37. *A Note on Poincaré Sums of Galois Representations*

By Takashi ONO
Department of Mathematics, The Johns Hopkins University

(Communicated by Shokichi IYANAGA, M. J. A., May 13, 1991)

This note is a fruit of recent conversations with Mr. Morishita on building non-abelian Kummer theory after the model of Weil [6].

Let k be any field, K be a finite Galois extension of k and ρ be a k-representation of the Galois group $G=G(K/k)$. Denote by K_ρ the intermediate field of the extension K/k which corresponds to the subgroup $\operatorname{Ker}\rho$ of G by Galois theory. In this paper, we shall supply an elementary construction of K_ρ over k which works simultaneously for all ρ's ((2.6) Theorem). When the characteristic of k is zero, we shall rewrite everything in terms of the character χ of ρ (§ 3).

§ 1. **$g(\theta)$.** Notation being as above, consider the following elements in the group ring $K[G]$:

(1.1) $$g(x)=\sum_{s\in G} x^s s, \qquad x\in K.^{1)}$$

We want to find $x\in K$ such that $g(x)\in K[G]^\times$, the group of invertible elements of the ring $K[G]$. Let us call a $\theta\in K$ a normal basis element if the set $\{\theta^s ; s\in G\}$ forms a normal basis for K/k.

(1.2) **Proposition.** *If $\theta\in K$ is a normal basis element for K/k, then $g(\theta)\in K[G]^\times$.*

Proof. Let $u=\sum_t x_t t$ with unknown $x_t\in K$. We have
$$g(\theta)u=\sum_s \theta^s s\sum_t x_t t=\sum_{s,t}\theta^{st^{-1}}x_t s$$
$$=\sum_s\left(\sum_t \theta^{st^{-1}}x_t\right)s.$$
Since $\det(\theta^{st^{-1}})\neq 0$,[2] one finds x_t, $t\in G$, so that
$$\sum_t \theta^{st^{-1}}x_t=\begin{cases}1 & \text{if } s=1,\\ 0 & \text{if } s\neq 1.\end{cases}$$
Hence $g(\theta)u=1$, i.e., $u=\sum_t x_t t$ is a right inverse of $g(\theta)$ in $K[G]$. Similarly, one finds a left inverse v of $g(\theta)$. Since $u=v$ by the associativity of multiplication in $K[G]$, $g(\theta)$ is an invertible element. Q.E.D.

§ 2. **$P_\rho(\theta)$.** K, k, G being as before, let ρ be a k-representation of G of degree n:

(2.1) $$\rho: G\longrightarrow GL_n(k).$$

The map ρ extends, by K-linearity, to a K-representation, written still by ρ, of the ring $K[G]$:

---

1) If $x\in K$ and $s\in G$, then the action of s on x will be denoted by sx or x^s. Since we use the convention $s(tx)=(st)x$, $t\in G$, we have $(x^t)^s=x^{st}$.

2) As for basic facts on normal bases, see [3, pp. 290–295].

(2.2) $$\rho: K[G] \longrightarrow M_n(K).$$

Now we have the *Poincaré sum* for ρ:

(2.3) $$P_\rho(x) \overset{\text{def}}{=} \rho(g(x)) = \sum_{s \in G} x^s \rho(s), \qquad x \in K,$$

where $g(x)$ is defined by (1.1).

(2.4) **Theorem.** *If θ is a normal basis element for K/k, then $P_\rho(\theta) \in GL_n(K)$ and $\rho(s) = P_\rho(\theta) P_\rho(\theta)^{-s}$.*

Proof. By (1.2), there is a $u \in K[G]$ such that $g(\theta)u = 1$. Hence $1 = \rho(g(\theta))\rho(u) = P_\rho(\theta)\rho(u)$ which implies that $P_\rho(\theta) \in GL_n(K)$. Next, putting $P = P_\rho(\theta)$, we have

$$\begin{aligned} \rho(s)P^s &= \rho(s)(\sum_t \theta^t \rho(t))^s = \rho(s) \sum_t \theta^{st} \rho(t) \\ &= \sum_t \theta^{st} \rho(st) = \sum_t \theta^t \rho(t) = P.^{3)} \end{aligned}$$

Q.E.D.

If ρ': $G \to GL_n(k)$ is another k-representation, we can speak of the equivalence:

(2.5) $$\rho \underset{k}{\sim} \rho' \qquad \text{if } \rho'(s) = U\rho(s)U^{-1}, \qquad U \in GL_n(k).$$

For ρ, we denote by K_ρ the intermediate field of K/k which corresponds to $\operatorname{Ker} \rho$ by Galois theory.

(2.6) **Theorem.** *Let θ be any normal basis element for a Galois extension K/k. Then we have $K_\rho = k(P_\rho(\theta))$. In particular, $K_\rho = K_{\rho'}$ if $\rho \underset{k}{\sim} \rho'$.*

Proof. Let H be the subgroup of G corresponding to the field $k(P)$, $P = P_\rho(\theta)$. Then, by (2.4), we have, for $s \in G$,

$$s \in H \Longleftrightarrow P^s = P \Longleftrightarrow \rho(s) = 1 \Longleftrightarrow s \in \operatorname{Ker} \rho,$$

which proves that $K_\rho = k(P)$. Furthermore, since $\operatorname{Ker} \rho = \operatorname{Ker} \rho'$ if $\rho \underset{k}{\sim} \rho'$, we have $K_\rho = K_{\rho'}$. Q.E.D.

§3. **Characteristic zero case.** From now on, assume that the characteristic of k is zero. Denote by χ the character of a k-representation ρ of G ((2.1)) and also the character of the extended K-representation ρ of $K[G]$ ((2.2)). On taking the trace of each matrix in (2.3), we are led to

(3.1) $$P_\chi(x) \overset{\text{def}}{=} \chi(g(x)) = \sum_{s \in G} x^s \chi(s), \qquad x \in K,$$

and obtain

(3.2) **Theorem.** *For any normal basis element θ for K/k, we have $K_\rho = k(P_\chi(\theta))$. In particular, $P_\chi(\theta) \neq 0$ if χ is nontrivial.*[4)]

Proof. Clearly $k(P_\chi(\theta)) \subset k(P_\rho(\theta)) = K_\rho$ by (2.6). The other inclusion $k(P_\chi(\theta)) \supset K_\rho$ follows from implications below:

$$\begin{aligned} P_\chi(\theta)^s = P_\chi(\theta) &\Longleftrightarrow \sum_{t \in G} \theta^{st} \chi(t) = \sum_{t \in G} \theta^t \chi(t) \\ &\Longleftrightarrow \chi(s^{-1}t) = \chi(t) \qquad \text{for all } t \in G \\ &\Longrightarrow \chi(s) = \chi(1) \Longleftrightarrow s \in \operatorname{Ker} \rho, \end{aligned}$$

---

3) Note that we did not appeal to ready-made "Hilbert 90" for each 1-cocycle ρ separately. On the other hand, Hilbert 90 deals with arbitrary 1-cocycle (not a homomorphism) and so our method does not work immediately to prove the invertibility of Poincaré sums for general 1-cocycles (see [5, p. 159]).

4) χ is trivial $\Longleftrightarrow$ $\operatorname{Ker} \rho = G$.

where we used that $\{\theta^s; s \in G\}$ is a basis for K/k and that the characteristic is zero (see [1, p. 35]). Q.E.D.

(3.3) **Remark.** In view of (3.2) we can write K_χ for K_ρ, i.e., $K_\chi = k(P_\chi(\theta))$.

§4. **Examples and comments.** (4.1) (Cyclotomic extension). Let $k=\boldsymbol{Q}$, $K=k(\zeta)$, $\zeta=a$ primitive lth root of 1, l being a prime $\neq 2$. ζ is a normal basis element for K/k. We have $G \approx \boldsymbol{F}_l^\times$. The unique character χ of G of order 2 is identified with the Legendre character of $\boldsymbol{F}_l^\times$. We have

Poincaré sum $P_\chi(\zeta) = \sum_{s \in G} \zeta^s \chi(s) = \sum_{x \in \boldsymbol{F}_l^\times} \zeta^x (x/l)$, the Gauss sum,

and $K_\chi = \boldsymbol{Q}(P_\chi(\zeta)) = \boldsymbol{Q}(\sqrt{l^*})$, $l^* = (-1)^{(l-1)/2} l$.

(4.2) (Cyclic Kummer extension). Assume that k contains a primitive nth root ζ of 1.[5] Let K/k be a cyclic extension of degree n with $G = \langle s \rangle$, θ be any normal basis element for K/k and χ the linear character of G defined by $\chi(s) = \zeta$. We have

Poincaré sum $P_\chi(\theta) = \sum_{i=0}^{n-1} \theta^{s^i} \zeta^i = (\theta, \zeta)$, the Lagrange resolvent.

Since $\operatorname{Ker} \chi = 1$, we have $K = K_\chi = k((\theta, \zeta))$; furthermore, as $\chi(s) = \zeta = (\theta, \zeta)^{1-s}$ by (2.4), we have $(\theta, \zeta)^n = a \in k$, i.e., $K = k(\sqrt[n]{a})$.

(4.3) (Regular representation). Let K/k be any Galois extension[5] and ρ be the regular representation of G. ρ is a k-representation; in fact, a $\boldsymbol{Q}$-representation, and $\operatorname{Ker} \rho = 1$, i.e., $K_\chi = K_\rho = K$. For a normal basis element θ for K/k, we have $P_\chi(\theta) = n\theta$, $n = [K:k]$.

(4.4) (χ's parametrize all normal subextensions of K/k). (4.3) enables us to find a k-representation ρ of G such that $L = K_\chi$ for a given normal subextension L/k of K/k. In fact, let N be the normal subgroup of G corresponding to L, r be the regular representation of G/N and ρ be the k-representation of G obtained naturally:

$$\rho: G \longrightarrow G/N \xrightarrow{r} GL_m(k), \qquad m = [L:k].$$

As $\operatorname{Ker} r = 1$, we have $\operatorname{Ker} \rho = N$ and hence $L = K_\chi$.

References

[1] Feit, W.: Characters of Finite Groups. Benjamin, New York-Amsterdam (1967).

[2] Iwasawa, K.: Daisukansuron. Theory of Algebraic Functions. Iwanami, Tokyo (1952) (in Japanese).

[3] Jacobson, N.: Basic Algebra. I. W. H. Freeman and Company, New York (1985).

[4] Morishita, M.: A Note on Non-abelian Kummer-Iwasawa Theory (unpublished).

[5] Serre, J.-P.: Corps Locaux. Hermann, Paris (1962).

[6] Weil, A.: Généralisation des fonctions abéliennes. P. et App., (IX) 17, pp. 47–87 (1938).

[5] k is of characteristic zero.