices to prove the following claim: there is more than one prime $\mathfrak{q}$ of K lying above q. Then (i) follows from the equivalence of the following two conditions on a prime number q.

(1) There is more than one prime of K lying above q.

(2) $q \neq p$ and $lcm(n, f) \neq p - 1$.

The laws of factorization of prime numbers in cyclotomic fields are well-known; see for example [Wa] (2.13). It is readily verified that they imply the equivalence of (1) and (2). Finally we argue by contradiction to prove the claim above. Assume that there is only one prime $\mathfrak{q}$ of K lying above q. Then, by (3.1), $\mathfrak{q}$ divides all algebraic conjugates of $\mathrm{Trace}_{N/K}\zeta$. Write $a = \mathrm{Trace}_{N/K}\zeta$. As $\mathcal{O}_N = \mathbb{Z}\mathrm{Gal}(N/\mathbb{Q}).\zeta$ it follows that $\mathcal{O}_K = \mathbb{Z}\mathrm{Gal}(K/\mathbb{Q}).a$. We have now shown that the algebraic conjugates of a form a $\mathbb{Z}$-basis of $\mathcal{O}_K$ and that they are all divisible by $\mathfrak{q}$. This is absurd and so we arrive at the required contradiction. This finishes the proof of (i).

(ii) It suffices to prove the following claim: $v_{\mathfrak{q}}(a) = v_{\bar{\mathfrak{q}}}(a)$ for at least one finite prime $\mathfrak{q}$ of K, where $v_{\mathfrak{q}}$ resp. $v_{\bar{\mathfrak{q}}}$ denotes the valuation corresponding

to $\mathfrak{q}$ resp. $\bar{\mathfrak{q}}$ and where $\bar{\mathfrak{q}}$ denotes the complex conjugate prime of $\mathfrak{q}$. Indeed, then it follows that there exists a finite prime $\mathfrak{q}$ of K with $\mathfrak{q} \neq \bar{\mathfrak{q}}$ and $v_{\mathfrak{q}}(a) \neq 0$. Then (ii) follows from the equivalence of the following two conditions on a prime number $q \neq p$.

(1) Complex conjugation c acts non-trivially on the set of primes of K above q.

(2) The order f of the class of q mod p in $\mathbb{F}_p^*$ is odd.

Again, this equivalence can be derived from [Wa] (2.13).

Finally we argue by contradiction to prove the claim above. Assume that $v_{\mathfrak{q}}(a) = v_{\bar{\mathfrak{q}}}(a)$ for each finite prime $\mathfrak{q}$ of K. Then $v_{\mathfrak{q}}(a\bar{a}^{-1}) = 0$ for each finite prime $\mathfrak{q}$ of K. It follows that $a\bar{a}^{-1}$ is an algebraic unit of absolute value 1 in the abelian extension K of $\mathbb{Q}$. It is well-known that this implies that $a\bar{a}^{-1}$ is a root of unity, so, as $\mu_K = \{\pm 1\}$, $a = \pm \bar{a}$. On the other hand, we have seen in the proof of (i) that implies $\mathcal{O}_K = \mathbb{Z}\mathrm{Gal}(K/\mathbb{Q}).a$, so the algebraic conjugates of a form a basis of the imaginary abelian field K, seen as a vector space over $\mathbb{Q}$. This contradicts $a = \pm \bar{a}$. This finishes the proof of the theorem. □

The assumption that n is odd in Theorem (3.2) cannot be omitted, as the case $\chi = \varepsilon$ of the following proposition shows.

(3.3) PROPOSITION. *If* $n = 4$, *then* $\chi(i(\mathcal{N}_S)i(\tau)^{-1}) = \pm 1$ *for each of the two* $\chi \in \mu_n$ *for which* $\chi^2 = \varepsilon$.

This result follows immediately from the following easy lemma together with the fact that if χ has order 2, the number $\chi(i(\tau))$ is the quadratic Gauss sum and so has absolute value $\sqrt{p}$. Let h mod p be a root of $X^2 + 1 = 0$ in $\mathbb{F}_p$.

(3.4) LEMMA.

(i) $\zeta + \zeta^h + \zeta^{h^2} + \zeta^{h^3} = (\zeta^{(1+h)/2} + \zeta^{(-1+h)/2})(\zeta^{(1-h)/2} + \zeta^{(-1-h)/2})$

(ii) $\zeta - \zeta^h + \zeta^{h^2} - \zeta^{h^3} = (\zeta^{(1+h)/2} - \zeta^{(-1+h)/2})(\zeta^{(1-h)/2} - \zeta^{(-1-h)/2})$

(iii) $$\frac{1+h}{2}(1, h, h^2, h^3) = \left(\frac{1+h}{2}, -\frac{1-h}{2}, -\frac{1+h}{2}, -\frac{1-h}{2}\right)$$

(iv) *If* T *is a transversal of* $\mu_2(\mathbb{F}_p^*)$ *in* $\mathbb{F}_p^*$, *then*

$$\prod_{t \in T} (\zeta^t + \zeta^{-t}) = \pm 1 \text{ and } \prod_{t \in T} (\zeta^t - \zeta^{-t}) = \pm \sqrt{\left(\frac{-1}{p}\right)p}.$$

4. On the relation of B with $\mathcal{N}_S$ and τ

The aim of this section is to establish the following formula in the group ring $\mathbb{Z}Z^*$ and some consequences of it. This section is without the assumption $f(\mathfrak{p} \mid p) = 1$.

(4.1) FORMULA.

$$p(S)^{-1}\mathcal{N}_S = \left[\sum_{\substack{T \\ s(T)=0}} p(T)^{-1} \right] + \tau . B$$

Proof.

$$p(S)^{-1}\mathcal{N}_S = \prod_{s \in S} \sum_{x \in \mu_n} (sx)^{-1}\psi(sx)$$

(on multiplying out and on using that S is a transversal of μ_n in Y^*)

$$= \sum_T p(T)^{-1}\psi(s(T))$$

(as for each $y \in Y^*$ multiplication by y induces a bijection from the set of transversals T with $s(T) = 1$ to the set of transversals T with $s(T) = y$)

$$= \sum_{\substack{T \\ s(T)=0}} p(T)^{-1} + \sum_{y \in Y^*} \sum_{\substack{T \\ s(T)=1}} (y^m p(T))^{-1}\psi(y)$$

$$= \sum_{\substack{T \\ s(T)=0}} p(T)^{-1} + \tau . B. \qquad \square$$

Let $c \in \mathbb{Z}C^*$ be the formal sum of the elements of μ_n.

(4.2) COROLLARY. *The following relation holds between the elements $i(\mathcal{N}_S)$, $i(\tau)$, $p(S) . B$ and c of the group ring $\mathbb{Q}^c\mu_n$.*

$$i(\mathcal{N}_S) = i(\tau)[(p(S)B)\ (1 + mc) - n^{m-1}c]$$

(4.3) REMARK. This corollary gives an explicit proof of statement (ii) of Theorem (2.1) in the case $\omega = \zeta$. In fact it gives a slightly stronger result: the element $i(\mathcal{N}_S)i(\tau)^{-1}$ lies in the integral group ring $R = \mathbb{Z}\mu_n$. Namely c lies in

$\mathbb{Z}\mu_n$ by definition and we have already pointed out, in (1.6), that $p(S) \cdot B$ lies in $\mathbb{Z}\mu_n$.

Proof of Corollary (4.2). Applying to formula (4.1) the homomorphism from $\mathbb{Z}\mu_p \times Y^*$ to $\mathbb{Z}Y^*$ which is induced by the projection map from $\mu_p \times Y^*$ to Y^*, one gets the following formula

$$p(S)^{-1}c^m = \sum_{\substack{T \\ s(T)=0}} p(T)^{-1} + mc \cdot \sum_{\substack{T \\ s(T)=0}} p(T)^{-1} \tag{4.4}$$

Combining (4.1) and (4.4) to eliminate the expression $\Sigma_{\substack{T \\ s(T)=0}} p(T)^{-1}$, one gets the following formula (taking into account that $c^m = n^{m-1}c$).

$$\mathcal{N}_S - n^{m-1}c = (\tau - mc) \cdot (p(S)B) \tag{4.5}$$

Applying the morphism i to formula (4.5) and using the following identity

$$c \cdot (1 + i(\tau)) = 0 \tag{4.6}$$

one gets the formula in the statement of the corollary. It remains to verify (4.6). We do this 'componentwise'. Let for each character χ of μ_n, the projection of $\mathbb{Q}^c\mu_n$ to the component $\mathbb{Q}^c$ of $\mathbb{Q}^c\mu_n$ which corresponds to χ, also be denoted by χ. We have to verify that for each χ either $\chi(c) = 0$ or $1 + \chi(i(\tau)) = 0$. If χ is non-trivial, then clearly $\chi(c) = 0$. If χ is the trivial character ε, then

$$1 + \chi(i(\tau)) = 1 + \sum_{y \in Y^*} i\psi(y) = \sum_{y \in Y} i\psi(y).$$

Now, by the surjectivity of the trace map from Y to $\mathbb{F}_p$, the homomorphism $i\psi$ from Y to μ_p is surjective; combining this with the fact that the sum in $\mathbb{Q}^c$ of μ_p is zero, its follows that $\Sigma_{y \in Y} i\psi(y)$ is zero. This finishes the proof of Corollary (4.2). □

Finally we record for later use the following formulas which follow from formula (4.1) by applying suitable characters of μ_{np} to it.

(4.7) COROLLARY.

(i) $n^m = \#\{T \mid s(T) = 0\} + \#(Y^*) \cdot \varepsilon(B)$

(ii) $\prod_{s \in S} \sum_{x \in \mu_n} \zeta^{Tr(xs)} = \#\{T \mid s(T) = 0\} - \varepsilon(B)$

where Tr denotes the trace map from Y to $\mathbb{F}_p$.

5. The relation of Jacobi sums with $\mathcal{N}_S$ and τ

For each character ϕ of Y^* its Gauss sum is defined by

$$\tau(\phi) = \sum_{z \in Y^*} \phi(z)^{-1} i\psi(z). \tag{5.1}$$

For each $k \in \mathbb{N}$ and for each choice $\phi_1, \ldots, \phi_k$ of k characters of Y^* one defines the following number

$$J(\phi_1, \ldots, \phi_k) = \tau(\phi_1), \ldots, \tau(\phi_k).\tau(\phi_1, \ldots, \phi_k)^{-1}. \tag{5.2}$$

This number is called a Jacobi sum; the study of Jacobi sums has a long history (see A. Weil's paper [We]). An easy property is that $J(\phi_1, \ldots, \phi_k)$ is an algebraic integer in the cyclotomic field generated by the values of the characters $\phi_j (1 \leqslant j \leqslant k)$.

(5.3) For each character χ of μ_n, let $\chi_1, \ldots, \chi_m$ be the characters of Y^* which extend χ, ordered in some way.

(5.4) THEOREM. *For each character χ of μ_n the following formula holds*

$$\chi(i(\mathcal{N}_S) i(\tau)^{-1}) = m^{-m} \sum_{(j_1, \ldots, j_m)} \chi_{j_1}(s) \ldots \chi_{j_m}(s_m) J(\chi_{j_1}, \ldots, \chi_{j_m}) \tag{5.5}$$

where the summation is only carried out over those m-tuples $(j_1, \ldots, j_m)$ for which $\chi_{j_1}(z) \ldots \chi_{j_m}(z) = \chi(z^m)$ for all $z \in Y^*$.

To prove this result we need the following formula

(5.6) LEMMA.

$$\sum_{x \in \mu_n} \chi(x)^{-1} i\psi(sx) = m^{-1} \sum_{j=1}^{m} \chi_j(s) \tau(\chi_j)$$

for each $s \in Y^*$ and all characters χ of μ_n.

Proof.

$$\begin{aligned} & m^{-1} \sum_{j=1}^{m} \chi_j(s) \tau(\chi_j) \\ & = m^{-1} \sum_{j=1}^{m} \chi_j(s) \sum_{z \in Y^*} \chi_j(z)^{-1} i\psi(z) \\ & = m^{-1} \sum_{z \in Y^*} i\psi(z) \sum_{j=1}^{m} \chi_j(zs^{-1}) \\ & = (\text{set } x = zs^{-1}) \end{aligned}$$

$$= m^{-1} \sum_{x \in Y^*} i\psi(xs) \sum_{j=1}^{m} \chi_j(x)^{-1}$$

(using that the inner sum equals $m\chi(x)^{-1}$ if $x \in \mu_n$ and that it equals zero otherwise)

$$= \sum_{x \in \mu_n} \chi(x)^{-1} i\psi(xs). \qquad \square$$

Moreover we need the following fact.

(5.7) LEMMA. *If the product* $\chi_{j_1}, \ldots, \chi_{j_m}$ *is not the character* $z \to \chi(z^m)$, *then the number*

$$u = \sum_{\rho} \chi_{j_{\rho(1)}}(s_1), \ldots, \chi_{j_{\rho(m)}}(s_m)$$

is zero, where ρ *runs over all permutations of the set* $\{1, \ldots, m\}$.

Proof. For the proof we may assume that χ is the trivial character on μ_n (for example by replacing χ_{j_1} by $\chi_{j_1}\chi_1^{-1}$, χ_{j_2} by $\chi_{j_2}\chi_1^{-1}$, etc.). Then u clearly does not depend on the choice of S. Moreover the assumption of the lemma amounts then to the following one: there is an element $x \in Y^*$ with

$$(\chi_{j_1} \ldots \chi_{j_m})(x) \neq 1.$$

Multiplying u with $(\chi_{j_1}. \ldots . \chi_{j_m})(x)$ one gets

$$\sum_{\rho} \chi_{j_{\rho(1)}}(xs_1). \ldots . \chi_{j_{\rho(m)}}(xs_m) \tag{5.8}$$

where again ρ runs over all permutations of the set $\{1, \ldots, m\}$. Clearly $\{xs_1, \ldots, xs_m\}$ is again a transversal of μ_n in Y^*, so the expression (5.8) is equal to u, by the independence of u on the choice of transversals. It follows that $u = 0$, as required. $\square$

(5.9) REMARK. If the product of $\chi_{j_1}, \ldots, \chi_{j_m}$ is the character $z \to \chi(z^m)$, then $\tau(\chi_{j_1}. \ldots . \chi_{j_m}) = \chi(i(\tau))$ by the definitions, where τ is the Gauss sum element defined in Section 1.

(5.10) *Proof of Theorem* (5.4).

$$\chi(i(\mathcal{N}_S)) = \prod_{s \in S} \sum_{x \in \mu_n} \chi(x)^{-1} i\psi(sx) = \prod_{s \in S} m^{-1} \sum_{j=1}^{m} \chi(s)\tau(\chi_j)$$

$$= m^{-m} \sum_{(j_1, \ldots, j_m)} \chi_{j_1}(s_1). \ldots . \chi_{j_m}(s_m)\tau(\chi_{j_1}). \ldots . \tau(\chi_{j_m})$$

where $(j_1,\ldots,j_m)$ runs over all m-tuples of elements of the set $\{1,\ldots,m\}$. Finaly one uses Lemma (5.7), Remark (5.9) and Definition (5.2) to finish the proof. □

(5.11) REMARK. One can simplify the expression in Theorem (5.4) by taking all terms together for which the sequence $j_1,\ldots,j_m$ is the same up to permutation: these sequences give rise to the same Jacobi sums. The coefficients of the Jacobi sums in the resulting expression are then rational integers.

6. On the counting of transversals

We recall our convention that the variable T runs over transversals of μ_n in Y^*. In this section we compare the numbers $b_0 = \#\{T|s(T) = 0\}$ and $b_1 = \#\{T|s(T) = 1\}$. We observe that the right hand side of the equality in Corollary (4.7) (ii) can be written as $b_0 - b_1$. We write

$q = \#Y$, that is, $q = p^{f(\mathfrak{p}|p)}$.

(6.1) PROPOSITION.
(i) $b_0 - b_1 < m^{-1}q^{m/2}$
(ii) $b_0 - b_1 \equiv n^m \bmod p$
(iii) *If n is odd, then* $b_0 - b_1 > 0$.

(6.2) REMARK. In particular we get the following easy to state result: for each odd order subgroup of the multiplicative group of a finite field there are more transversals with sum zero than with sum one.

(6.3) REMARK. Knowing $b_0 - b_1$ amounts to knowing $\varepsilon(B) = b_1$. Namely, by Corollary (4.7)(i) one has $n^m = b_0 + \#(Y^*).b_1$.

Proof of Proposition (6.1). (i) Combining Corollary (4.7)(ii) with formula (5.5) for the case $\chi = \varepsilon$ and using the estimate $|J| \leqslant q^{m/2}$, which results from the fact that $|\tau(\chi)| = q^{1/2}$, one gets immediately the estimation $|b_0 - b_1| < m^{-m}.m^{m-1}q^{m/2} = m^{-1}q^{m/2}$.

(ii) By Corollary (4.7)(i) and by the congruence $\#(Y^*) \equiv -1 \bmod p$ one gets $b_0 - b_1 \equiv n^m \bmod p$.

(iii) Assume that n is odd. First we prove that for any s the sum $\Sigma_{x\in\mu_n}\zeta^{Tr(xs)}$ is not zero. The only $\mathbb{Q}$-linear relation of the p-th roots of unity is, up to scalars from $\mathbb{Q}$, the relation $\Sigma_{j=0}^{p-1}\zeta^j$; there are p terms in it and our sum consists of n terms and p does not divide n. Therefore $\Sigma_{x\in\mu_n}\zeta^{Tr(xs)} \neq 0$.

Now as n is odd, $-1 \notin \mu_n$, so for each coset R of μ_n in $Y^* = \mathbb{F}_q^*$ the cosets

R and $-R$ are different. Therefore one can pair the factors in the product $\Pi_{s\in S}\,\Sigma_{x\in\mu_n}\,\zeta^{Tr(xs)}$ into pairs of complex conjugate numbers; so this expression is a non-negative real number, and so it is even a positive real number, as all its factors are $\neq 0$, as we have seen above. By Corollary (4.7) (ii) this finishes the proof of statement (iii). □

7. The determination of the quotient of $i(\mathcal{N}_S)$ and $i(\tau)$ modulo p

In this section we assume again that the prime $\mathfrak{p}$ is of degree one over p. Let χ be the identity map on μ_n, viewed as a primitive character of μ_n. For each $j\in(\mathbb{Z}/n)^*$ let $\sigma_j\in \mathrm{Gal}(\mathbb{Q}(\mu_{np})/\mathbb{Q}(\mu_p))$ be defined by $\sigma_j(\xi)=\xi^j$ for all $\xi\in\mu_n$. Let for each $t\in\mathbb{R}$ the number $\{t\}$ be defined by $0\leqslant\{t\}<1$ and $t-\{t\}\in\mathbb{Z}$. Let $\mathfrak{B}$ be the unique prime ideal of $\mathbb{Q}(\mu_{np})$ above the chosen prime $\mathfrak{p}$.

(7.1) PROPOSITION. *The following congruences hold*

$$\chi^k(i(\mathcal{N}_S)i(\tau)^{-1}) \equiv -n^m(mh)!\,h!^{-m}p(S)^h \bmod \sigma_j^{-1}(\mathfrak{B})$$

for all $j\in(\mathbb{Z}/n)^*$ and all $k\in\mathbb{Z}/n$, where h is defined to be $n\{kj/n\}$. In particular $\chi^k(i(\mathcal{N}_S)i(\tau)^{-1})$ is always a p-unit.

Proof. We embed $\mathbb{Q}(\mu_{np})$ in $\mathbb{Q}_p^c$, an algebraic closure of $\mathbb{Q}_p$, the field of p-adic rationals, by the embedding which corresponds to the prime $\mathfrak{B}$. Let ζ be the p-th root of unity for which $i\psi(x)=\zeta^x$ for all $x\in Y=\mathbb{F}_p$. Now we are going to determine the leading parts of the local expansions of $\chi^k i(\mathcal{N}_S)$ and $\chi^k i(\tau)$ at the primes above p. To begin with

$$\left[\sum_{x\in\mu_n}\chi(x)^{-k}\,i\psi(sx)\right]^{\sigma_j}=\sum_{x\in\mu_n}x^{-kj}\zeta^{sx}$$

(writing $\zeta=1+(\zeta-1)$ and expanding by Newton's binomium)

$$=\sum_x\sum_{r=0}^{\infty}\binom{sx}{r}(\zeta-1)^r x^{-kj}=\sum_{r=0}^{\infty}(\zeta-1)^r\sum_{x\in\mu_n}\binom{sx}{r}x^{-kj}. \qquad (*)$$

Using that $\binom{sx}{r}$ is a polynomial in x of degree r and that $\Sigma_{x\in\mu_n}x^t=n$ if $t\equiv 0 \bmod n$ and $=0$ otherwise, one concludes that in the expression above the smallest $r\in\mathbb{R}$ for which

$$\sum_{x\in\mu_n}\binom{sx}{r}x^{-kj},\ \text{the coefficient of } (\zeta-1)^r,\ \text{is non-zero, is } r=n\left\{\frac{kj}{n}\right\}.$$

It follows that

$$(*) \equiv \left(n\left\{\frac{kj}{n}\right\}\right)!^{-1} s^{n\{kj/n\}} n(\zeta - 1)^{n\{kj/n\}} \bmod \mathscr{B}^{n\{kj/n\}+1}.$$

Therefore

$$(\chi^k(i(\mathscr{N}_S)))^{\sigma_j} \equiv n^m \left(n\left\{\frac{kj}{n}\right\}\right)!^{-m} p(S)^{n\{kj/n\}} (\zeta - 1)^{mn\{kj/n\}} \bmod \mathscr{B}^{mn\{kj/n\}+1}.$$

This implies that

$$\chi^k(i(\mathscr{N}_S)) \equiv n^m \left(n\left\{\frac{kj}{n}\right\}\right)!^{-m} p(S)^{n\{kj/n\}} (\zeta - 1)^{mn\{kj/n\}} \bmod \mathscr{B}^{mn\{kj/n\}+1}. \quad (7.2)$$

Expanding the Gauss sum $\chi^k(i(\tau))$ in a similar way one gets

$$\chi^k(i(\tau)) \equiv -\left(\left\{\frac{kj}{n}\right\}(p-1)\right)!^{-1} (\zeta - 1)^{\{kj/n\}(p-1)} \bmod \sigma_j^{-1}(\mathscr{B})^{\{kj/n\}(p-1)}. \quad (7.3)$$

Combining (7.2) and (7.3) one gets the congruence in the statement of Proposition (7.1). □

(7.4) REMARK. Alternatively one can derive that the numbers $\chi^k(i(\mathscr{N}_S)i(\tau)^{-1})$ are p-units from the fact that ζ generates a local normal integral basis of N/K at the prime p. (See the last statement on p. 221 of [F1]).

(7.5) REMARK. Proposition (7.1) determines the element $i(\mathscr{N}_S)i(\tau)^{-1}$ in the group ring $\mathbb{Z}\mu_n$ modulo p.

A special case of the congruence of the proposition is the following one which is the core of Kronecker's sign determination of the quadratic Gauss sum.

(7.6) COROLLARY.

$$\left(\sum_{k=1}^{p-1} \left(\frac{k}{p}\right)\zeta^k\right)^{-1} \prod_{j=1}^{(p-1)/2} (\zeta^{2j-1} - \zeta^{-(2j-1)}) \equiv 1 \bmod p.$$

Proof. One has to apply Proposition (7.1) with $n = 2$ and with S the set of the classes modulo p of the odd numbers $1, 3, 5, \ldots, p-2$. Then the left-hand side of the congruence of Proposition (7.1) specializes to the left-hand side of the congruence (7.7). The right-hand side of the congruence of Proposition (7.1) specializes to

$$-2^{(p-1)/2}(1.3.5.\ldots.p-2).\left(\frac{p-1}{2}\right)!$$

$$\equiv -(1.3.5.\ldots.(p-2)).(2.4.6.\ldots.(p-2))$$

$$\equiv -(p-1)! \equiv 1 \bmod p.$$

This finishes the proof. □

8. The case $n = 4$

In this section we prove the following result.

(8.1) PROPOSITION. *Let $n = 4$ and assume that $\wp$ is of degree one over p. For each $\omega \in \mathcal{O}_N$ and each primitive character χ of μ_n the following inequality holds for the algebraic integer $\chi(\mathcal{N}_S^{\omega} i(\tau)^{-1})$ in the Gaussian field $\mathbb{Q}(i)$*

$$|\chi(\mathcal{N}_S^{\omega} i(\tau)^{-1})|^2 \geqslant 2^m p^{-1/2} \left| \mathrm{Norm}_{N^+/\mathbb{Q}} \frac{\omega - \bar{\omega}}{\zeta - \bar{\zeta}} \right|$$

where N^+ is the real subfield of N and where the superscript $^-$ denotes complex conjugation. Moreover if $\omega \neq \bar{\omega}$, then

$$|\chi(\mathcal{N}_S^{\omega} i(\tau)^{-1})|^2 \geqslant 2^m p^{-1/2}.$$

The motivation to search for this inequality is that it has the following Galois module theoretic consequence which follows using Proposition (2.1).

(8.2) COROLLARY. *If p is a prime number $\equiv 1 \bmod 4$. Then $N = \mathbb{Q}(\mu_p)$ has no normal integral basis over the subfield K with $[N:K] = 4$.*

Proof of (8.1). Let $h \bmod p$ be a generator of $\mu_4(\mathbb{F}_p)$ and write $i = \chi(h \bmod p)$. Then $i^2 = -1$. We simplify notation by denoting for each $\omega \in \mathcal{O}_N$ and each $s \in \mathbb{F}_p^*$ the result of hitting ω by the field automorphism of $N = \mathbb{Q}(\mu_p)$ which raises p-th roots of unity to the power s by ω^s. For each $s \in S$

$$\chi(\mathcal{N}_S^{\omega}) = \prod_{s \in S} (\omega^s + \omega^{sh} i + \omega^{sh^2} i^2 + \omega^{sh^3} i^3)$$

$$= \prod_{s \in S} (\omega^s - \overline{\omega^s}) + i(\omega^{sh} - \overline{\omega^{sh}}).$$

Therefore, as $z - \bar{z}$ is totally imaginary

$$
\begin{aligned}
|\chi(\mathcal{N}_S^{\omega})|^2 &= \prod_{s\in S} (|\omega^s - \overline{\omega^s}|^2 + |\omega^{sh} - \overline{\omega^{sh}}|^2) \\
&\geq \prod_{s\in S} 2|\omega^s - \overline{\omega^s}\|\omega^{sh} - \overline{\omega^{sh}}| \\
&= 2^m\sqrt{p}\left|\prod_{s\in S}\left(\frac{\omega^s - \overline{\omega^s}}{\zeta^s - \overline{\zeta^s}}\cdot\frac{\omega^{sh} - \overline{\omega^{sh}}}{\zeta^{sh} - \overline{\zeta^{sh}}}\right)\right| \\
&= 2^m\sqrt{p}\left|\operatorname{Norm}_{N^+/\mathbb{Q}}\frac{\omega - \bar{\omega}}{\zeta - \overline{\zeta}}\right|.
\end{aligned}
$$

Using moreover the fact that Gauss sums have absolute value $\sqrt{p}$, so $|\chi(i(\tau))| = \sqrt{p}$, one gets the first inequality in the statement of the proposition. The proof of the proposition is finished by the remark that

$$\frac{\omega - \bar{\omega}}{\zeta - \overline{\zeta}} \in \mathcal{O}_{N^+}$$

and that, as a consequence

$$\left|\operatorname{Norm}_{N^+/\mathbb{Q}}\left(\frac{\omega - \bar{\omega}}{\zeta - \overline{\zeta}}\right)\right| \geqslant 1 \quad \text{if } \omega \neq \bar{\omega}. \qquad \square$$

(8.3) REMARK. The requirement in Proposition (8.1) that χ is primitive is essential. See Proposition (3.3).

References

[B] Brinkhuis, J., Normal integral bases and complex conjugation, *J. Reine angew. Math.* 375/376 (1987), 157–166.

[B-S] Borevich, Z and Shafarevich, I., *Number Theory*, Academic Press: London and New York, 1966.

[C] Cougnard, J., Quelques extension modérément ramifiées sans base normale, *J. London Math. Soc.* 31 (1985), 200–204.

[F] Fröhlich, A., Galois module structure of algebraic integers, *Ergebnisse Math.* Vol. 1, Springer 1983.

[G] Greither, C., Relative integral normal bases in $\mathbb{Q}(\zeta_p)$, *J. Number Theory*, Vol. 35, No. 2 (1990), 180–193.

[H] Hellegouarch, Y. et Toffin, P., Nombres exceptionnels attachés aux corps cyclotomiques, *Séminaire de théorie des Nombres de l'Université de Caen (1987–1989), Exposé IV.*

[L] Loxton, J. H., Products related to Gauss sums, *J. Reine angew. Math.* 268/269 (1974), 53–67.

[T] Taylor, M., Classgroups of group rings, *LMS Lecture Notes Series* 91 (1984).

[Wa] Washington, L. C., *Introduction to Cyclotomic Fields*, Graduate texts in Math. 83 (1980).

[We] Weil, A., Sommes de Jacobi et caractères de Hecke, *Collected papers, Volume III*, 329–342 (1980).