71. A Note on Poincaré Sums of Galois Representations. III

By Takashi ONO
Department of Mathematics, The Johns Hopkins University

(Communicated by Shokichi IYANAGA, M. J. A., Oct. 14, 1991)

This is a continuation of our preceding papers [4], [5]. In this paper, we shall notice a formalism of Poincaré sums $P(K/k,\chi)$ for any Galois extension (in characteristic zero) which is the analogue of Artin's formalism of L-series in [1]. Brauer's theorem on induced characters will describe $P(K/k,\chi)$ in terms of such sums for cyclic Kummer extensions, i.e., of the Lagrange resolvents.

§1. Supernormal bases. To define Poincaré sums for many Galois extensions simultaneously, we need to modify the existence proof of ordinary normal bases.

Let k be a field of characteristic zero and K/k be a finite Galois extension with the Galois group $G=G(K/k)$. An element $\theta\in K$ will be called a *supernormal* basis elements for K/k if θ is a normal basis element for each Galois extension K/L, $k\subseteq L\subseteq K$, i.e., if $\{\theta^s\}$, $s\in G(K/L)$, forms a normal basis for K/L for each L.

(1.1) **Proposition.** *A supernormal basis always exists.*

Proof. We modify the ordinary proof as follows.[1] Let $X=X_G=\{X_s\}_{s\in G}$ be variables indexed by G. For a subgroup $H=G(K/L)$ of G, we set $X_H=\{X_s\}_{s\in H}$, $P_H(X_H)=\det(X_{st})$, $s,t\in H$ and $P(X)=\prod_{H\subseteq G}P_H(X_H)$. The values of polynomials $P_H(X_H)$ after putting $X_1=1$, $X_s=0$ for $s\neq 1$, are ± 1 and so is the value of $P(X)$. Hence, by the algebraic independence of the set G over K, there exists an element $\theta\in K$ such that $P(\theta^s)\neq 0$, $s\in G$, which implies that $P_H(\theta^s)=\det(\theta^{st})\neq 0$, $s,t\in H$, for all H. Therefore $\{\theta^s\}_{s\in H}$ forms a normal basis for K/L, Q.E.D.

(1.2) **Remark.** From now on, we shall fix once for all a supernormal basis element θ for a given K/k. If a subextension L/k of K/k happens to be a Galois extension, then we shall agree to use $T_{K/L}\theta$ as the normal basis element for L/k.

§2. Induction of characters. In view of (1.2), for K/k and L, we can speak of the Poincaré sum

(2.1) $$P(K/L,\psi)\overset{\text{def}}{=}\sum_{s\in H}\theta^s\psi(s),\qquad H=G(K/L),$$

where ψ is an L-character of $G(K/L)$.[2]

If, in particular, L/k is a Galois extension, then we have

---

[1] See e.g. [3] p.294 for normal bases. The validity of (1.1) was first communicated to me by Mr. Morishita; his proof is based on the method in [2] p.201.

[2] A character χ of a finite group G is an F-character if χ is the trace of an F-representation $\rho: G\to GL_n(F)$.

(2.2) $$P(L/k,\varphi)\overset{\mathrm{def}}{=}\sum_{r\in G/H}(T_{K/L}\theta)^r\varphi(r),$$

where φ is a k-character of $G/H=G(L/k)$.

For a k-character ψ of H, denote by ψ^G the k-character of G induced from ψ. Then

(2.3) $$P(K/k,\psi^G)=\sum_{r\in G/H}P(K/L^r,\psi^r)$$

where $\psi^r(u)=\psi(r^{-1}ur)$, $u\in H^r=rHr^{-1}$.[3)]

Proof of (2.3). For a function f on H we associate a function f^0 on G by

$$f^0(s)=\begin{cases} f(s) & \text{if } s\in H,\\ 0 & \text{if } s\notin H.\end{cases}$$

Then we have

(2.4) $$\psi^G(s)=\frac{1}{h}\sum_{t\in G}\psi^0(t^{-1}st),\qquad h=|H|.$$

Hence, by (2.1), (2.4), we have

$$P(K/k,\psi^G)=\frac{1}{h}\sum_{s\in G}\theta^s\sum_{t\in G}\psi^0(t^{-1}st)=\frac{1}{h}\sum_{t,s\in G}\theta^s\psi^0(t^{-1}st)$$

$$=\frac{1}{h}\sum_{t\in G}\sum_{s\in H^t}\theta^s\psi^t(s)=\frac{1}{h}\sum_{t\in G}P(K/L^t,\psi^t)=\sum_{r\in G/H}P(K/L^r,\psi^r),$$

Q.E.D.

If L/k is a Galois extension, for a k-character φ of G/H, we denote by φ' the k-character of G given by $\varphi'(s)=\varphi(sH)$. Then we have

(2.5) $$P(K/k,\varphi')=P(L/k,\varphi),\qquad L/k \text{ galois}.$$

In fact,

$$P(K/k,\varphi')=\sum_{s\in G}\theta^s\varphi(sH)=\sum_{r\in G/H}\sum_{t\in H}\theta^{rt}\varphi(rtH)=\sum_{r\in G/H}\sum_{t\in H}\theta^{rt}\varphi(r)$$

$$=\sum_{r\in G/H}\Big(\sum_{t\in H}\theta^{rt}\Big)\varphi(r)=\sum_{r\in G/H}(T_{K/L}\theta)^r\varphi(r)=P(L/k,\varphi),$$ Q.E.D.

§3. **Galois extensions of type (*K*).** Notation being as before, a Galois extension K/k is said to be a *(K)-extension* if k contains the mth roots of unity where m is the exponent of $G=G(K/k)$. We shall also call m the exponent of K/k. Needless to say that K/k is a Kummer extension if and only if K/k is an abelian (K)-extension. By a theorem of Brauer ([6] p. 94), if K/k is a (K)-extension, every character of every subgroup of G is a k-character.

(3.1) **Remark.** Let K/k be a cyclic Kummer extension of degree m and χ be a linear character of $G=\langle g\rangle$. Put $\zeta=\chi(g)$, an mth root of unity. Then we have $P(K/k,\chi)=\sum_{i=0}^{m-1}\theta^{g^i}\zeta^i=(\theta,\zeta)_{K/k}$, the Lagrange resolvent. We know that $(\theta,\zeta)^m_{K/k}\in k^\times$.

(3.2) **Theorem.** *Let K/k be a (K)-extension and χ be a character of $G=G(K/k)$. Then the Poincaré sum $P(K/k,\chi)$ is a linear combination with integer coefficients of Lagrange resolvents.*

---

3) Here we identify G/H with a system of representatives of left cosets mod. H. Note that each of L^r, H^r, ψ^r makes sense (independent of choice of r mod. H) and that ψ^r is a k-character of H^r.

Proof. By a theorem of Brauer together with a property of supersolvable groups (cf. [6] p. 78, Theorem 20), we have

$$\chi=\sum_{i=1}^{N} a_i\psi_i^G, \qquad a_i \in \boldsymbol{Z}, \tag{3.3}$$

where ψ_i is a linear character of some $H_i \subseteq G$. Since $P(K/k, \chi)$ is additive in χ, we have, by (2.3)

$$P(K/k,\chi)=\sum_{i=1}^{N} a_i P(K/k, \psi_i^G)=\sum_{i=1}^{N} a_i \sum_{r\in G/H_i} P(K/L_i^r, \psi_i^r), \qquad H_i=G(K/L_i). \tag{3.4}$$

Putting $H=H_i$, $L=L_i$, we have, by (2.5),

$$P(K/L^r, \psi^r)=P(K_{\psi^r}/L^r, \psi^r), \tag{3.5}$$

where K_{ψ^r}/L^r is cyclic Kummer as ψ^r is linear, Q.E.D.[4]

§4. **An example.** Let F be a real Galois extension over $\boldsymbol{Q}$ such that $G=G(F/\boldsymbol{Q})=Q_8$, the quaternion group: $Q_8=\langle\sigma_1, \sigma_2\rangle$, $\sigma_1^4=1$, $\sigma_1^2=\sigma_2^2=\varepsilon$, $\sigma_2\sigma_1\sigma_2^{-1}=\sigma_1^{-1}$. For example, $F=\boldsymbol{Q}(\alpha)$, $\alpha=((2+\sqrt{2})(3+\sqrt{3}))^{1/2}$, is such a field. As Q_8 has exponent 4, $F/\boldsymbol{Q}$ is not a (K)-extension. To get a (K)-extension, we set $K=kF$, $k=\boldsymbol{Q}(i)$; we have $G(K/k)=G(F/\boldsymbol{Q})=Q_8$. The only nonlinear irreducible character χ of Q_8 is given by $\chi(1)=2$, $\chi(\varepsilon)=-2$ and $\chi(s)=0$ for $s\neq 1, \varepsilon$. If θ is a supernormal basis element for K/k, then

$$P(K/k,\chi)=2(\theta-\theta^{\varepsilon}). \tag{4.1}$$

Note that $K=k(P(K/k,\chi))$ since $\operatorname{Ker}\chi^*=\{s\in G\,;\,\chi^*(s)=\chi(s)/\chi(1)=1\}=1$. Let $H_\nu=\langle\sigma_\nu\rangle$, $\nu=1,2,3$, with $\sigma_3=\sigma_1\sigma_2$. Let ψ_ν, $\nu=1,2,3$, be the linear character of H_ν such that $\psi_\nu(\sigma_\nu)=i$. Then one verifies that

$$\chi=\psi_\nu^G, \qquad \nu=1,2,3. \tag{4.2}$$

Let L_ν be the fixed field of H_ν. As $L_\nu=L_\nu^s$ for all $s\in G$ and $\psi_\nu^{r_\nu}(\sigma_\nu)=-i$ whenever $r_\nu\notin H_\nu$, we have, by (2.3), (4.2),

$$\begin{aligned} P(K/k,\chi)&=P(K/L_\nu, \psi_\nu)+P(K/L_\nu, \psi_\nu^{r_\nu})\\ &=(\theta, i)_{K/L_\nu}+(\theta,-i)_{K/L_\nu}, \qquad \nu=1,2,3. \end{aligned} \tag{4.3}$$

By abuse of notation, let us put

$$P=P(K/k,\chi), \quad A_\nu=(\theta, i)_{K/L_\nu}, \quad B_\nu=(\theta,-i)_{K/L_\nu}, \qquad \nu=1,2,3. \tag{4.4}$$

In view of properties of the Lagrange resolvents, we have

$$A_\nu^4,\ B_\nu^4\in L_\nu^\times, \quad A_\nu^{\sigma_\nu}=-iA_\nu, \quad B_\nu^{\sigma_\nu}=iB_\nu \qquad \nu=1,2,3.\text{[5]} \tag{4.5}$$

From (4.3), (4.5), we have

$$P=A_\nu+B_\nu, \quad P^{\sigma_\nu}=-i(A_\nu-B_\nu), \qquad \nu=1,2,3. \tag{4.6}$$

As $K=k(P)$ and $P^{\varepsilon}=-P$, the minimal polynomial $f_P(X)$ of P over k must be

$$\begin{aligned} f_P(X)&=\prod_{\nu=0}^{3}(X^2-(P^{\sigma_\nu})^2)\\ &=(X^4-4A_1B_1X^2-(A_1^2-B_1^2)^2)(X^2+(A_2-B_2)^2)(X^2+(A_3-B_3)^2).\text{[6]} \end{aligned} \tag{4.7}$$

Since coefficients of $f_P(X)$ are in k, (4.7) provides us with four algebraic relations over k of six resolvents.

---

[4] In general, for K/k and a k-representation ρ of $G=G(K/k)$, we denote by K_χ, $\chi=\chi^\rho$, the subfield corresponding to $\operatorname{Ker}\rho$ (cf. [4]). Hence χ can also be considered as a character of $G/\operatorname{Ker}\rho=G(K_\chi/k)$

[5] Note also that $A_1^{\sigma_2}=\frac{1}{2}(i(B_2-A_2)+(B_3-A_3))$, $B_1^{\sigma_2}=\frac{1}{2}(i(B_2-A_2)-(B_3-A_3))$, etc.

[6] We put $\sigma_0=1$.

References

[1] Artin, E.: Zur Theorie der L-Reihen mit allgemeinen Gruppencharakteren. Hamb. Abh., **8**, 292–306 (1930).

[2] Fujisaki, G.: Fields and Galois Theory. Iwanami, Tokyo (1977) (in Japanese).

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

[4] Ono, T.: A note on Poincaré sums of Galois representations. Proc. Japan Acad., **67A**, 145–147 (1991).

[5] ——: A note on Poincaré sums of Galois representations. II. ibid., **67A**, 240–242 (1991).

[6] Serre, J.-P.: Linear Representations of Finite Groups. Springer-Verlag, New York (1977).