

Gauss sums and Poincaré sums (a sketch)

By Takashi Ono

Department of Mathematics, The Johns Hopkins University, Baltimore, Maryland, 21218, U.S.A.

May 28, 2006

Abstract: colors but no sound

Key Words: Indra's Pearls

1 $(\mathfrak{g}, (G, M))$

Let G be a group and M be a left G -module. Consider a *finite* group \mathfrak{g} which acts naturally on (G, M) . In other words, we assume that G is a left \mathfrak{g} -group, M is a left \mathfrak{g} -module so that $\sigma(sx) = \sigma s^\sigma x$, $\sigma \in \mathfrak{g}, s \in G, x \in M$. Let c be a cocycle of \mathfrak{g} in G . By definition, c is a map $\mathfrak{g} \rightarrow G$ such that $c(\sigma\tau) = c(\sigma)^\sigma c(\tau)$, $\sigma, \tau \in \mathfrak{g}$. For a cocycle c , we associate a \mathbf{Z} -module M_c by

$$M_c = \{x \in M; c(\sigma)^\sigma x = x, \sigma \in \mathfrak{g}\}. \quad (1)$$

As the group \mathfrak{g} is finite, we can speak of a sum

$$p_c(x) = \sum_{\tau \in \mathfrak{g}} c(\tau)^\tau x, \quad x \in M. \quad (2)$$

We shall put

$$P_c = \{y = p_c(x), x \in M\}. \quad (3)$$

One verifies that

$$|\mathfrak{g}|M_c \subseteq P_c \subseteq M_c \quad (4)$$

⁰2000 Mathematics Subject Classification. 11R34

Dedicated to Professor S. Iyanaga, M.J.A., on his 100th birthday

where $|\mathfrak{g}|$ is the order of \mathfrak{g} . Denote by $Z(\mathfrak{g}, G)$ the set of all cocycles of \mathfrak{g} in G . Two cocycles c, c' are equivalent $c' \sim c$ if there is a $u \in G$ such that $c'(\sigma) = u^{-1}c(\sigma) \sigma u$ for some $u \in G$ for all $\sigma \in \mathfrak{g}$. One verifies that the map $x \mapsto u^{-1}x$ induces an isomorphism of factor modules : $M_c/P_c \simeq M_{c'}/P_{c'}$. Consequently the structure of the module M_c/P_c depends only on the cohomology class $\gamma = [c]$ in the (1st) cohomology set $H^1(\mathfrak{g}, G) = Z(\mathfrak{g}, G)/\sim$. If we put $c = 1$ in (1),(3), then we have

$$M_1 = M^{\mathfrak{g}}, \quad P_1 = N(M)$$

and so

$$M_1/P_1 = \hat{H}^0(\mathfrak{g}, M).$$

For a general $\gamma = [c] \in H^1(\mathfrak{g}, G)$, we have a right to make identification

$$M_c/P_c = \hat{H}^0(\mathfrak{g}, M)_{\gamma}, \tag{5}$$

the Tate group *twisted* by γ .

In view of (5) we shall put

$$i_{\gamma}(\mathfrak{g}, M) = [M_c : P_c], \quad \gamma = [c] \in H^1(\mathfrak{g}, G). \tag{6}$$

The determination of the *index* $i_{\gamma}(\mathfrak{g}, M)$ is our basic theme inspired by Poincaré.

In the next three sections we shall review classical cases from our view point.

2 Gauss sums

Let l be an odd prime, $\zeta = e^{\frac{2\pi i}{l}}$ and $K = \mathbf{Q}(\zeta)$, the l -th cyclotomic field. Denote by \mathcal{O} the ring of integers of K . In accordance with notation in **1**, we set

$$M = \mathcal{O}^+, \quad G = \mathcal{O}^{\times}, \quad \mathfrak{g} = \text{Gal}(K/\mathbf{Q})$$

One knows that

$$M = \mathbf{Z}[\zeta] \simeq \mathbf{Z}^{l-1}, \quad \mathfrak{g} \simeq \mathbf{F}_l^{\times}. \tag{7}$$

Note that one can think of $\sigma \in \mathfrak{g}$ as an element of \mathbf{Z} by the the reciprocity map in the second isomorphism in (7). Let us look at two famous cocycles

$c \in Z(\mathfrak{g}, G)$.

(A) The *circular units* $c(\sigma) = \frac{1-\zeta^\sigma}{1-\zeta}$ form a cocycle. For this we have

$$M_c = \frac{l}{1-\zeta} \mathbf{Z} = P_c, \quad \text{hence } i_\gamma(\mathfrak{g}, M) = 1 \quad (8)$$

(B) The *Legendre character* $c(\sigma) = \left(\frac{\sigma}{l}\right)$ can be thought as a cocycle (actually a homomorphism) of \mathfrak{g} in G . For this we have

$$M_c = \mathbf{Z}\tau = P_c, \quad \text{hence } i_\gamma(\mathfrak{g}, M) = 1 \quad (9)$$

where

$$\tau = \sum_{t=0}^{l-1} \left(\frac{t}{l}\right) \zeta^t,$$

the classical Gauss sum.

3 Theta series

For a point τ in the upper half plane, let $L_\tau = \mathbf{Z} + \mathbf{Z}\tau$ and $E_\tau = \mathbf{C}/L_\tau$, the elliptic curve over \mathbf{C} . Let \mathcal{O} be the ring of entire functions. In accordance with notation in **1**, we set

$$M = \mathcal{O}^+, \quad G = \mathcal{O}^\times, \quad \mathfrak{g} = \pi_1(E_\tau) \simeq L_\tau.$$

Note that one can think of $\sigma \in \mathfrak{g}$ as $\sigma = m + n\tau$, $m, n \in \mathbf{Z}$. Let us look at the following cocycle

$$c(\sigma)(z) = \mathbf{e}\left(\frac{\tau n^2}{2} - nz\right). \quad (10)$$

For this we have

$$M_c = \mathbf{C}\vartheta_3 = P_c^*, \quad \text{hence } i_\gamma(\mathfrak{g}, M) = 1 \quad (11)$$

where

$$\vartheta_3 = \sum_{n \in \mathbf{Z}} c(n\tau)(z).$$

the Jacobi theta series.

4 Poincaré series

This time, let \mathcal{O} be the ring of holomorphic functions on the upper half plane. In accordance with notation in **1**, we set

$$M = \mathcal{O}^+, \quad G = \mathcal{O}^\times, \quad \mathfrak{g} = SL_2(\mathbf{Z})$$

where for $x = x(z) \in \mathcal{O}$ the group \mathfrak{g} acts by the rule

$${}^\sigma x(z) = x(\sigma^{-1}z) = x\left(\frac{az+b}{cz+d}\right), \quad (12)$$

where $\sigma^{-1} = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$.

For the cocycle $c(\sigma)(z) = \frac{1}{(cz+d)^4}$ we have

$$M_c = \left\{ x \in M; x\left(\frac{az+b}{cz+d}\right) = (cz+d)^4 x(z), \quad \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in SL_2(\mathbf{Z}) \right\} \quad (13)$$

and

$$M_c = \mathbf{C}G_2 = P_c^*, \quad \text{hence} \quad i_\gamma(\mathfrak{g}, M) = 1, \quad (14)$$

where

$$G_2(z) = \sum_{(m,n) \neq (0,0)} \frac{1}{(mz+n)^4}$$

the Eisenstein series of weight 4.

5 Real quadratic fields

Let $K = \mathbf{C}(\sqrt{d})$ be a real quadratic field and \mathcal{O} be the ring of integers of K . In accordance with notation in **1**, we set

$$M = \mathcal{O}^+, \quad G = \mathcal{O}^\times, \quad \mathfrak{g} = \text{Gal}(K/\mathbf{Q}) = \langle \tau \rangle.$$

Since \mathfrak{g} is cyclic, one can identify a cocycle c of \mathfrak{g} in G with any element of G of norm 1. Let ε be the fundamental unit of K of norm 1 and think this as a cocycle. Hence, by (1),(3)

$$M_\varepsilon = \{x \in \mathcal{O}; \varepsilon^\tau x = x\}, \quad P_\varepsilon = \{x + \varepsilon^\tau x, \quad x \in \mathcal{O}\}$$

and

$$i_\varepsilon(\mathfrak{g}, M) = [M_\varepsilon : P_\varepsilon] = 1 \text{ or } 2. \quad (15)$$

Here we have an interesting result due to Seok-Min Lee. Notation being as above

- (i) $d \equiv 1 \pmod{4} \Rightarrow i_\varepsilon = 1$
- (ii) $d \equiv 2 \pmod{4} \Rightarrow i_\varepsilon = 2$
- (iii) $d \equiv 3 \pmod{4}$ and $a_r \equiv 1 \pmod{2} \Rightarrow i_\varepsilon = 1$
- (iv) $d \equiv 3 \pmod{4}$ and $a_r \equiv 0 \pmod{2} \Rightarrow i_\varepsilon = 2$

where

$$\sqrt{d} = [a_0; \overline{a_1, \dots, a_{r-1}, a_r, a_{r-1}, \dots, a_1, 2a_0}]$$

6 Galois extensions K/k

Let us look at the above result of S-M Lee from a general view point. We shall denote by k either a global or a local field (of characteristic 0). As such, k is either a finite extension of \mathbf{Q} or \mathbf{Q}_p . We denote by \mathcal{O}_k the ring of integers of k .

Let K/k be a finite Galois extension with the Galois group $\mathfrak{g} = \text{Gal}(K/k)$. Then \mathfrak{g} acts on the ring \mathcal{O}_K of integers of K and hence on the group \mathcal{O}_K^\times . For a cocycle $c \in Z(\mathfrak{g}, \mathcal{O}_K^\times)$ we shall look at modules M_c, P_c defined by (1),(3) with $M = \mathcal{O}_K^+$. First, viewing c as a cocycle in $Z(\mathfrak{g}, K^\times)$, we have, by *Hilbert 90*, $c(\sigma) = \xi^{-1} \sigma \xi$ where ξ may be chosen from \mathcal{O}_K . Then we find that $M_c = \mathcal{O}_K \cap \xi^{-1} \mathcal{O}_k$.

In other words, we have

$$\xi M_c = \xi \mathcal{O}_K \cap \mathcal{O}_k = (\xi \mathcal{O}_K)^\mathfrak{g}, \quad \xi \in \mathcal{O}_K \quad (16)$$

Second, as $p_c(x) = \xi^{-1} \sum_{\sigma \in \mathfrak{g}} \sigma \xi \sigma x$, we have

$$\xi p_c(x) = T_{K/k}(\xi x). \quad (17)$$

From (16),(17) we obtain

$$M_c/P_c = (\xi \mathcal{O}_K)^\mathfrak{g}/T_{K/k}(\xi \mathcal{O}_K) = \hat{H}^0(\mathfrak{g}, M)_\gamma, \quad c(\sigma) = \xi^{-1} \sigma \xi \quad (18)$$

An ideal \mathfrak{A} in \mathcal{O}_K will be called *ambiguous* if $\sigma\mathfrak{A} = \mathfrak{A}$, $\sigma \in \mathfrak{g}$. Let \mathfrak{p} be a prime ideal in \mathcal{O}_k . The prime decomposition of \mathfrak{p} in K is of the form

$$\mathfrak{p} = \prod_{\mathfrak{P}|\mathfrak{p}} \mathfrak{P}^{e_{\mathfrak{P}}} = \left(\prod_{\mathfrak{P}|\mathfrak{p}} \mathfrak{P} \right)^{e_{\mathfrak{p}}}. \quad (19)$$

Let us put

$$\mathfrak{p}^{\#} = \prod_{\mathfrak{P}|\mathfrak{p}} \mathfrak{P}$$

Note that (19) becomes

$$\mathfrak{p} = \mathfrak{p}^{\#e_{\mathfrak{p}}} \quad (20)$$

It is easy to see that

$$\mathfrak{A} \subset \mathcal{O}_K \text{ is ambiguous} \Leftrightarrow \mathfrak{A} = \prod_{\mathfrak{p}} \mathfrak{p}^{\#m_{\mathfrak{p}}} \quad (21)$$

For a real number x , put $[x] =$ the smallest integer $\geq x$. Hence when $x \notin \mathbf{Z}$, $[x] = [x] + 1$.

Proposition 1 *Let $\mathfrak{A} = \prod_{\mathfrak{p}} \mathfrak{p}^{\#m_{\mathfrak{p}}}$ be an ambiguous ideal. Then we have*

$$\mathfrak{A}^g = \mathfrak{A} \cap \mathcal{O}_k = \prod_{\mathfrak{p}} \mathfrak{p}^{\left[\frac{m_{\mathfrak{p}}}{e_{\mathfrak{p}}} \right]}$$

For a Galois extension K/k of number fields or local fields, denote by $\mathcal{D}_{K/k}$ the different of the extension. It is an ambiguous integral ideal in K . So it can be expressed as

$$\mathcal{D}_{K/k} = \prod_{\mathfrak{p}} \mathfrak{p}^{\#t_{\mathfrak{p}}}. \quad (22)$$

Proposition 2 *Let $\mathfrak{A} = \prod_{\mathfrak{p}} \mathfrak{p}^{\#m_{\mathfrak{p}}}$ be an integral ambiguous ideal in K . Then*

$$T_{K/k}\mathfrak{A} = \prod_{\mathfrak{p}} \mathfrak{p}^{\left[\frac{m_{\mathfrak{p}} + t_{\mathfrak{p}}}{e_{\mathfrak{p}}} \right]}.$$

Since $\xi \in \mathcal{O}_K$ and $c(\sigma) \in \mathcal{O}_K^{\times}$, $\mathfrak{A} = \xi\mathcal{O}_K$ is an integral ambiguous ideal, and hence we obtain, from (18), Proposition 1, Proposition 2, the following

Proposition 3 $(M_c : P_c) = \prod_{\mathfrak{p}} N_{\mathfrak{p}}^{\left[\frac{m_{\mathfrak{p}} + t_{\mathfrak{p}}}{e_{\mathfrak{p}}} \right] - \left\lceil \frac{m_{\mathfrak{p}}}{e_{\mathfrak{p}}} \right\rceil}$, where $N_{\mathfrak{p}} = (\mathcal{O}_k : \mathfrak{p})$.

From now on, let K/k be a Galois extension of number fields and $\mathfrak{g} = \text{Gal}(K/k)$. Let $\mathfrak{P}, \mathfrak{p}$ be prime ideals of K, k , respectively such that $\mathfrak{P} \mid \mathfrak{p}$. Denote by $K_{\mathfrak{P}}, k_{\mathfrak{p}}$ the completions of K, k , respectively. Then $K_{\mathfrak{P}}/k_{\mathfrak{p}}$ is also a Galois extension whose Galois group $\mathfrak{g}_{\mathfrak{P}}$ may be identified as the decomposition group at \mathfrak{P} in G . Clearly, $\mathcal{O}_K, \mathcal{O}_k$ are embedded in $\mathcal{O}_{K_{\mathfrak{P}}}, \mathcal{O}_{k_{\mathfrak{p}}}$, respectively and similarly for groups of units. Therefore, any cocycle $c \in Z(\mathfrak{g}, \mathcal{O}_K^\times)$ induces naturally a cocycle $c_{\mathfrak{P}} \in Z(\mathfrak{g}_{\mathfrak{P}}, \mathcal{O}_{K_{\mathfrak{P}}}^\times)$. Thus, we are ready to use Proposition 3 to find $(M_c : P_c), (M_{c_{\mathfrak{P}}} : P_{c_{\mathfrak{P}}})$. If ξ is a solution to the cocycle c for \mathfrak{g} (see (18)), then ξ is one to the cocycle $c_{\mathfrak{P}}$ for $\mathfrak{g}_{\mathfrak{P}}$. Put

$$\mathfrak{A} = \xi \mathcal{O}_K = \prod_{\mathfrak{p}} \mathfrak{p}^{\#m_{\mathfrak{p}}} \quad (23)$$

and define

$$\mathfrak{A}_{\mathfrak{P}} = \xi \mathcal{O}_{K_{\mathfrak{P}}} \quad (24)$$

Since

$$m_{\mathfrak{p}} = \nu_{\mathfrak{P}}(\mathfrak{A}) = \nu_{\mathfrak{P}}(\mathfrak{A}_{\mathfrak{P}})$$

the exponent $m_{\mathfrak{p}}$ for $\mathfrak{A}_{\mathfrak{P}}$ is consistent with double purposes, global and local. Next, since, by (22), we have

$$\mathcal{D}_{K/k} = \prod_{\mathfrak{p}} \mathfrak{p}^{\#t_{\mathfrak{p}}} = \prod_{\mathfrak{P}} \mathfrak{P}^{t_{\mathfrak{P}}} = \prod_{\mathfrak{P}} \mathcal{D}_{K_{\mathfrak{P}}/k_{\mathfrak{p}}}.$$

Now, applying Proposition 3 to a local field k , we have

Proposition 4 $(M_{c_{\mathfrak{P}}} : P_{c_{\mathfrak{P}}}) = N_{\mathfrak{P}} \left[\frac{m_{\mathfrak{P}} + t_{\mathfrak{P}}}{e_{\mathfrak{P}}} \right] - \lceil \frac{m_{\mathfrak{P}}}{e_{\mathfrak{P}}} \rceil$

Note also that as $e_{\mathfrak{p}} = 1, t_{\mathfrak{p}} = 0$ for almost all \mathfrak{p} , the indices $(M_{c_{\mathfrak{P}}} : P_{c_{\mathfrak{P}}}) = 1$ for almost all \mathfrak{P} .

Summarizing all these, we obtain

Theorem 1 *Let K/k be a finite Galois extension of number fields and $\mathfrak{g} = \text{Gal}(K/k)$. For a cocycle $c \in Z(\mathfrak{g}, \mathcal{O}_K^\times)$ denote by $c_{\mathfrak{P}}$ the cocycle induced from c by localization at \mathfrak{P} . Then we have the product relation $(M_c : P_c) = \prod_{\mathfrak{p}} (M_{c_{\mathfrak{P}}} : P_{c_{\mathfrak{P}}})$ where for each \mathfrak{p} we choose one \mathfrak{P} dividing \mathfrak{p} .*

From the ramification theory of Galois extensions we have

$$t_{\mathfrak{p}} \geq e_{\mathfrak{p}} - 1, \quad \text{for all } \mathfrak{p}$$

$$t_{\mathfrak{p}} \geq 1 \Leftrightarrow e_{\mathfrak{p}} \geq 2 \quad (\text{Dedekind}).$$

Needless to say, if $e_{\mathfrak{p}} = 1$ then \mathfrak{p} is unramified, if $t_{\mathfrak{p}} = e_{\mathfrak{p}} - 1 \geq 1$ then \mathfrak{p} is said to be tamely ramified. Furthermore, if \mathfrak{p} is such that $t_{\mathfrak{p}} \geq e_{\mathfrak{p}} \geq 2$ then \mathfrak{p} is wildly ramified. (Note that \mathfrak{p} is wildly ramified $\Leftrightarrow p \mid e_{\mathfrak{p}}$, where p means the characteristic of the finite field $\mathcal{O}_k/\mathfrak{p}$.)

We will use these terms for extensions in an obvious way. Proposition 4 implies immediately the following

Theorem 2 *Let K/k be a finite Galois extension of number fields. If K/k is unramified or tamely ramified, then $M_c = P_c$ for all cocycle $c \in Z(\text{Gal}(K/k), \mathcal{O}_K^\times)$*

Since we have

$$i_\gamma(K/k) = (M_c : P_c), \quad \gamma \in H^1(\mathfrak{g}, \mathcal{O}_K^\times) \quad (25)$$

we can express Theorem 2 as

Theorem 3 *For a finite Galois extension K/k of number fields, we have $i_\gamma(K/k) = \prod_{\mathfrak{p}} i_{\gamma_{\mathfrak{p}}}(K_{\mathfrak{p}}/k_{\mathfrak{p}})$.*

Now passing to localization, choose a prime element $\Pi \in K_{\mathfrak{p}}$. Then the relation

$$\sigma \Pi = \Pi z_\sigma, \quad \sigma \in \mathfrak{g}_{\mathfrak{p}}, \quad z_\sigma \in \mathcal{O}_{K_{\mathfrak{p}}}^\times,$$

defines the cohomology class

$$\gamma_{K_{\mathfrak{p}}/k_{\mathfrak{p}}} = [z] \in H^1(\mathfrak{g}_{\mathfrak{p}}, \mathcal{O}_{K_{\mathfrak{p}}}^\times). \quad (26)$$

We know that the group $H^1(\mathfrak{g}_{\mathfrak{p}}, \mathcal{O}_{K_{\mathfrak{p}}}^\times)$ is cyclic of order $e_{\mathfrak{p}}$ generated by $\gamma_{K_{\mathfrak{p}}/k_{\mathfrak{p}}}$. (See [2].) Therefore for any class $\gamma = [c] \in H^1(\mathfrak{g}_{\mathfrak{p}}, \mathcal{O}_{K_{\mathfrak{p}}}^\times)$, a unique integer $m \pmod{e_{\mathfrak{p}}}$ is determined so that

$$\gamma = (\gamma_{K_{\mathfrak{p}}/k_{\mathfrak{p}}})^m \quad (27)$$

In otherwords,

$$c \sim z^m \quad (28)$$

Now, let ξ be a solution in K to the cocycle c in (18). Then (28) means that

$$\frac{\sigma\xi}{\xi} = u^{-1} \frac{\sigma\Pi^m}{\Pi^m} \sigma u, \quad u \in \mathcal{O}_{K_{\mathfrak{p}}}^\times$$

or

$$u\Pi^m = \xi v \pi^r$$

where $v \in \mathcal{O}_{k_{\mathfrak{p}}}^\times$ and π being a prime element in $k_{\mathfrak{p}}$. In view of (15), we find

$$m = m_{\mathfrak{p}} + r e_{\mathfrak{p}}$$

and so

$$m \equiv m_{\mathfrak{p}} \pmod{e_{\mathfrak{p}}} \tag{29}$$

7 Quadratic fields again

Now that we have a product relation (Theorem 3), our problem of indices for global fields is entirely reduced to local computations. As the easiest example, let us look at our old works again. (See [1],[3].)

Let $K = \mathbf{Q}(\sqrt{d})$ where d is a square free integer. Let p, \mathfrak{P} be primes of \mathbf{Q}, K , respectively, such that $\mathfrak{P} \mid p$. When extensions $K_{\mathfrak{P}}/\mathbf{Q}_p$ is unramified or tamely ramified, then by Proposition 4, $i_{\gamma_{\mathfrak{P}}}(K_{\mathfrak{P}}/\mathbf{Q}_p) = 1$. Therefore only wildly ramified case must be taken care of. This is precisely the case where

$$p = 2 \quad d \equiv 2, 3 \pmod{4}.$$

(i) $p = 2, d \equiv 2 \pmod{4}$. In this case, $\mathcal{D}_{K_{\mathfrak{P}}/\mathbf{Q}_2} = \mathfrak{P}^3$ and so $t_2 = 3$. Since the order of the cohomology group $H^1(\mathfrak{g}_{\mathfrak{P}}, \mathcal{O}_{K_{\mathfrak{P}}}^\times) = \langle \gamma_{\mathfrak{P}}(K_{\mathfrak{P}}/\mathbf{Q}_2) \rangle$ is $e_2 = 2$, we find that the number m , in (27), is either 0 or 1. As we are allowed to replace m_2 by $m \pmod{e_2}$, we get, using Proposition 4,

$$i_1(K_{\mathfrak{P}}/\mathbf{Q}_2) = 2^{\lfloor \frac{t_2}{e_2} \rfloor} = 2^{\lfloor \frac{3}{2} \rfloor} = 2$$

and, for $\gamma \neq 1$,

$$\begin{aligned} i_{\gamma}(K_{\mathfrak{P}}/\mathbf{Q}_2) &= \\ &= 2^{\lfloor \frac{t_2 + m_2}{e_2} \rfloor - \lceil \frac{m_2}{e_2} \rceil} \\ &= 2^{\lfloor \frac{3+1}{2} \rfloor - \lceil \frac{1}{2} \rceil} = 2 \end{aligned}$$

So the index $i_\gamma = 2$ always.

(ii) $p = 2$, $d \equiv 3 \pmod{4}$. In this case we have $t_2 = 2$. The similar calculation as above shows this time that

$$i_\gamma = \begin{cases} 2 & \text{when } \gamma = 1, \text{ i.e. when } m_2 \text{ is even,} \\ 1 & \text{when } \gamma \neq 1, \text{ i.e. when } m_2 \text{ is odd.} \end{cases}$$

8 Hopf map

By the Hopf map $h : \mathbf{R}^4 \rightarrow \mathbf{R}^3$ we shall mean a map $y = h(x)$ given by a system of three quadratic forms of four variables:

$$\begin{aligned} y_1 &= x_0^2 + x_1^2 - x_2^2 - x_3^2 \\ y_2 &= 2(x_1x_2 + x_0x_3) \\ y_3 &= 2(x_1x_3 - x_0x_2). \end{aligned}$$

One checks that $h(S^3) \subseteq S^2$ where S^i is the unit sphere of dimension i . Let $\mathbf{H} = \mathbf{R} + \mathbf{R}i + \mathbf{R}j + \mathbf{R}k$ be the division ring of the (Hamilton) quaternions and \mathbf{H}_0 the vector part of \mathbf{H}

$$\mathbf{H}_0 = \{v \in \mathbf{H}; v = x_1i + x_2j + x_3k\}.$$

The *involution* on \mathbf{H} is the map $x = x_0 + v \mapsto x^* = x_0 - v$ with the well known properties. We set

$$Tx = x + x^* = 2x_0 \quad (\text{trace}), \quad Nx = xx^* = x_0^2 + x_1^2 + x_2^2 + x_3^2 \quad (\text{norm})$$

We have

$$\mathbf{H}_0 = \{x \in \mathbf{H}; Tx = 0\}. \quad (30)$$

By the relation $N(xy) = NxNy$, the set $\mathbf{H}^\times = \{x \in \mathbf{H}; Nx \neq 0\}$ forms a group and hence

$$\mathbf{H}_1 = \{x \in \mathbf{H}; Nx = 1\} = S^3 \quad (31)$$

becomes its subgroup.

In terms of the involution, the Hopf map is simply

$$h(x) = xix^*, \quad x \in \mathbf{H}. \quad (32)$$

Since $\mathbf{H} = \mathbf{R} + \mathbf{R}i + \mathbf{R}j + \mathbf{R}k = \mathbf{C} + \mathbf{C}j$, one can write

$$x = \alpha + \beta j, \quad \alpha, \beta \in \mathbf{C}.$$

Then we find $x^* = \bar{\alpha} - \beta j$.
 Call φ the map $\mathbf{H} \rightarrow M_2(\mathbf{C})$:

$$\varphi(x) = \begin{bmatrix} \alpha & \beta \\ -\bar{\beta} & \bar{\alpha} \end{bmatrix}$$

Then we have

$$\varphi(x^*) = \varphi(x)^* = {}^t\overline{\varphi(x)}.$$

Consequently, an isomorphism

$$\mathbf{H}_1 \simeq SU(2). \quad (33)$$

On the other hand, φ induces an isomorphism

$$\mathbf{H}_0 \simeq \mathfrak{su}(2) = \{X \in M_2(\mathbf{C}); X^* + X = \text{tr } X = 0\}. \quad (34)$$

Viewing the Hopf map h as $\mathbf{H}_1 \rightarrow \mathbf{H}_0$, we obtain

$$h(x) = xix^* = xix^{-1} = (\text{Ad } x)i \quad (35)$$

and the *fibration* $0 \rightarrow S^1 \rightarrow S^3 \rightarrow S^2 \rightarrow 0$.

9 Quaternion algebras

Let F be a field of characteristic $\neq 2$. For $a, b \in F^\times$ denote by $A = (a, b)_F$ the quaternion algebra with basis $\{1, u_1, u_2, u_3\}$ with the multiplication table

$$u_i u_j = -u_j u_i, \quad (i \neq j), \quad u_1 u_2 = u_3, \quad u_2 u_3 = u_1, \quad u_3 u_1 = u_2, \quad u_1^2 = a, \quad u_2^2 = b, \quad u_3^2 = -ab$$

Let $K = F(\sqrt{a})$. We define an F -algebra map

$$\varphi : A \rightarrow M_2(K) \quad (36)$$

by

$$\begin{aligned} u_1 &\mapsto \begin{bmatrix} \sqrt{a} & 0 \\ 0 & \sqrt{a} \end{bmatrix}, \\ u_2 &\mapsto \begin{bmatrix} 0 & 1 \\ b & 0 \end{bmatrix}, \\ u_3 &\mapsto \begin{bmatrix} 0 & \sqrt{a} \\ -b\sqrt{a} & 0 \end{bmatrix} \end{aligned}$$

To be precise, we have

$$\varphi(x) = \begin{bmatrix} x_0 + x_1\sqrt{a} & x_2 + x_3\sqrt{a} \\ b(x_2 - x_3\sqrt{a}) & x_0 - x_1\sqrt{a} \end{bmatrix}$$

In A we have an involution $x \mapsto x^*$, Tx and Nx , as in **8** which are compatible with the usual notation in linear algebra via the map φ . For example equalities like

$$Tx = \text{tr } x = 2x_0, \quad Nx = \det x = x_0^2 - ax_1^2 - bx_2^2 + abx_3^2$$

make sense.

Again as in **8**, we define A_0, A_1 for $A = (a, b)_F$:

$$A_0 = \{x \in A; Tx = 0\} = \left\{x = \begin{bmatrix} x_1\sqrt{a} & x_2 + x_3\sqrt{a} \\ b(x_2 - x_3\sqrt{a}) & -x_1\sqrt{a} \end{bmatrix}\right\} \quad (37)$$

$$A_1 = \{g \in A; Ng = 1\} = \{g \in A; \det g = 1\} \quad (38)$$

A_1 is a group acting on the vector space A_0 over F by

$$g \circ x = gxg^{-1} = gxg^* \quad (39)$$

Lemma 1 *For $x \in A$, $x \neq 0$, we have $x \in A_0 \Leftrightarrow x^2 \in F$ and $x \notin F$.*

10 Case $K=\mathbf{Q}$

Let $A = (a, b)_F$ be quaternion algebra as in **9**. Since $K = F(\sqrt{a})$ we have two cases: $K = F$ or $[K : F] = 2$. From now on, we shall assume that $F = \mathbf{Q}$. So either $K = \mathbf{Q}$ or $K = \mathbf{Q}(\sqrt{a})$. In this section, we assume, for simplicity, that $a = b = 1$. The map φ in (36) boils down to

$$A = (1, 1)_{\mathbf{Q}} \simeq M_2(\mathbf{Q}) \quad (40)$$

given by

$$x \mapsto \varphi(x) = \begin{bmatrix} x_0 + x_1 & x_2 + x_3 \\ x_2 - x_3 & x_0 - x_1 \end{bmatrix}$$

Now set

$$A(\mathbf{Z}) = \varphi^{-1}(M_2(\mathbf{Z})) \quad (41)$$

In other words, via φ , one can write $A(\mathbf{Z}) = M_2(\mathbf{Z})$. Then set

$$A_0(\mathbf{Z}) = A_0 \cap A(\mathbf{Z}).$$

From (40), we infer that

$$A_0(\mathbf{Z}) = \left\{ x = \begin{bmatrix} h & k \\ l - k & -h \end{bmatrix}, \quad h, k, l \in \mathbf{Z} \right\} \quad (42)$$

For a square free integer m , set

$$S(m) = \{x \in A_0(\mathbf{Z}); \det x = m\} = \{x \in A(\mathbf{Z}), \operatorname{tr} x = 0, \det x = m\} \quad (43)$$

For $x \in S(m)$, its characteristic polynomial is $f(t) = t^2 + m \in \mathbf{Z}[t]$. In general, for a polynomial $f \in \mathbf{Z}[t]$ put

$$M_2(\mathbf{Z}, f) = \{x \in M_2(\mathbf{Z}); f(x) = 0\}$$

Then we have

Lemma 2 $S(m) = M_2(\mathbf{Z}, t^2 + m)$.

. Now the group $G = GL_2(\mathbf{Z})$ acts on $S(m)$ by $g \circ x = gxg^{-1}$. Let us denote the orbit space by

$$S(m)/G.$$

By Lemma 2, we have $S(m)/G = M_2(\mathbf{Z}, t^2 + m)/G$. On the other hand, it follows from a well known theorem that one has a bijection

$$M_2(\mathbf{Z}, t^2 + m)/G \simeq I(\mathbf{Z}[\sqrt{-m}])/G \quad (44)$$

where $I(\mathbf{Z}[\sqrt{-m}])$ means the set of all ideals of the order $\mathbf{Z}[\sqrt{-m}]$.

If, in particular, $m \equiv 1, 2 \pmod{4}$, then $I(\mathbf{Z}[\sqrt{-m}])$ is the maximal order of K and, by Lemma 2, we obtain

$$|S(m)/G| = h(\sqrt{-m}),$$

the class number of the quadratic field $\mathbf{Q}(\sqrt{-m})$.

11 Case $K = \mathbf{Q}(\sqrt{a})$

Let $A = (a, b)_{\mathbf{Q}}$. We assume now that $K = \mathbf{Q}(\sqrt{a})$ is a quadratic field. From now on we set

$$\theta = \sqrt{a}.$$

We denote by \mathcal{O} the ring of integers of K . We find it convenient to assume that $a \equiv 2, 3 \pmod{4}$ so that

$$\mathcal{O} = \mathbf{Z}[\theta].$$

The Galois group \mathfrak{g} of K/\mathbf{Q} is cyclic of order 2; the unique generator will be given by $x \mapsto \bar{x}$. For example,

$$\bar{\theta} = -\theta.$$

Finally, for simplicity, we assume that

$$b = -1.$$

The map φ in (36) goes like

$$A = (a, -1)_{\mathbf{Q}} \simeq M_2(K) \tag{45}$$

with

$$x = x_0 + x_1u_1 + x_2u_2 + x_3u_3 \mapsto \varphi(x) = \begin{bmatrix} x_0 + x_1\theta & x_2 + x_3\theta \\ x_2 - x_3\theta & x_0 - x_1\theta \end{bmatrix}.$$

For integral points of A , we set , as in (41)

$$A(\mathbf{Z}) = \varphi^{-1}(M_2(\mathcal{O})) = \left\{ x = \begin{bmatrix} z & w \\ -\bar{w} & \bar{z} \end{bmatrix} \in M_2(\mathcal{O}) \right\} \tag{46}$$

Furthermore ,we set

$$A_1(\mathbf{Z}) = \left\{ g = \begin{bmatrix} \alpha & \beta \\ -\bar{\beta} & \bar{\alpha} \end{bmatrix}; \alpha, \beta \in \mathcal{O}, \det g = \alpha\bar{\alpha} + \beta\bar{\beta} = 1 \right\} \tag{47}$$

$$A_0(\mathbf{Z}) = \left\{ x = \begin{bmatrix} z & w \\ -\bar{w} & \bar{z} \end{bmatrix}; z, w \in \mathcal{O}, \operatorname{tr} x = z + \bar{z} = 0 \right\} \tag{48}$$

In accordance with notation in **1**, we set

$$M = A_0(\mathbf{Z}), \quad G = A_1(\mathbf{Z}), \quad \mathfrak{g} = \text{Gal}(K/\mathbf{Q})$$

Let us study the cohomology set $H^1(\mathfrak{g}, G)$. As explained in the beginning of **5**, we have

$$Z^1(\mathfrak{g}, G) = \left\{ c = \begin{bmatrix} z & w \\ -\bar{w} & \bar{z} \end{bmatrix} \in G, \quad c\bar{c} = 1 \right\} \quad (49)$$

and

$$c' \sim c, \quad c, c' \in Z^1(\mathfrak{g}, G) \Leftrightarrow c' = g^{-1}cg, \quad \exists g \in G. \quad (50)$$

The following lemma follows from our assumption $b = -1$

Lemma 3 $\bar{g} = u_2 g u_2^{-1}, \quad u_2 = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$

We set

$$S = A_1(\mathbf{Z}) \cap A_0(\mathbf{Z}) = \{s \in A(\mathbf{Z}); \text{tr } s = 0, \text{det } s = 1\} \quad (51)$$

Note that $u_2 \in S$.

Lemma 4 $Z^1 u_2 = S$.

Theorem 4 *Let $A = (a, -1)_{\mathbf{Q}}$ where a is a square free integer such that $a \equiv 2, 3 \pmod{4}$. Let $S = A_1(\mathbf{Z}) \cap A_0(\mathbf{Z})$ and $\mathfrak{g} = \text{Gal}(\mathbf{Q}(\sqrt{a})/\mathbf{Q})$. Then we have $H^1(\mathfrak{g}, A_1(\mathbf{Z})) \simeq S/A_1(\mathbf{Z})$.*

Remark 1 *To know the set $H^1(\mathfrak{g}, A_1(\mathbf{Z}))$ is, of course, necessary to study thoroughly our system $(\mathfrak{g}, (G, M))$ in **1**. We hope to come back to this problem sometime soon.*

References

[1] Ono, T. : A Note on Poincaré sums for finite groups. Proc. Japan Acad., **79A**, 95-97 (2003).

[2] Ono, T. : On Poincaré sums for local fields. Proc. Japan Acad., **79A**, 115-118 (2003).

[3] Lee, S-M, and Ono, T. : On a certain invariant for real quadratic fields. Proc. Japan Acad., **79A**, 119-122 (2003).

[4] Ono, T : On Poincaré sums for number fields. Proc. Japan Acad., **81A**, 65-68 (2005).

[5] Cassels, J.W.S., and Fröhlich, A. (eds.): Algebraic Number Theory (Proc. Instructional Conf., Brighton, 1965). Academic Press, London-New York (1967).