On Poincaré sums for local fields

By Takashi Ono

Department of Mathematics, The Johns Hopkins University, Baltimore, Maryland, 21218-2686, U. S. A.

(Communicated by Shokichi Iyanaga, M. J. A., Sept. 12, 2003)

Abstract: Let K/k be a finite Galois extension of local fields. To each class $\gamma = [c]$ in $H^1(\mathrm{Gal}(K/k), U_K)$, U_K being the group of units of K, we associate an index $i_\gamma(K/k) = (M_c : P_c)$ after the model of Poincaré series and study its relation to the ramification theory of K/k.

Key words: $\mathfrak{p}$-adic fields; cohomology groups; differents; ramifications; cyclotomic fields.

1. Introduction. This is a continuation of papers [1, 2] where we looked at mainly (global) quadratic fields. In this paper, however, we will steer toward Galois extensions of local fields.

Let K/k be a finite Galois extension of $\mathfrak{p}$-adic number fields with the Galois group $G = \mathrm{Gal}(K/k)$. Denote by $\mathcal{O}_K$ the ring of integers in K, by $\mathfrak{P}$ the prime ideal of $\mathcal{O}_K$ and by U_K the group of units of $\mathcal{O}_K$. For the ground field k, we adopt notation $\mathcal{O}_k$, $\mathfrak{p}$ and U_k similarly.

Following Poincaré, we set, for a cocycle c of G in U_K,

$$M_c = \{a \in \mathcal{O}_K;\, c_s{}^s a = a, \quad s \in G\}, \tag{1}$$

$$P_c = \Big\{p_c(a) = \sum_{t \in G} c_t{}^t a, \quad a \in \mathcal{O}_K\Big\}. \tag{2}$$

One finds that $|G|M_c \subseteq P_c \subseteq M_c$ and that the $|G|$-torsion finite module M_c/P_c depends only on the class $\gamma = [c]$. Therefore one can associate an invariant to a finite Galois extension K/k of $\mathfrak{p}$-adic fields by

$$i_\gamma(K/k) := (M_c : P_c), \quad \gamma \in H^1(G, U_K). \tag{3}$$

In this paper, we will study some relations of $i_\gamma(K/k)$ with the ramification theory of K/k. We will mention some applications to cyclotomic and Kummer extensions.

As for basic facts on number theory, see [3].

2. Canonical class $\boldsymbol{\gamma_{K/k}}$. Notation being as in **1**, let us fix a prime element Π in K. Then we have

$${}^s\Pi = \Pi z_s, \quad s \in G, \quad z_s \in U_K. \tag{4}$$

The mapping $s \mapsto z_s$ is a 1-cocycle of G in U_K. Since the change of the prime element Π changes the cocycle z to z' cohomologous to it, Π has an ability of bringing a canonical class $\gamma_{K/k} = [z]$ in the cohomology group $H^1(G, U_K)$.

3. $\boldsymbol{H^1(G, U_K)}$. Let $\gamma = [c]$ be any class $\in H^1(G, U_K)$. Since U_K is a subgroup of $K^\times$ there is, by Hilbert theorem 90, an element $a \in K^\times$ such that

$$c_s = \frac{{}^s a}{a}. \tag{5}$$

Now write

$$a = \Pi^m u, \quad u \in U_K, \quad m \in \mathbf{Z}. \tag{6}$$

In view of (4), we have

$${}^s a = {}^s\Pi^m \ {}^s u = \Pi^m z_s{}^m \ {}^s u, \tag{7}$$

and, by (5), (6), (7), we have

$$c_s = u^{-1} z_s{}^m \ {}^s u \Rightarrow c \sim z^m \Rightarrow \gamma = \gamma_{K/k}^m.$$

In other words, $H^1(G, U_K)$ is a cyclic group generated by the canonical class $\gamma_{K/k}$.

Let us count the order of the group. Consider the short exact sequence of G-groups

$$1 \longrightarrow U_K \longrightarrow K^\times \longrightarrow \mathbf{Z} \longrightarrow 1$$

where the map $K^\times \to \mathbf{Z}$ is the valuation v_K with the trivial action of G on $\mathbf{Z}$. Passing to cohomology, we have the exact sequence:

$$\begin{aligned} 1 \to U_k \to k^\times \to \mathbf{Z} \to H^1(G, U_K) \\ \to H^1(G, K^\times) = 1. \end{aligned} \tag{8}$$

Because of the relation $v_K(x) = ev_k(x)$, $x \in k$, $e = e(K/k)$ being the ramification index for K/k, we obtain from (8)

Theorem 1. *The group $H^1(G, U_K)$ is cyclic of order $e = e(K/k)$ generated by $\gamma_{K/k}$.*

2000 Mathematics Subject Classification. 11F85.

4. $\boldsymbol{i_\gamma(K/k)}$. We shall obtain a preliminary formula for $i_\gamma(K/k)$. For any $\gamma = [c]$ in $H^1(G, U_K)$, by Theorem 1, there is an $m \in \mathbf{Z}$, $0 \le m < e$ so that $\gamma = {\gamma_{K/k}}^m$ or $c \sim z^m$. In case $m = 0$, we have $\gamma = [1]$, and $M_1 = \mathcal{O}_k$, $P_1 = \operatorname{Tr} \mathcal{O}_K$. Then we set

$$(9) \qquad i_1(K/k) = (\mathcal{O}_k : \operatorname{Tr} \mathcal{O}_K).$$

In case $m > 0$, the condition $0 < m < e$ implies that

$$(10) \qquad \mathcal{O}_k \cap \mathfrak{P}^m = \mathfrak{p}.$$

Back to (1) with $\gamma = [c] = {\gamma_{K/k}}^m = [z^m]$, assuming still $m > 0$ and $c = z^m$ without loss of generality, we obtain

$$\begin{aligned} a \in M_c \Leftrightarrow c_s{}^s a = a \Leftrightarrow \frac{{}^s\Pi^m}{\Pi^m} \cdot {}^s a = a \Leftrightarrow {}^s\Pi^{m\,s} a \\ = \Pi^m a \Leftrightarrow \Pi^m a \in \mathcal{O}_k \Leftrightarrow a \in \frac{\mathcal{O}_k}{\Pi^m} \cap \mathcal{O}_K \\ = \frac{\mathcal{O}_k \cap \Pi^m \mathcal{O}_K}{\Pi^m} = \frac{\mathcal{O}_k \cap \mathfrak{P}^m}{\Pi^m} = \frac{\mathfrak{p}}{\Pi^m} \end{aligned}$$

and so

$$(11) \qquad M_c = \frac{\mathfrak{p}}{\Pi^m}.$$

Next we look at (2). This time, for $a \in \mathcal{O}_K$, we have

$$\begin{aligned} p_c(a) &= \sum_{s \in G} c_s{}^s a = \sum_{s \in G} \frac{{}^s\Pi^m}{\Pi^m} \cdot {}^s a \\ &= \frac{1}{\Pi^m} \sum_{s \in G} {}^s\Pi^m a = \frac{\operatorname{Tr}(\Pi^m a)}{\Pi^m}. \end{aligned}$$

Therefore we have

$$(12) \qquad P_c = \frac{\operatorname{Tr} \mathfrak{P}^m}{\Pi^m}.$$

From (3), (11), (12), it follows that

$$(13) \qquad i_\gamma(K/k) = (\mathfrak{p} : \operatorname{Tr} \mathfrak{P}^m).$$

If we define an integer $r_\gamma = r_\gamma(K/k)$ by the relation, including the case $\gamma = 1$,

$$(14) \qquad \operatorname{Tr} \mathfrak{P}^m = \mathfrak{p}^{r_\gamma},$$

then, from (13), we have

$$(15) \qquad i_\gamma(K/k) = N\mathfrak{p}^{r_\gamma(K/k)-1}, \quad \gamma \ne 1,$$

where $N\mathfrak{p} = (\mathcal{O}_k : \mathfrak{p})$. As for $\gamma = 1$, in view of (9), we have

$$(16) \qquad i_1(K/k) = (\mathcal{O}_k : \mathfrak{p}^{r_1}) = N\mathfrak{p}^{r_1}.$$

5. $\boldsymbol{r_\gamma(K/k)}$. We want to express the number $r_\gamma = r_\gamma(K/k)$ in (14), (16) in terms of other basic invariants of K/k.

First, we shall consider the case $\gamma \ne 1$. Starting with (14), we have

$$(17) \qquad \begin{aligned} \operatorname{Tr} \mathfrak{P}^m = \mathfrak{p}^r \Rightarrow \mathcal{O}_k &= \mathfrak{p}^{-r} \operatorname{Tr} \mathfrak{P}^m \\ &= \operatorname{Tr}(\mathfrak{p}^{-r} \mathfrak{P}^m) = \operatorname{Tr} \mathfrak{P}^{-er+m} \end{aligned}$$

where $e = e(K/k)$ denotes the ramification index for K/k, namely

$$\mathfrak{p} = \mathfrak{P}^e.$$

Next, let $\mathfrak{D} = \mathfrak{D}(K/k)$, the different for K/k, and let $t = t(K/k)$ be defined by

$$\mathfrak{D} = \mathfrak{P}^t.$$

Since (17) means that $\mathfrak{P}^{-er+m} \subset \mathfrak{D}^{-1}$ we infer that

$$r \le \frac{t+m}{e}.$$

Conversely, a similar argument starting with the relation $\operatorname{Tr} \mathfrak{P}^m \not\subset \mathfrak{p}^{r+1}$ implies that

$$\frac{t+m}{e} < r + 1.$$

Cosequently we get

$$(18) \qquad r_\gamma(K/k) = \left[\frac{t+m}{e}\right]$$

and, by (15),

$$(19) \qquad i_\gamma(K/k) = (N\mathfrak{p})^{\left[\frac{t+m}{e}\right]-1}, \quad \gamma \ne 1.$$

In case $\gamma = 1$, starting with (16) we have

$$(20) \qquad r_1(K/k) = \left[\frac{t}{e}\right]$$

and, by (17),

$$(21) \qquad i_1(K/k) = N\mathfrak{p}^{\left[\frac{t}{e}\right]}.$$

As is well-known, there is a formula for t in terms of higher ramification groups:

$$V_i = \{s \in G; {}^s a \equiv a \pmod{\mathfrak{P}^{i+1}}\}, \quad i \ge -1$$

where $V_{-1} = G$, $V_0 = T$, the inertia group and $V_1 = V$, the (first) ramification group. The set $\{V_i\}$, $i \ge -1$, forms a normal series of G such that $V_i = 1$ for $i \gg 1$. The formula is

$$(22) \qquad t = (e-1) + \sum_{i=1}^{\infty} (|V_i| - 1).$$

Then we find that $e - 1 \le t$. Furthermore, we have

$$(23) \qquad \begin{aligned} t = e - 1 \Leftrightarrow V = 1 \Leftrightarrow p \nmid e \\ \Leftrightarrow K/k : \text{tamely ramified.} \end{aligned}$$

6. Vanishing of $i_\gamma(K/k)$. Having obtained formulas (19), (21) for $i_\gamma(K/k)$, one derives from them many results. We will here consider the question under what conditions $i_\gamma(K/k)=1$.

(i) K/k is unramified. $(e=1,\ t=0)$. In this case, $H^1(G,U_K)=1$ by Theorem 1, and so m=0. The case (19) is absent and we have $i_1(K/k)=1$ by (21).

(ii) K/k is tamely ramified. $(e-1=t\neq 0)$. If $\gamma=1$, i.e. $m=0$, then

$$\left[\frac{t}{e}\right]=\left[\frac{e-1}{e}\right]=0$$

and so

$$i_1(K/k)=1. \tag{24}$$

On the other hand, if $\gamma\neq 1$, i.e. $m>0$, then

$$\left[\frac{e-1+m}{e}\right]-1=\left[\frac{m-1}{e}\right]=0$$

and so

$$i_\gamma(K/k)=1. \tag{25}$$

(iii) K/k is wildly ramified, $(0\neq e-1<t)$. If $\gamma=1$, then

$$\left[\frac{t}{e}\right]=0.$$

But, then, $e-1<t<e$ which is absurd.
If $\gamma\neq 1$, then

$$\left[\frac{t+m}{e}\right]=1.$$

Then we have $e\le t+m<2e$. Summing up,

Theorem 2. *If K/k is unramified, then $i_1(K/k)=1$. ($\gamma=1$ is the only possibility).*

If K/k is tamely ramified, then $i_\gamma(K/k)=1$ for all γ. If K/k is wildly ramified, then $i_\gamma(K/k)=1\Leftrightarrow\gamma\neq 1$ and $e\le t+m<2e$.

7. Totally ramified extensions. Let K/k be a totally ramified Galois extension of $\mathfrak{p}$-adic fields. As is well-known, such an extension can be written as $K=k(\Pi)$ with a prime element Π whose minimal polynomial $f(X)\in\mathcal{O}_k[X]$ is of Eisenstein type. Then we have

$$t=v_K(f'(\Pi))\qquad \mathfrak{D}=\mathfrak{P}^t.$$

Since $e=(K:k)$ in our case, we have, from (19), (21),

$$i_\gamma(K/k)=(N\mathfrak{p})^{\left[\frac{v_K(f'(\Pi))+m}{e}\right]-1},\quad \gamma\neq 1 \tag{26}$$

and

$$i_1(K/k)=N\mathfrak{p}^{\left[\frac{v_K(f'(\Pi))}{e}\right]}. \tag{27}$$

Consider, in particular, a polynomial

$$f(X)=X^e-a\in\mathcal{O}_k[X],\quad v_\mathfrak{p}(a)=1,\quad p\nmid e. \tag{28}$$

Let Π be a root of $f(X)=0$. Assume that k contains all e-th roots of 1. Then K/k is a totally and tamely ramified Galois extension. Since $f'(\Pi)=e\Pi^{e-1}$ we have $v_K(f'(\Pi))=e-1$ and one checks again the vanishing, for all $\gamma\in H^1(G,U_K)$, of $i_\gamma(K/k)$ for Kummer extensions.

8. p^n-th cyclotomic fields. Let p be an odd prime number, n a natural number, $\mathbf{Q}_p$ the field of p-adic numbers and ζ a primitive p^n-th root of unity taken from the algebraic closure of $\mathbf{Q}_p$. We set $k=\mathbf{Q}_p$, $K=\mathbf{Q}_p(\zeta)$ in accordance with notation in **1**. One knows that $\Pi=\zeta-1$ is a prime element in $\mathcal{O}_K$. Then our canonical class $\gamma_{K/k}=[c]$ is given by a system of *cyclotomic units*:

$$c_s=\frac{{}^s\Pi}{\Pi}=\frac{{}^s\zeta-1}{\zeta-1},\quad s\in G.$$

For each n, we have

$$e=\varphi(p^n),\quad t=n\varphi(p^n)-p^{n-1}. \tag{29}$$

In what follows, we shall restrict our attension on the canonical class $\gamma_{K/k}$, for simplicity.

Case 1. $n=1$. We have $e=p-1$ and $t=p-2$. Then $t=e-1$ and so K/k is tamely ramified by (23) and hence $i_\gamma(K/k)=1$ for all γ by Theorem 2.

Case 2. $n=2$. We have $e=p(p-1)$ and $t=p(2p-3)$. It is easy to check that

$$e-1<t<2e-1,\quad\text{or}\quad e<t+1<2e.$$

So K/k is wildly ramified by (23). However, we have $i_{\gamma_{K/k}}(K/k)=1$ by Theorem 2 with $m=1$.

Case 3. $n\ge 3$. From (29), it follows that

$$n-1<\frac{t+1}{e}=n-\frac{p^{n-1}-1}{\varphi(p^n)}<n$$

and

$$r_{\gamma_{K/k}}=n-1,\quad\text{for}\quad n\ge 3. \tag{30}$$

Consequently, from (15), (30), we obtain

Theorem 3. *Let p be an odd prime, n a natural number, ζ a primitive p^n-th root of 1 and $K=\mathbf{Q}_p(\zeta)$. Then we have*

$$i_{\gamma_{K/\mathbf{Q}_p}}=1\quad\textit{when}\quad n=1,\quad =p^{n-2}\quad\textit{when}\quad n\ge 2.$$

References

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

[2] Lee, S. M., and Ono, T.: On a certain invariant for real quadratic fields. (To appear in Proc. Japan Acad.).

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