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

$$g(\theta)u=\sum_s \theta^s s\sum_t x_t t=\sum_{s,t}\theta^{st^{-1}}x_t s$$
$$=\sum_s\Big(\sum_t \theta^{st^{-1}}x_t\Big)s.$$

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) $$\rho\colon G\longrightarrow GL_n(k).$$

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].