On Poincaré sums for number fields

By Takashi Ono

Department of Mathematics, The Johns Hopkins University
Baltimore, Maryland 21218, U.S.A.
(Communicated by Shokichi Iyanaga, M. J. A., April 12, 2005)

Abstract: Let G be a finite group acting on a ring R. To know the twisted Tate cohomology $\hat{H}^0(G,R^+)_\gamma$ parametrized by $\gamma=[c]\in H^1(G,R^\times)$ is a basic theme inspired by Poincaré. We shall consider this when G is the Galois group of a Galois extension K/k of number fields and R is the ring of integers of K.

Key words: Number fields; local fields; cohomology groups; ambiguous ideals; differents; ramifications.

1. Introduction. This is a continuation of [1, 2]. We shall determine, for any finite Galois extension K/k of number fields, the index $i_\gamma(K/k)$ where $\gamma=[c]\in H^1(\mathrm{Gal}(K/k),\mathcal{O}_K^\times)$. It is crucial to look at the prime decomposition of principal ideal generated by a special value of Poincaré sum related to the cocycle c. This clarifies a mysterious looking criterion for parity of indices for real quadratic fields. (See [3]) As for basic facts on number theory, see [4].

2. The map p_c. Let R be a ring with unit 1_R, G a finite group acting on R (as ring automorphisms) and $R^\times$ the group of units of R. We denote the action by $x\mapsto {}^s x$, $x\in R$, $s\in G$. Since G acts on $R^\times$ (as group automorphisms) the 1-st cocycle set $Z^1(G,R^\times)$ makes sense:

$$(1)\quad \begin{aligned} &Z^1(G,R^\times)\\ &\quad=\{c:G\to R^\times,\ c(st)=c(s)\ {}^s c(t),\ s,t\in G\}.\end{aligned}$$

We consider a map $p_c:R\to R$, for $c\in Z^1(G,R^\times)$:

$$(2)\qquad p_c(x)=\sum_{s\in G}c(s)\ {}^s x,\quad x\in R.$$

Clearly the map is additive. A basic observation is the following criterion so that $p_c(\alpha)\in R^\times$ for some $\alpha\in R$.

Theorem 1 (Hilbert). *Assume that $|G|1_R\in R^\times$. For a cocycle $c\in Z^1(G,R^\times)$, we have*

$$c\sim 1\ (c \textit{ is a coboundary})$$
$$\Leftrightarrow p_c(\alpha)\in R^\times \textit{ for some } \alpha\in R.$$

When that is so, we have

$$c(s)=p_c(\alpha)\ {}^s p_c(\alpha)^{-1}.$$

Proof. Suppose first that

$$(3)\qquad p_c(\alpha)=\sum_t c(t)\ {}^t\alpha\in R^\times.$$

Apply s on both sides of (3) and then multiply $c(s)$ on the results. Then, in view of (1), we have

$$c(s)\ {}^s p_c(\alpha)=\sum_t c(s)\ {}^s c(t)\ {}^{st}\alpha=\sum_t c(st)\ {}^{st}\alpha=p_c(\alpha).$$

As $p_c(\alpha)\in R^\times$, we obtain $c\sim 1$. Conversely, assume that $c\sim 1$. So $c(s)=\alpha\ {}^s\alpha^{-1}$, $\alpha\in R^\times$. Put $x=\alpha$ in (2). Then we find

$$p_c(\alpha)=\sum_s c(s)\ {}^s\alpha=\alpha|G|1_R\in R^\times.$$

□

Corollary 1 (Hilbert Theorem 90). *If K/k is a finite Galois extension of fields, then $H^1(\mathrm{Gal}(K/k),K^\times)=1$.*

Proof. By the linear independence of characters, for any cocycle $c\in Z^1(\mathrm{Gal}(K/k),K^\times)$, we have $p_c(\theta)=\sum_{s\in\mathrm{Gal}(K/k)}c(s)\ {}^s\theta\neq 0$ for some $\theta\in K$ and the assertion follows from Theorem 1. □

3. The module M_c/P_c. Notation being as in **1**, for a cocycle $c\in Z(G,R^\times)$, we set

$$(4)\quad M_c=\{x\in R,\ c(s)\ {}^s x=x,\ \text{ for all } s\in G\},$$

$$(5)\qquad P_c=\{p_c(x),\ \text{ for all } x\in R\}.$$

(4), (5) imply the relation

$$(6)\qquad p_c(a)=|G|a,\ \text{ when } a\in M_c$$

2000 Mathematics Subject Classification. 11R34.
Dedicated to Professor S. Iyanaga, M. J. A., on his 99th birthday.

and we find

$$|G|M_c \subseteq P_c \subseteq M_c. \tag{7}$$

The structure of the module M_c/P_c depends only on the cohomology class $\gamma = [c]$ in $H^1(G, R^\times)$. As for details of idetification of the quotient module M_c/P_c with the (modified) Tate group $\hat{H}^0(G, R^+)_\gamma$, see [1].

4. Galois extensions K/k. In what follows, we 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 $G = \mathrm{Gal}(K/k)$. Then G acts on the ring $\mathcal{O}_K$ of integers of K and hence on the group $\mathcal{O}_K^\times$. For a cocycle $c \in Z^1(G, \mathcal{O}_K^\times)$ we shall look at modules M_c, P_c defined by (4), (5) with $R = \mathcal{O}_K$. First, viewing c as a cocycle in $Z^1(G, K^\times)$, we have, by Corollary 1, $c(s) = \xi^{-1}\ {}^s\xi$ 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

$$\xi M_c = \xi\mathcal{O}_K \cap \mathcal{O}_k = (\xi\mathcal{O}_K)^G, \quad \xi \in \mathcal{O}_K. \tag{8}$$

Second, as $p_c(x) = \xi^{-1} \sum_{s\in G} {}^s\xi\ {}^sx$, we have

$$\xi p_c(x) = T_{K/k}(\xi x). \tag{9}$$

From (8), (9) we obtain

$$M_c/P_c = (\xi\mathcal{O}_K)^G / T_{K/k}(\xi\mathcal{O}_K) = \hat{H}^0(G, R^+)_\gamma, \quad c(s) = \xi^{-1}\ {}^s\xi. \tag{10}$$

5. Ambiguous ideals. Notation being as in **3**, an ideal $\mathfrak{A}$ in $\mathcal{O}_K$ will be called *ambiguous* if ${}^s\mathfrak{A} = \mathfrak{A}$, $s \in G$. Let $\mathfrak{p}$ be a prime ideal in $\mathcal{O}_k$. The prime decomposition of $\mathfrak{p}$ in K is of the form

$$\mathfrak{p} = \prod_{\mathfrak{P}|\mathfrak{p}} \mathfrak{P}^{e_\mathfrak{P}} = \Bigl(\prod_{\mathfrak{P}|\mathfrak{p}} \mathfrak{P}\Bigr)^{e_\mathfrak{p}}. \tag{11}$$

Let us put

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

Note that (11) becomes

$$\mathfrak{p} = \mathfrak{p}^{\# e_\mathfrak{p}}. \tag{12}$$

It is easy to see that

$$\mathfrak{A} \subset \mathcal{O}_K \ \text{ is ambiguous } \Leftrightarrow \mathfrak{A} = \prod_\mathfrak{p} \mathfrak{p}^{\# m_\mathfrak{p}}. \tag{13}$$

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

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

$$\mathfrak{A}^G = \mathfrak{A} \cap \mathcal{O}_k = \prod_\mathfrak{p} \mathfrak{p}^{\lceil \frac{m_\mathfrak{p}}{e_\mathfrak{p}} \rceil}.$$

Proof. Let $m_\mathfrak{p} = qe_\mathfrak{p} + r$, $0 \leq r \leq e_\mathfrak{p} - 1$. We have

$$\mathfrak{p}^{\# m_\mathfrak{p}} = \mathfrak{p}^{\# q e_\mathfrak{p}} \mathfrak{p}^{\# r} = \mathfrak{p}^q \mathfrak{p}^{\# r} = \mathfrak{p}^{\left[\frac{m_\mathfrak{p}}{e_\mathfrak{p}}\right]} \mathfrak{p}^{\# r}.$$

Then our assertion follows since

$$\mathfrak{p}^{\# r} \cap \mathcal{O}_k = \begin{cases} 1 & \text{when } \ r = 0, \\ \mathfrak{p} & \text{when } \ r > 0. \end{cases}$$

□

6. Differents. 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

$$\mathcal{D}_{K/k} = \prod_\mathfrak{p} \mathfrak{p}^{\# t_\mathfrak{p}}. \tag{14}$$

Proposition 2. *Let $\mathfrak{A} = \prod_\mathfrak{p} \mathfrak{p}^{\# m_\mathfrak{p}}$ be an integral ambiguous ideal in K. Then $T_{K/k}\mathfrak{A} = \prod_\mathfrak{p} \mathfrak{p}^{\left[\frac{m_\mathfrak{p} + t_\mathfrak{p}}{e_\mathfrak{p}}\right]}$.*

Proof. Let $\mathfrak{p}$ be a prime ideal in k and h be an integer ≥ 0. By the definition of $\mathcal{D}_{K/k}$, we get the following chains of logical equivalences:

$$\begin{aligned} \mathfrak{p}^h \mid T_{K/k}\mathfrak{A} &\Leftrightarrow \mathfrak{p}^h \mid \mathfrak{A}\mathcal{D}_{K/k} \Leftrightarrow (\mathfrak{p}^\#)^{e_\mathfrak{p} h} \mid \mathfrak{A}\mathcal{D}_{K/k} \\ &\Leftrightarrow (\mathfrak{p}^\#)^{e_\mathfrak{p} h} \mid (\mathfrak{p}^\#)^{m_\mathfrak{p} + t_\mathfrak{p}} \\ &\Leftrightarrow e_\mathfrak{p} h \leq m_\mathfrak{p} + t_\mathfrak{p} \Leftrightarrow h \leq \left[\frac{m_\mathfrak{p} + t_\mathfrak{p}}{e_\mathfrak{p}}\right]. \end{aligned}$$

□

Back to the situation in **3**, since $\xi \in \mathcal{O}_K$ and $c(s) \in \mathcal{O}_K^\times$, $\mathfrak{A} = \xi\mathcal{O}_K$ is an integral ambiguous ideal, and hence we obtain, from (10), Proposition 1, Proposition 2, the following

Proposition 3.

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

7. Localization. From now on, let K/k be a Galois extension of number fields and $G = \mathrm{Gal}(K/k)$. 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 $G_\mathfrak{P}$ 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 $c \in Z^1(G, \mathcal{O}_K^\times)$ induces naturally a cocycle $c_\mathfrak{P} \in Z^1(G_\mathfrak{P}, \mathcal{O}_{K_\mathfrak{P}}^\times)$. 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 G (see (10)), then ξ is one to the cocycle $c_\mathfrak{P}$ for $G_\mathfrak{P}$. Put

$$\mathfrak{A} = \xi\mathcal{O}_K = \prod_\mathfrak{p} \mathfrak{p}^{\# m_\mathfrak{p}} \tag{15}$$

and define

$$\mathfrak{A}_\mathfrak{P} = \xi\mathcal{O}_{K_\mathfrak{P}}. \tag{16}$$

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 (14), 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.
$(M_{c_\mathfrak{P}} : P_{c_\mathfrak{P}}) = N\mathfrak{p}^{\left[\frac{m_\mathfrak{p}+t_\mathfrak{p}}{e_\mathfrak{p}}\right] - \left\lceil \frac{m_\mathfrak{p}}{e_\mathfrak{p}} \right\rceil}$.

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 2. *Let K/k be a finite Galois extension of number fields and $G = \mathrm{Gal}(K/k)$. For a cocycle $c \in Z^1(G, \mathcal{O}_K^\times)$ 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 3. *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 $c \in Z^1(\mathrm{Gal}(K/k), \mathcal{O}_K^\times)$.*

8. Canonical class for local fields. Let K/k be a Galois extension of number fields or local fields. In view of the remark at the end of **3**, we have a right to write

$$i_\gamma(K/k) = (M_c : P_c), \quad \gamma \in H^1(G, \mathcal{O}_K^\times). \tag{17}$$

Then we can express Theorem 2 as

Theorem 4. *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

$${}^s\Pi = \Pi z_s, \quad s \in G_\mathfrak{P}, \quad z_s \in \mathcal{O}_{K_\mathfrak{P}}^\times,$$

defines the cohomology class

$$\gamma_{K_\mathfrak{P}/k_\mathfrak{p}} = [z] \in H^1(G, \mathcal{O}_{K_\mathfrak{P}}^\times). \tag{18}$$

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

$$\gamma = (\gamma_{K_\mathfrak{P}/k_\mathfrak{p}})^m. \tag{19}$$

In otherwords,

$$c \sim z^m. \tag{20}$$

Now, let ξ be a solution in K to the cocycle c in (10). Then (20) means that

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

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

$$m \equiv m_\mathfrak{p} \bmod e_\mathfrak{p}. \tag{21}$$

9. Quadratic fields. Now that we have a product relation (Theorem 4), 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

$$p = 2 \quad \equiv 2,\ 3 \bmod 4.$$

(i) $p = 2$, $d \equiv 2 \bmod 4$. 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 $H^1(G, \mathcal{O}_{K_{\mathfrak{P}}}^{\times}) = \langle \gamma_{\mathfrak{P}}(K_{\mathfrak{P}}/\mathbf{Q}_2) \rangle$ is $e_2 = 2$, we find that the number m, in (19), is eather 0 or 1. As we are allowed to replace m_2 by $m \bmod e_2$, we get, using Proposition 4,

$$i_1(K_{\mathfrak{P}}/\mathbf{Q}_2) = 2^{\left[\frac{t_2}{e_2}\right]} = 2^{\left[\frac{3}{2}\right]} = 2$$

and, for $\gamma \neq 1$,

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

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

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

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

References

[1] T. Ono, A note on Poincaré sums for finite groups, Proc. Japan Acad. Ser. A Math. Sci. **79** (2003), no. 4, 95–97.

[2] T. Ono, On Poincaré sums for local fields, Proc. Japan Acad. Ser. A Math. Sci. **79** (2003), no. 7, 115–118.

[3] S.-M. Lee and T. Ono, On a certain invariant for real quadratic fields, Proc. Japan Acad. Ser. A Math. Sci. **79** (2003), no. 8, 119–122.

[4] J. W. S. Cassels and A. Fröhlich (eds.), *Algebraic Number Theory, Proc. Instructional Conf.,* (*Brighton, 1965*), Academic Press, London-New York (1986).