ISRAEL JOURNAL OF MATHEMATICS 116 (2000), 345–365

ON THE GALOIS MODULE STRUCTURE OF SEMISIMPLE HOLOMORPHIC DIFFERENTIALS

BY

PEDRO RICARDO LÓPEZ-BAUTISTA

Departamento de Ciencias Básicas, Universidad Autónoma Metropolitana-Azcapotzalco Av. San Pablo No. 180, Col. Reynosa Tamaulipas Azcapotzalco D.F., C.P. 02200, México, D.F.
e-mail: rlopez@hp9000a1.uam.mx

AND

GABRIEL DANIEL VILLA-SALVADOR*

Departamento de Matemáticas, Centro de Investigación y de Estudios Avanzados del I.P.N. Apartado Postal 14-740, 07000 México, D.F.
e-mail: villa@math.cinvestav.mx

ABSTRACT

Let L/K be a finite Galois p-extension of algebraic function fields of one variable over an algebraically closed field k of characteristic p, with Galois group $G = \mathrm{Gal}(L/K)$. The space $\Omega_L^s(0)$ of semisimple holomorphic differentials of L is the k-vector space of holomorphic differentials which are fixed by the Cartier operator. We obtain the isomorphism classes and multiplicities of the summands in a Krull–Schmidt decomposition of the $k[G]$-module $\Omega_L^s(0)$ into a direct sum of indecomposable $k[G]$-modules.

1. Introduction

Let L be an algebraic function field in one variable over an algebraically closed constant field k. The space $\Omega_L(0)$ of holomorphic differentials of L forms a k-vector space of dimension g_L, the genus of L. Let G be a finite group of automorphisms of L/k. There is a natural action of G on $\Omega_L(0)$. Therefore,

* Partially supported by CONACyT, project No. 25063-E.
Received March 11, 1998 and in revised form January 18, 1999

$\Omega_L(0)$ has structure of $k[G]$-module where $k[G]$ is the group ring with coefficients in k.

The problem of determining the $k[G]$-module structure of $\Omega_L(0)$ has been studied by many authors (see [16] for more details). In the classical case, that is, when k is the field of complex numbers, following a suggestion of E. Hecke, Chevalley and Weil determined completely its structure for arbitrary G. However, if k has characteristic $p > 0$ this problem is still open.

An explicit determination of a $k[G]$-module A is one which determines the isomorphism classes and multiplicities of the indecomposable summands in a decomposition of A as direct sum of indecomposable $k[G]$-modules.

Assume now that G is a finite p-subgroup of $\mathrm{Aut}(L/k)$, where p is an arbitrary rational prime. Let K denote the field fixed by G, where k is a field of characteristic p.

In this situation we are interested in $\Omega_L^s(0)$, the submodule of $\Omega_L(0)$ generated by the holomorphic differentials of L which are invariant under $\mathcal{C}$, the Cartier operator. We have that $\Omega_L^s(0)$ is isomorphic as $k[G]$-module to the elements of order dividing p of the Jacobian of a smooth curve with function field L ([11], Proposition 10). It is well-known that as k-modules $\Omega_L^s(0) \cong k^{\tau_L}$, where τ_L is the Hasse–Witt invariant of L.

Nakajima ([8], Theorem 2) obtained two $k[G]$-exact sequences which determine implicitly the structure as $k[G]$-module of $\Omega_L^s(0)$, the first one when the extension L/K is ramified and the second one when the extension L/K is unramified. In the case L/K is ramified, Nakajima established the $k[G]$-exact sequence $0 \to \Omega_L^s(0) \to k[G]^{r-1+\tau_K} \to \ker(\Phi) \to 0$, where τ_K is the Hasse–Witt invariant of K,

$$\Phi = \bigoplus_{i=1}^{r} \Phi_i, \quad \Phi_i\Big(\sum_{\sigma \in G/G_i} a_\sigma \sigma\Big) = \sum_{\sigma\in G/G_i} a_\sigma,$$

and $G_1, \dots, G_r$ are the decomposition groups of the prime divisors $P_1, \dots, P_r$ of K ramified in L. Therefore, if L/K is ramified it follows that the implicit structure as $k[G]$-module of $\Omega_L^s(0)$ is given by

$$\Omega_L^s(0) \cong k[G]^u \oplus \Omega(\ker(\Phi))$$

where u is a nonnegative integer and Ω denotes the Heller's loop-space operation.

We are interested in the explicit structure as $k[G]$-module of $\Omega_L^s(0)$. This structure is known when L/K is an unramified extension [16], when there exists a fully ramified prime in the extension L/K [17] and finally when there exists a unique maximal decomposition group and this is normal in G [17]. This problem has been investigated by many authors (see [8], [12], [14], [16], and [17] for more details).

In this paper we obtain unconditionally and explicitly the Galois module structure of $\Omega_L^s(0)$ (Theorem 1). The work of A. Weiss on indecomposable modules for finite p-groups is crucial in the proof of the main result of this paper.

2. Notation and preparatory results

In this paper p will denote an arbitrary rational prime number and G a finite p-group.

We will denote the disjoint union of the sets $X_1, \ldots, X_n$ by $\biguplus_{i=1}^n X_i$, $\mathbb{N} := \{1, 2, 3, \ldots\}$, $\mathbb{N}_0 := \mathbb{N} \cup \{0\}$. For an arbitrary field k we have that if M is a finitely generated $k[G]$-module, then M is a projective $k[G]$-module if and only if M is an injective $k[G]$-module.

For a $k[G]$-module M, we denote by $M^G := \{m \in M: gm = m \text{ for all } g \in G\}$ and we define the map $\mathcal{N}: M \to M$ by

$$\mathcal{N}(m) = \Big(\sum_{g \in G} g\Big) m.$$

Any non-zero $k[G]$-module M can be written as a direct sum $M \cong \bigoplus_{i=1}^s M_i$ in terms of indecomposable $k[G]$-modules M_i. By the Krull–Schmidt–Azumaya Theorem ([3], Theorem 6.12), the components M_i's are uniquely determined up to isomorphism.

If F is a field and X is a finite set, we set $\widehat{X} := \sum_{x \in X} x \in F[X]$.

PROPOSITION 1: *Let G be a finite p-group and $H_1, \ldots, H_r$ subgroups of G. We consider the natural action of G on the set $S := \biguplus_{i=1}^r G/H_i$. Then, as $k[G]$-modules,*

$$\frac{\bigoplus_{i=1}^{r} k[G/H_i]}{ke^*} \cong \frac{k[S]}{k\widehat{S}} \tag{1}$$

where

$$ke^* = \left\{ \Big(\sum_{\sigma_1 \in G/H_1} a\sigma_1, \cdots, \sum_{\sigma_r \in G/H_r} a\sigma_r \Big) \in \bigoplus_{i=1}^{r} k[G/H_i]: a \in k \right\}.$$

Proof: We consider the $k[G]$-isomorphism

$$\phi: \bigoplus_{i=1}^{r} k[G/H_i] \to k[\biguplus_{i=1}^{r} G/H_i]$$

given by

$$\phi\left(\left(\sum_{\sigma_1\in G/H_1} a_{\sigma_1}\sigma_1,\cdots,\sum_{\sigma_r\in G/H_r} a_{\sigma_r}\sigma_r\right)\right)=\sum_{i=1}^{r}\sum_{\sigma_i\in G/H_i} a_{\sigma_i}\sigma_i.$$

Then, as $k[G]$-modules, $\bigoplus_{i=1}^r k[G/H_i] \cong k[\biguplus_{i=1}^r G/H_i]$. The result follows. ∎

Let P be a $k[G]$-module. We write $P = P^{(0)} \oplus P^{(1)}$ where $P^{(0)}$ is $k[G]$-injective and $P^{(1)}$ does not have injective $k[G]$-components. For a $k[G]$-exact sequence $0 \to M \to Y \to N \to 0$ with Y an injective $k[G]$-module, we set $\Omega^{\#}(M) := N^{(1)}$ and $\Omega(N) := M^{(1)}$. The module $\Omega^{\#}(M)$ is called the **dual of the Heller's loop-space operation of** M and $\Omega(N)$ is called the **Heller's loop-space operation of** N.

PROPOSITION 2: *Let k be a field and let G be a finite p-group. Let M be a finitely generated $k[G]$-module such that $M \cong M^{(1)}$. Then*

(a) $\Omega\left(\Omega^{\#}(M)\right) \cong M$ *as $k[G]$-modules.*
(b) $\Omega^{\#}(\Omega(M)) \cong M$ *as $k[G]$-modules.*
(c) *If M is an indecomposable $k[G]$-module, then $\Omega^{\#}(M)$ is an indecomposable $k[G]$-module.*
(d) *Let k be of characteristic p and $H \leq G$. Then $\Omega^{\#}(k[G/H])$ is an indecomposable $k[G]$-module and*

$$\Omega^{\#}(k[G/H]) \cong \frac{k[G]}{k[G/H]}$$

as $k[G]$-modules.

Proof: ([3], Propositions 78.4, 78.5 and [17]). ∎

Let L/k be a field of algebraic functions with k a perfect field of characteristic p.

From ([4], Theorem 2.1) and ([7], Corollary 4.6) it follows that L/k is a separably generated extension. Let x be a separating element of L, that is, the extension $L/k(x)$ is finite and separable. Therefore $L = k(x,y)$ for some $y \in L$. If y is not a separating element of L then $y^{1/p}$ is a separating element ([4], Corollary to Theorem 2.1), thus y^{1/p^t} is a separating element of L where t is the inseparability exponent of y over $k(x)$ and we have that $L = k(x, y^{1/p^t})$.

PROPOSITION 3: *Let L/k be a field of algebraic functions with k a perfect field of characteristic p such that x is a separating element of L. Then $L^p(x)/L^p$ is an inseparable extension of degree p and every element $f \in L$ can be written in a unique way as $f = \sum_{i=0}^{p-1} f_i^p x^i$ where $f_i \in L$, $i \in [\![0, p-1]\!]$.*

Proof: Since $L/k(x)$ is a separably generated extension, we have that $L = L^p k(x) = L^p(x)$. From ([7], Corollary 6.3) it follows that $\{x\}$ is a p-transcendence basis of L. From ([7], Lemma 6.4) it follows that $[L^p(x) : L^p] = p$. The extension $L^p(x)/L^p$ is inseparable. It follows that every element $f \in L$ can be written uniquely as $f = \sum_{i=0}^{p-1} f_i^p x^i$ where $f_i \in L$, $i \in [\![0, p-1]\!]$. ∎

Let $f \in L = L^p(x)$. We define the **Tate-trace** of f by

$$S_x(f) := S_x\left(\sum_{i=0}^{p-1} f_i^p x^i\right) = f_{p-1}^p.$$

We have that S_x is L^p-linear and that $S_x(f)^{1/p} = f_{p-1}$.

In the extension $L^p(x)/L^p$ we consider the formal derivation

$$D_x\left(\sum_{i=0}^{p-1} h_i^p x^i\right) = \sum_{i=1}^{p-1} i h_i^p x^{i-1}.$$

The k-vector space Ω_L of the differentials of L is an L-vector space and $\dim_L(\Omega_L) = 1$.

Let η be the unit divisor of L. We set $\Omega_L(0) := \{\omega\colon \omega \in \Omega_L$ and such that $\eta|\omega\}$.

The space $\Omega_L(0)$ is called **the space of holomorphic differentials of** L.

Let $\omega_0 \in \Omega_L - (0)$. Since $\dim_L(\Omega_L) = 1$ we have that every differential $\omega \in \Omega_L$ is expressed uniquely as $\omega = \varphi\omega_0$, $\varphi \in L$. Since k is a perfect field, then there exists a separating element x in L. We have that $dx \in \Omega_L$ is different from zero ([2], Theorem 4). Therefore every differential $\omega \in \Omega_L$ is expressed uniquely as $\omega = f dx$ for some $f \in L$. Furthermore, from Proposition 3 it follows that

$$\omega = \left(\sum_{i=0}^{p-1} f_i^p x^i\right) dx.$$

Now we consider k algebraically closed of characteristic p. We define $\mathcal{C}\colon \Omega_L \to \Omega_L$ the Cartier operator by $\mathcal{C}(\omega) = f_{p-1} dx$.

PROPOSITION 4: *The Cartier operator $\mathcal{C}$ does not depend on the separating element of the field L.*

Proof: Let x, y be two separating elements of L. If $\omega \in \Omega_L$ we have that $\omega = fdy$ for some $f = \sum_{i=0}^{p-1} f_i^p x^i \in L$ and $\omega = gdx$ for some $g \in L$. Therefore $\omega = fdy = fD_x(y)dx = gdx$. Since $\dim_L(\Omega_L) = 1$ it follows that $fD_x(y) = g$.

We have that

$$S_x(f) = S_x\Big(f\frac{1}{D_x(y)^{p-1}}\Big)$$

([13], Theorem 1). Hence, we obtain

$$\begin{aligned} \mathcal{C}(fdy) &= f_{p-1}dy = S_y(f)^{1/p}dy = S_x\left(f\frac{1}{D_x(y)^{p-1}}\right)^{1/p} dy \\ &= S_x\left(f\frac{1}{D_x(y)^{p-1}}\right)^{1/p} D_x(y)dx = \left(S_x\left(f\frac{1}{D_x(y)^{p-1}}\right) D_x(y)^p\right)^{1/p} dx \\ &= S_x\left(f\frac{D_x(y)^p}{D_x(y)^{p-1}}\right)^{1/p} dx = S_x\left(fD_x(y)\right)^{1/p} dx = S_x(g)^{1/p}dx \\ &= \mathcal{C}(gdx). \quad \blacksquare \end{aligned}$$

Let V, W be k-vector spaces. An application ϕ: $V \to W$ is said to be p^{-1}**-linear** if ϕ satisfies $\phi(v_1 + v_2) = \phi(v_1) + \phi(v_2)$ and $\phi(r\alpha) = r^{1/p}\phi(\alpha)$ $\forall r \in k, \forall \alpha \in V$.

Since η, the unit divisor of L, is an integral divisor it follows from ([12], Lemma 2.1) that the Cartier operator $\mathcal{C}$ is a map p^{-1}-linear such that $\mathcal{C}$: $\Omega_L(0) \to \Omega_L(0)$. Since k is algebraically closed we have that ([12], Theorem 2.2) $\Omega_L(0) \cong \Omega_L^s(0) \oplus \Omega_L^n(0)$, where $\Omega_L^s(0)$ is the subspace of **semisimple holomorphic differentials** of L and $\Omega_L^n(0)$ is the subspace of **nilpotent holomorphic differentials** of L, that is, $\Omega_L^n(0) = \{\omega \in \Omega_L(0)\colon \mathcal{C}^m(\omega) = 0 \text{ for some } m \in \mathbb{N}\}$.

3. Semisimple holomorphic differentials

Let k be an algebraically closed field of characteristic p, L/K a finite Galois p-extension of algebraic function fields of one variable over k with Galois group $G = \mathrm{Gal}(L/K)$. Let $x \in L$ be a separating element. Let $S := \{P_1, \ldots, P_r\}$ be the set consisting of the prime divisors of K, which are ramified in L/K. For each $i \in [\![1, r]\!]$ we choose Q_i a prime divisor of L such that Q_i divides to P_i. We define the set $\widehat{S} := \{Q_1, Q_2, \ldots, Q_r\}$. Let $G_i := \{\sigma \in G\colon Q_i^\sigma = Q_i\} = \mathrm{Dec}(Q_i \mid P_i)$ be the decomposition group of the prime Q_i. We have that if Q_i^* is any other prime divisor of L dividing P_i, then the group $G_i = \mathrm{Dec}(Q_i \mid P_i)$ is conjugated to the group $G_i^* = \mathrm{Dec}(Q_i^* \mid P_i)$. Therefore we have that $k[G/G_i] \cong k[G/G_i^*]$ as $k[G]$-modules.

Let $\sigma \in G = \mathrm{Gal}(L/K)$, $\omega \in \Omega_L$. We have that $\omega = hdx$ for some $h \in L$. From Proposition 3 it follows that the action of G on Ω_L is given by $\sigma\omega = \sum_{i=0}^{p-1} \sigma(h_i)^p x^i dx$. Thus, Ω_L is a $k[G]$-module, $\Omega_L(0)$ is a $k[G]$-submodule of Ω_L and $\Omega_L^s(0)$ is a $k[G]$-submodule of $\Omega_L(0)$.

Nakajima ([8], Theorem 2) obtained two $k[G]$-exact sequences which determine implicitly the $k[G]$-module structure of $\Omega_L^s(0)$ for every extension L/K.

If the extension L/K is unramified we have the $k[G]$-exact sequence

$$0 \longrightarrow \Omega_L^s(0) \longrightarrow k[G]^{\tau_K} \longrightarrow I_G \longrightarrow 0, \tag{2}$$

where $I_G = \langle g - 1 \mid g \in G \rangle$.

If the extension L/K is ramified we have the $k[G]$-exact sequence

$$0 \longrightarrow \Omega_L^s(0) \longrightarrow k[G]^{r-1+\tau_K} \longrightarrow \ker(\Phi) \longrightarrow 0, \tag{3}$$

where the $k[G]$-epimorphism Φ: $\bigoplus_{i=1}^r k[G/G_i] \to k$ is defined by

$$\Phi = \bigoplus_{i=1}^{r} \Phi_i, \Phi_i\Big(\sum_{\sigma \in G/G_i} a_\sigma \sigma \Big) = \sum_{\sigma \in G/G_i} a_\sigma .$$

From (3) it follows that $\Omega(\ker(\Phi)) \cong \Omega_L^s(0)^{(1)}$ as $k[G]$-modules. Since $\Omega_L^s(0)^{(0)}$ is a finitely generated projective $k[G]$-module, we have that $\Omega_L^s(0)^{(0)}$ is a free $k[G]$-module. Therefore $\Omega_L^s(0)^{(0)} \cong k[G]^u$ for some $u \geq 0$. Consequently we obtain that

$$\Omega_L^s(0) \cong k[G]^u \oplus \Omega(\ker(\Phi)). \tag{4}$$

For a $k[G]$-module M, we will denote by $\mathbb{X}(M) := \mathrm{Hom}_k(M,k)$ the contragredient of M.

PROPOSITION 5: *Let M be a finitely generated $k[G]$-module. Then $\Omega^{\#}(\mathbb{X}(M)) \cong \mathbb{X}(\Omega(M))$ as $k[G]$-modules.*

Proof: ([3], Proposition 78.4). ∎

PROPOSITION 6: *Let L/K be a finite Galois p-extension of algebraic function fields of one variable with Galois group $G = \mathrm{Gal}(L/K)$ and field of constants an algebraically closed field k of characteristic p. Let $P_1, \dots, P_r$ be the ramified prime divisors in L/K and let $G_1, \dots, G_r$ be their decomposition groups, respectively. Let $\Omega_L^s(0)$ be the $k[G]$-module of the semisimple differentials holomorphic of L. Let Φ be the application given in (3). Then*

(a) $\mathbb{X}(\ker(\Phi)) \cong \frac{\bigoplus_{i=1}^{r} k[G/G_i]}{ke^*}$ *as* $k[G]$*-modules, where* ke^* *is the diagonal of* $\bigoplus_{i=1}^{r} k[G/G_i]$*, that is,*

$$ke^* = \left\{ \left(\sum_{\sigma \in G/G_1} x\sigma, \ldots, \sum_{\sigma \in G/G_r} x\sigma \right) \in \bigoplus_{i=1}^{r} k[G/G_i] \colon x \in k \right\}.$$

(b) *Let* c *be the minimal natural number such that there exists an epimorphism of* $k[G]$*-modules* $\rho\colon k[G]^c \to \ker(\Phi)$ *and* $u \in \mathbb{N}_0$ *such that* $\Omega_L^s(0)^{(0)} \cong k[G]^u$*. Then*

$$u = r - 1 - c + \tau_K, \tag{5}$$

and $k[G]^c$ *is the projective* $k[G]$*-cover of* $\ker(\Phi)$*.*

(c) *Let* d *be the minimal natural number such that there exists a monomorphism of* $k[G]$*-modules* $f\colon \frac{\bigoplus_{i=1}^{r} k[G/G_i]}{ke^*} \to k[G]^d$*. Then* $c = d$*,* $k[G]^c$ *is the injective* $k[G]$*-envelope of* $\frac{\bigoplus_{i=1}^{r} k[G/G_i]}{ke^*}$ *and there exists a* $k[G]$*-exact sequence*

$$0 \longrightarrow \frac{\bigoplus_{i=1}^{r} k[G/G_i]}{ke^*} \longrightarrow k[G]^c \longrightarrow \Omega^{\#}\left(\frac{\bigoplus_{i=1}^{r} k[G/G_i]}{ke^*}\right) \longrightarrow 0. \tag{6}$$

(d) *There exists a* $k[G]$*-exact sequence*

$$0 \to \frac{\bigoplus_{i=1}^{r} k[G/G_i]}{ke^*} \to k[G]^{r-1+\tau_K} \to \mathbb{X}(\Omega_L^s(0)) \to 0.$$

(e) $\mathbb{X}(\Omega_L^s(0)) \cong k[G]^u \oplus \Omega^{\#}\left(\frac{\bigoplus_{i=1}^{r} k[G/G_i]}{ke^*}\right)$ *as* $k[G]$*-modules, for some* $u \geq 0$*.*

Proof:

(a) Since Φ is a $k[G]$-epimorphism we have the $k[G]$-exact sequence

$$0 \longrightarrow \ker(\Phi) \longrightarrow \bigoplus_{i=1}^{r} k[G/G_i] \xrightarrow{\Phi} k \longrightarrow 0. \tag{7}$$

From ([6], Lemmas 3.5, 3.8-iii) and (7) we obtain the $k[G]$-exact sequence

$$0 \longrightarrow \mathbb{X}(k) \longrightarrow \bigoplus_{i=1}^{r} \mathbb{X}(k[G/G_i]) \longrightarrow \mathbb{X}(\ker(\Phi)) \longrightarrow 0. \tag{8}$$

From (8) it follows that

$$\mathbb{X}(\ker(\Phi)) \cong \frac{\bigoplus_{i=1}^{r} \mathbb{X}(k[G/G_i])}{\mathbb{X}(k)} \cong \frac{\bigoplus_{i=1}^{r} k[G/G_i]}{ke^*}. \tag{9}$$

(b) Follows from (3), (4), Schanuel's Lemma for injective $k[G]$-modules and the Krull–Schmidt–Azumaya Theorem.

(c) Set $T := \frac{\bigoplus_{i=1}^{r} k[G/G_i]}{ke^*}$. We have the $k[G]$-exact sequence

$$0 \longrightarrow T \longrightarrow k[G]^d \longrightarrow \operatorname{coker}(f) \longrightarrow 0. \tag{10}$$

From (a) and (10) we have the $k[G]$-exact sequence

$$0 \longrightarrow \mathbb{X}(\operatorname{coker}(f)) \longrightarrow k[G]^d \longrightarrow \ker(\Phi) \longrightarrow 0. \tag{11}$$

Since $k[G]^c$ is the projective $k[G]$-cover of $\ker(\Phi)$ it follows that $d = c$. Since $(k[G]^c, \rho)$ is the injective $k[G]$-envelope of T we have that there exists a $k[G]$-exact sequence

$$0 \longrightarrow T \longrightarrow k[G]^c \longrightarrow \operatorname{coker}(\rho) \longrightarrow 0 \tag{12}$$

where $\operatorname{coker}(\rho) \cong \Omega^{\#}(T) \oplus k[G]^b$ for some $b \geq 0$. From (12) we obtain

$$\frac{k[G]^c}{T} \cong \Omega^{\#}(T) \oplus k[G]^b.$$

Since

$$\mathcal{N}\left(\frac{k[G]^c}{T}\right) = 0$$

we have that $b = 0$ ([15], Proposition 1).

(d) From ([6], Lemma 3.8-iii) and (3) we have the $k[G]$-exact sequence

$$0 \to \mathbb{X}(\ker(\Phi)) \to \mathbb{X}\left(k[G]^{r-1+\tau_K}\right) \to \mathbb{X}(\Omega_L^s(0)) \to 0. \tag{13}$$

From (9) and (13) we obtain the $k[G]$-exact sequence

$$0 \longrightarrow \frac{\bigoplus_{i=1}^{r} k[G/G_i]}{ke^*} \longrightarrow k[G]^{r-1+\tau_K} \longrightarrow \mathbb{X}(\Omega_L^s(0)) \longrightarrow 0. \tag{14}$$

(e) From (4), (9) and Proposition 5, it follows that, as $k[G]$-modules,

$$\mathbb{X}(\Omega_L^s(0)) \cong k[G]^u \oplus \mathbb{X}(\Omega(\ker(\Phi))) \cong k[G]^u \oplus \Omega^{\#}\left(\frac{\bigoplus_{i=1}^{r} k[G/G_i]}{ke^*}\right). \qquad \blacksquare$$

Let

$$T := \frac{\bigoplus_{i=1}^{r} k[G/G_i]}{ke^*} \cong \mathbb{X}(\ker(\Phi)).$$

We have

PROPOSITION 7: *Let $k[G]^c$ be the injective $k[G]$-envelope of T. Then*

$$c = \dim_k \left(T^G\right).$$

Proof: From (6) we obtain the $k[G]$-exact sequence

$$0 \longrightarrow T^G \longrightarrow (k[G]^c)^G \longrightarrow \left(\Omega^{\#}(T)\right)^G. \tag{15}$$

Therefore we obtain a $k[G]$-monomorphism $T^G \to k^c$. It follows that $c' := \dim_k \left(T^G\right) \leq \dim_k (k^c) = c$ and $T^G \cong k^{c'} \subseteq k[G]^{c'}$. Therefore there exists a $k[G]$-monomorphism ρ: $T^G \to k[G]^{c'}$. Since $k[G]^{c'}$ is an injective $k[G]$-module and the inclusion map i: $T^G \to T$ is a $k[G]$-monomorphism, it follows that there exists $\widehat{\rho}$: $T \to k[G]^{c'}$ a $k[G]$-homomorphism such that $\rho = \widehat{\rho} \circ i$. Suppose that $\ker(\widehat{\rho}) \neq 0$. Since k is a field of characteristic p, G a p-group and $\ker(\widehat{\rho})$ a $k[G]$-module we have $(\ker(\widehat{\rho}))^G \neq 0$ ([10], Theorem 2). However $(\ker(\widehat{\rho}))^G = T^G \cap \ker(\widehat{\rho}) = \ker(\rho) = \{0\}$. Therefore $\widehat{\rho}$: $T \to k[G]^{c'}$ is a $k[G]$-monomorphism. Since c is minimal it follows that $c \leq c'$. Hence $c' = c$. ∎

If A is a G-module then $H^n(G, A)$ will denote the n-**th cohomology group of** G **with coefficients in the module** A.

PROPOSITION 8: *Let G be a finite p-group, $H_1, \ldots, H_r$ subgroups of G,*

$$\mathcal{T}_r := \frac{\bigoplus_{i=1}^r k[G/H_i]}{ke^*}.$$

For each $i \in [\![1, r]\!]$, let $\widehat{H_i} := \langle gH_ig^{-1} \mid g \in G\rangle$ be the normal closure of the subgroup H_i in G. We set $\widehat{H} := \widehat{H_1} \cdots \widehat{H_r}$ and let $d_{G/\widehat{H}}$ be the minimal number of generators of the group $G/\widehat{H}$. Then $\dim_k(T^G) = \dim_k \left(\mathcal{T}_r{}^G\right) = r - 1 + d_{G/\widehat{H}}$.

Proof: For each $i \in [\![1, r]\!]$ we consider the maps α_i: $ke_i^* \to k[G/H_i]$ with $\alpha_i(x) = \sum_{\sigma \in G/H_i} x\sigma$. Since G acts trivially on ke_i^* we have that $(ke^*)^G \cong ke^*$ and $H^1(G, ke_i^*) \cong \operatorname{Hom}(G, k)$.

Let α_i^* be the application induced by α_i on the cohomology groups.

Let r_i: $k[G/H_i] \to k$ be the k-linear map sending the coset H_i to 1 and all other cosets of H_i to 0. Since $k[G/H_i]$ is the induced module $\operatorname{Ind}_{H_i}^G k$, it follows from Shapiro's Lemma that r_i together with restriction of operators from G to H_i induces an isomorphism $H^1(G, k[G/H_i]) \to H^1(H_i, k) \cong \operatorname{Hom}(H_i, k)$.

Therefore α_i^* is identified with the homomorphism $\operatorname{Hom}(G, k) \to \operatorname{Hom}(H_i, k)$ induced by restricting characters from G to H_i. Thus $\psi \in \ker(\alpha_i^*)$ if and only if ψ is trivial on the subgroup of G generated by the conjugates of H_i.

Thus, we have that $\psi \in \ker(\alpha_i^*) \iff \widehat{H}_i \leq \ker(\psi)$.

Let $\psi \in \ker(\alpha_i^*) \subseteq \mathrm{Hom}(G,k)$. There exists a unique $\widehat{\psi} \in \mathrm{Hom}(G/\widehat{H}_i, k)$ such that $\widehat{\psi}(g\widehat{H}_i) = \psi(g)$ for all $g \in G$. Then, we have the $k[G]$-isomorphism

$$\rho\colon \ker(\alpha_i^*) \to \mathrm{Hom}(G/\widehat{H}_i, k) \text{ such that } \psi \to \widehat{\psi}. \tag{16}$$

Let $\Phi(G/\widehat{H}_i)$ be the Frattini subgroup of $G/\widehat{H}_i$. Then

$$\begin{aligned} \dim_k(\ker(\alpha_i^*)) &= \dim_k\left(\mathrm{Hom}\left(\frac{G}{\widehat{H}_i}, k\right)\right) \\ &= \dim_k\left(\mathrm{Hom}\left(\frac{G/\widehat{H}_i}{\Phi\left(G/\widehat{H}_i\right)}, k\right)\right) = d_{G/\widehat{H}_i}. \end{aligned} \tag{17}$$

Now we consider the $k[G]$-exact sequence,

$$0 \longrightarrow ke^* \xrightarrow{\alpha} \bigoplus_{i=1}^{r} k[G/H_i] \xrightarrow{\pi} \mathcal{T}_r \longrightarrow 0 \tag{18}$$

where $\alpha((x,\dots,x)) = (\alpha_1(x),\dots,\alpha_r(x))$. From (18) we obtain

$$\begin{aligned} &0 \longrightarrow (ke^*)^G \xrightarrow{\varphi_3} \left(\bigoplus_{i=1}^{r} k[G/H_i]\right)^G \xrightarrow{\varphi_2} \mathcal{T}_r{}^G \xrightarrow{\varphi_1} H^1(G, ke^*) \\ &\xrightarrow{\alpha^*} \bigoplus_{i=1}^{r} H^1(G, k[G/H_i]) \longrightarrow H^1(G, \mathcal{T}_r) \longrightarrow \cdots. \end{aligned} \tag{19}$$

Therefore from (19) we obtain the exact sequence

$$\begin{aligned} &0 \longrightarrow ke^* \xrightarrow{\varphi_3} (ke^*)^r \xrightarrow{\varphi_2} \mathcal{T}_r{}^G \xrightarrow{\varphi_1} \mathrm{Hom}(G,k) \\ &\xrightarrow{\alpha^*} \bigoplus_{i=1}^{r} H^1(G, k[G/H_i]) \longrightarrow H^1(G, \mathcal{T}_r) \longrightarrow \cdots. \end{aligned} \tag{20}$$

Hence, we obtain

$$0 \longrightarrow ke^* \xrightarrow{\varphi_3} (ke^*)^r \xrightarrow{\varphi_2} \mathcal{T}_r{}^G \xrightarrow{\varphi_1} \ker(\alpha^*) \longrightarrow 0. \tag{21}$$

It follows that $\dim_k(\ker(\varphi_1)) = r-1$. Thus we have the k-exact sequence

$$0 \longrightarrow (ke^*)^{r-1} \longrightarrow \mathcal{T}_r{}^G \longrightarrow \ker(\alpha^*) \longrightarrow 0. \tag{22}$$

Since $\alpha^*(\psi) = (\alpha_1^*(\psi),\dots,\alpha_r^*(\psi))$, we have that

$$\begin{aligned} \psi \in \ker(\alpha^*) &\iff \psi \in \ker(\alpha_i^*)\ \forall\, i \in [\![1,r]\!], \\ &\iff \widehat{H_i} \le \ker(\psi)\ \forall\, i \in [\![1,r]\!], \\ &\iff \widehat{H} = \widehat{H_1}\cdots\widehat{H_r} \le \ker(\psi). \end{aligned}$$

Hence, we have $\ker(\alpha^*) \cong \operatorname{Hom}(G/\widehat{H}, k)$ and $\dim_k(\ker(\alpha^*)) = d_{G/\widehat{H}}$. Finally, from (22), we obtain $\dim_k\left(\mathcal{T}_r{}^G\right) = r - 1 + d_{G/\widehat{H}}$. ∎

PROPOSITION 9: *Let L/K be a finite Galois p-extension of algebraic function fields of one variable with an algebraically closed field k of characteristic p as its exact field of constants with Galois group $G = \operatorname{Gal}(L/K)$. Let $H_1, \ldots, H_r$ be arbitrary subgroups of G. Reordering the indices and taking conjugates if necessary, let $1 \leq i_1 < i_2 < \cdots < i_{s-1} < i_s = r$ be such that*

$$\begin{array}{cccl} H_1, & \ldots, & H_{i_1-1} \subseteq & H_{i_1} \\ H_{i_1+1}, & \ldots, & H_{i_2-1} \subseteq & H_{i_2} \\ & \vdots & & \\ H_{i_{s-1}+1}, & \ldots, & H_{i_s-1} \subseteq & H_{i_s} = H_r \end{array}$$

and such that the subgroups $H_{i_1}, H_{i_2}, \ldots, H_{i_s}$ satisfy the condition that if for $1 \leq j, k \leq s$ there exists some $g \in G$ such that $H_{i_j}^g = gH_{i_j}g^{-1} \subseteq H_{i_k}$, then $j = k$. Let $A_2 := \{i_1, i_2, \ldots, i_s\}$ and $A_1 := [\![1, r]\!] - A_2$. Then

$$\frac{\bigoplus_{i=1}^r k[G/H_i]}{ke^*} \cong \bigoplus_{i \in A_1} k[G/H_i] \oplus \frac{\bigoplus_{i \in A_2} k[G/H_i]}{ke^*_{A_2}},$$

where

$$ke^*_{A_2} := \left\{\left(\sum_{\sigma \in G/H_{i_1}} x\sigma, \ldots, \sum_{\sigma \in G/H_{i_s}} x\sigma\right) \in \bigoplus_{i \in A_2} k[G/H_i] \colon x \in k\right\}.$$

Proof: For each $j \in [\![1, s]\!]$ we define the $k[G]$-monomorphism,

$$\begin{array}{cccc} \Lambda_{\widehat{\imath_j}}\colon & k[G/H_{i_j}] & \to & k[G/H_{\widehat{\imath_j}}] \\ & \sum\limits_{\psi \in G/H_{i_j}} a_\psi \psi & \to & \sum\limits_{\psi \in G/H_{i_j}} a_\psi \sum\limits_{\substack{\sigma \subseteq \psi \\ \sigma \in G/H_{\widehat{\imath_j}}}} \sigma, \end{array}$$

where $\widehat{\imath_j} \in [\![i_{j-1} + 1, i_j - 1]\!]$, $i_0 = 0$. We define the following $k[G]$-homomorphism

$$\Lambda\colon \bigoplus_{i=1}^r k[G/H_i] \to \frac{\bigoplus_{i=1}^r k[G/H_i]}{ke^*} \text{ by } \left(\xi_1, \cdots, \xi_{i_j}, \cdots, \xi_r\right) \to \overline{(c_1, \ldots, c_{r-1}, c_r)},$$

where

$$c_t = \begin{cases} \xi_t + \Lambda_t\left(\xi_{i_j}\right) & \text{if } t \in [\![i_{j-1} + 1, i_j - 1]\!], \\ \xi_{i_j} & \text{if } t = i_j. \end{cases}$$

Λ is a $k[G]$-epimorphism with $\ker(\Lambda) = D \subseteq \bigoplus_{i=1}^{r} k[G/H_i]$ where

$$D := \left\{ \left(0,\dots,0, \sum_{\psi\in G/H_{i_1}} x\psi, 0,\dots,0, \sum_{\psi\in G/H_{i_2}} x\psi, \right.\right.$$
$$\left.\left. 0,\dots,0, \sum_{\psi\in G/H_{i_s}} x\psi\right) : x\in k \right\}. \qquad \blacksquare$$

Professor Alfred Weiss proved that the $F[G]$-module $\frac{F[S]}{F\widehat{S}}$ is an indecomposable $F[G]$-module, where F is an arbitrary field of characteristic p, G a finite p-group and $S := \biguplus_{i=1}^{r} G/H_i$ with H_i arbitrary subgroups of G satisfying that $H_i^g = gH_ig^{-1} \subsetneq H_j$ for some $g \in G \iff i = j$.

PROPOSITION 10 (Weiss): *Let G be a finite p-group, F a field of characteristic p, S a finite set, such that G acts on S, H a subgroup of G acting by restriction on S and B an $F[G]$-module. Then*

(a) *The set $\mathbf{S} := \{\widehat{X}\colon X$ is a H-orbit in $S\}$ is an F-base of the module $(F[S])^H$ and $\bar{\mathbf{S}} := \{\widehat{X} + F\widehat{S}\colon X$ is a H-orbit in $S\}$ is an F-generator of the module $\frac{(F[S])^H}{F\widehat{S}}$.*

(b) *We consider the homomorphism of F-algebras*

$$\begin{array}{cccc} \psi\colon & \mathrm{End}_{F[G]}(B) & \to & \mathrm{End}_F\left(\frac{B}{I_GB}\right) \\ & f & \to & \widehat{f}. \end{array}$$

Let $A := \psi\left(\mathrm{End}_{F[G]}(B)\right)$. Then

$$\frac{A}{\mathrm{rad}(A)} \cong \frac{\mathrm{End}_{F[G]}(B)}{\mathrm{rad}\left(\mathrm{End}_{F[G]}(B)\right)}$$

where $\mathrm{rad}(A)$ denotes the Jacobson radical of A.

(c) *Let $B := \frac{F[S]}{F\widehat{S}}$. Then B is an indecomposable $F[G]$-module if and only if A is a local ring.*

Proof:

(a) It is clear.

(b) Since G is a finite p-group and F is a field of characteristic p we have that I_G is a nilpotent ideal ([9], Lemma 2.21). Therefore there exists $s \in \mathbb{N}$ such that $I_G^s = (0)$. We have that $\ker(\psi) = \{f \in \mathrm{End}_{F[G]}(B) : f(B) \subseteq I_GB\}$ is a nilpotent ideal. Then $\ker(\psi) \subseteq \mathrm{rad}\left(\mathrm{End}_{F[G]}(B)\right)$. It follows from ([3], Proposition 5.1) that

$$\operatorname{rad}\left(\frac{\operatorname{End}_{F[G]}(B)}{\ker(\psi)}\right) \cong \frac{\operatorname{rad}\left(\operatorname{End}_{F[G]}(B)\right)}{\ker(\psi)}.$$

Since ψ: $\operatorname{End}_{F[G]}(B) \to A$ is an epimorphism we have that

$$\frac{\operatorname{End}_{F[G]}(B)}{\ker(\psi)} \cong A.$$

Hence

$$\frac{\frac{\operatorname{End}_{F[G]}(B)}{\ker(\psi)}}{\operatorname{rad}\left(\frac{\operatorname{End}_{F[G]}(B)}{\ker(\psi)}\right)} \cong \frac{\operatorname{End}_{F[G]}(B)}{\operatorname{rad}\left(\operatorname{End}_{F[G]}(B)\right)} \cong \frac{A}{\operatorname{rad}(A)}.$$

(c) We have that B is a finitely generated $F[G]$-module. From ([3], Proposition 6.10) we obtain that B is an indecomposable $F[G]$-module if and only if $\operatorname{End}_{F[G]}(B)$ is a local ring and that $\operatorname{End}_{F[G]}(B)$ is a local ring if and only if

$$\frac{\operatorname{End}_{F[G]}(B)}{\operatorname{rad}\left(\operatorname{End}_{F[G]}(B)\right)} \cong \frac{A}{\operatorname{rad}(A)}$$

is a division ring. From ([3], Proposition 5.21) we have that $\frac{A}{\operatorname{rad}(A)}$ is a division ring if and only if A is a local ring. ∎

Let G be a finite p-group, H a subgroup of G such that G acts on a finite set S and X an H**-orbit over** S. We say that X is a **Weiss** H**-orbit over** S if X contains some $s \in S$ such that the stabilizer G_s satisfies $G_s \leq H$.

Let X be an H-orbit over S and let $s \in S$. If $G_s = H_s$, then $G_s \subseteq H$ and X is a Weiss H-orbit over S. Conversely, if X is a Weiss H-orbit over S then there exists $t \in S$ such that $G_t \subseteq H$. It follows that if $g \in G_t$, then $g \in H$ and $gt = t$. Therefore $G_t \subseteq H_t$ so that $G_t = H_t$. Therefore X is a Weiss H-orbit over S if and only if $G_s = H_s$ for some $s \in X$ if and only if $G_s \subseteq H$ for some $s \in X$.

Let F be a field of characteristic p and H a subgroup of G. If X is a left transversal of H in G and M is an $F[G]$-module, we consider the map $\operatorname{Tr}_{G/H}$: $M^H \to M^G$ defined by $\operatorname{Tr}_{G/H}(m) = \sum_{g_i \in X} g_i m$.

PROPOSITION 11 (Weiss): *Let G be a finite p-group, F a field of characteristic p, S a finite set such that G acts on S, H a subgroup of G acting by restriction on S. Then $\mathcal{B} := \{\operatorname{Tr}_{G/H}(\widehat{X})$: X is a Weiss H-orbit$\}$ is an F-base of the module $\operatorname{Tr}_{G/H}\left(F[S]^H\right)$.*

Proof: We consider $\varepsilon \in \operatorname{Tr}_{G/H}\left(F[S]^H\right)$. Then

$$\varepsilon = \operatorname{Tr}_{G/H}\left(\sum_{i=1}^{t} r_i \widehat{X_i}\right) = \sum_{i=1}^{t} r_i \operatorname{Tr}_{G/H}(\widehat{X_i})$$

where $r_i \in F$ and X_i, $i \in [\![1,t]\!]$ are the H-orbits over S. Let $s \in S$ and let X_i be an H-orbit over S such that $s \in X_i$. We have that if $H = \biguplus_{i=1}^{[H:H_s]} h_i H_s$ then the H-orbit X_i is given by $X_i = \{h_i s \colon i \in [\![1, [H : H_s]]\!]\}$. From ([6], Lemma 8.3), we obtain

$$\begin{aligned}\operatorname{Tr}_{G/H}(\widehat{X_i}) &= \operatorname{Tr}_{G/H} \operatorname{Tr}_{H/H_s}(s) = \operatorname{Tr}_{G/H_s}(s) = \operatorname{Tr}_{G/G_s} \operatorname{Tr}_{G_s/H_s}(s) \\ &= \operatorname{Tr}_{G/G_s}([G_s : H_s]s) = [G_s : H_s] \operatorname{Tr}_{G/G_s}(s) = \begin{cases} \widehat{Q}_s & \text{if } G_s = H_s, \\ 0 & \text{otherwise,} \end{cases}\end{aligned}$$

where $\widehat{Q}_s$ is the G-orbit over S containing s. Therefore

$$\varepsilon = \sum_{i=1}^{t} r_i [G_s : H_s] \operatorname{Tr}_{G/G_s}(s) = \sum_{i=1}^{n} r_i \operatorname{Tr}_{G/H}(\widehat{X_i})$$

where the X_i's are Weiss H-orbits over S. Furthermore, we have that $\mathcal{B}$ is an F-linearly independent set. Hence $\mathcal{B}$ is an F-base of $\operatorname{Tr}_{G/H}\left(F[S]^H\right)$. ∎

PROPOSITION 12 (Weiss): *Let G be a finite p-group, F a field of characteristic p and $H_1, \ldots, H_r$ subgroups of G satisfying:*

$$H_i^g = gH_ig^{-1} \subseteq H_j \quad \text{for some } g \in G \iff i = j \tag{23}$$

and such that G acts in a natural way on the set $S := \biguplus_{i=1}^{r} G/H_i$. Then

$$B := \frac{F[S]}{F\widehat{S}}$$

is an indecomposable $F[G]$-module.

Proof: Let $A := \{\widehat{f} \colon f \in \operatorname{End}_{F[G]}(B)\}$, where

$$\widehat{f} \in \operatorname{End}_F\left(\frac{B}{I_G B}\right) \quad \text{and} \quad \widehat{f}(x + I_G B) = f(x) + I_G B.$$

From Proposition 10 it follows that in order to prove the $F[G]$-indecomposability of the module B it suffices to prove that A is a local ring.

Let $v_j := \pi(H_j + F\widehat{S})$, $j \in [\![1,r]\!]$ where

$$\pi \colon B \to \frac{B}{I_G B}$$

is the canonical projection. We define the set $V := \{v_j \colon j \in [\![1,r]\!]\}$. If $g \in G$ we have that $(g-1)(H_j + F\widehat{S}) \in I_G B$. Therefore

$$\pi(gH_j + F\widehat{S}) = \pi(H_j + F\widehat{S}) = v_j \quad \forall g \in G \quad \forall j \in [\![1,r]\!].$$

We have that V is an F-generator set of the module $\frac{B}{I_G B}$. Now, if $x \in F\widehat{S}$ then

$$x = \sum_{j=1}^{r} \sum_{g_j \in T(G/H_j)} (bg_j - b)H_j \in I_G F[S],$$

where $T(G/H_j)$ is a left transversal of H_j in G. Therefore $F\widehat{S} \subseteq I_G F[S]$. The application

$$\begin{array}{rccc} \rho\colon & I_G F[S] & \to & I_G\left(\frac{F[S]}{F\widehat{S}}\right) \\ & \sum\limits_{i=1}^{n} x_i y_i & \to & \sum\limits_{i=1}^{n} x_i\left(y_i + F\widehat{S}\right), \end{array}$$

where $x_i \in I_G$, $y_i \in F[S]$ is an $F[G]$-epimorphism and $\ker(\rho) \cong F\widehat{S}$. If $x \in F\widehat{S}$ then

$$x = \sum_{j=1}^{r} \sum_{g_j \in T(G/H_j)} (bg_j - b)H_j.$$

Therefore $\rho(x) = 0$. Hence $F\widehat{S} \subseteq \ker(\rho)$. Conversely, if $x \in \ker(\rho)$ then

$$\rho(x) = \rho\left(\sum_{i=1}^{n} x_i y_i\right) = \sum_{i=1}^{n} x_i(y_i + F\widehat{S}) = F\widehat{S} = 0.$$

It follows that $\sum_{i=1}^{n} x_i y_i + F\widehat{S} = F\widehat{S}$. Therefore $\sum_{i=1}^{n} x_i y_i = x \in F\widehat{S}$. Hence $\ker(\rho) \cong F\widehat{S}$. Then

$$I_G B \cong \frac{I_G F[S]}{F\widehat{S}}.$$

We consider now an element $x \in I_G F[S]$. We have that $x = \sum_{i=1}^{n} x_i y_i$ for some $x_i \in I_G$, $y_i \in F[S]$. Hence

$$(24)\quad x_i y_i = \left(\sum_{g \in G} r_g g\right)\left(\sum_{j=1}^{n} \sum_{\sigma_j \in G/H_j} a_{\sigma_j}\sigma_j\right) = \sum_{j=1}^{n} \sum_{\sigma_j \in G/H_j} \sum_{g \in G} \left(r_g a_{\sigma_j}\right)\sigma_j.$$

Therefore, for each $\sigma_j \in G/H_j$ and for each $j \in [\![1, r]\!]$ the coefficients of the summand $\sum_{g \in G}\left(r_g a_{\sigma_j} g\right)\sigma_j$ satisfy $\sum_{g \in G} r_g a_{\sigma_j} = (\sum_{g \in G} r_g)a_{\sigma_j} = 0$. Now, let $a_1 v_1 + \cdots + a_r v_r = 0$ be any linear F-combination of the v_i equal to zero. Therefore

$$(a_1 H_1 + \cdots + a_r H_r) + F\widehat{S} \in I_G B \cong \frac{I_G F[S]}{F\widehat{S}}.$$

From (24) it follows that $a_i = 0\ \forall i \in [\![1, r]\!]$. Therefore V is an F-base of $\frac{B}{I_G B}$. Hence $\widehat{f}$ is completely determined by its values on the v_j and

$$\widehat{f}(v_j) = f\left(H_j + F\widehat{S}\right) + I_G B.$$

Let $x_j \in F[S]$ be such that $f(H_j + F\widehat{S}) = x_j + F\widehat{S}$. Since $f \in \mathrm{End}_{F[G]}(B)$ it follows that for every $g \in G$, $gx_j + F\widehat{S} = gf(H_j + F\widehat{S}) = f(gH_j + F\widehat{S})$. Therefore, if $g \in H_j$ we have that $f(gH_j + F\widehat{S}) = f(H_j + F\widehat{S}) = x_j + F\widehat{S}$. Hence

$$f(H_j + F\widehat{S}) \in \frac{F[S]^{H_j}}{F\widehat{S}}.$$

The module $\frac{F[S]^{H_j}}{F\widehat{S}}$ is an F-module generated by the set

$$\left\{\widehat{X} + F\widehat{S}\colon X \text{ is a } H_j\text{-orbit over } S\right\}.$$

Therefore

$$(25)\quad f(H_j + F\widehat{S}) = \sum_{X \in S/H_j} a_j(X)(\widehat{X} + F\widehat{S}) = \left(\sum_{X \in S/H_j} a_j\,(X)\,\widehat{X}\right) + F\widehat{S},$$

where $a_j\,(X) \in F$ and S/H_j represents the set of H_j-orbits over S.

Since $F\widehat{S} = \widehat{S} + F\widehat{S}$ we have that

$$F\widehat{S} = \sum_{j=1}^{r} \mathrm{Tr}_{G/H_j}(f(H_j + F\widehat{S})) = \sum_{j=1}^{r} \sum_{X \in S/H_j} a_j(X)\,\mathrm{Tr}_{G/H_j}(\widehat{X}) + F\widehat{S}.$$

If X is not a Weiss H-orbit, from Proposition 11 we obtain that $\mathrm{Tr}_{G/H_j}(\widehat{X}) = 0$. Therefore

$$(26)\quad \sum_{j=1}^{r} \sum_{X \in S/H_j} a_j(X)\,\mathrm{Tr}_{G/H_j}(\widehat{X}) + F\widehat{S} = \sum_{j=1}^{r} \sum_{X \in W} a_j(X)\,\mathrm{Tr}_{G/H_j}(\widehat{X}) + F\widehat{S},$$

where W is the set of Weiss H_j-orbits over S. Since X is an H_j-orbit over S, we have that $X = \{gg'H_i\colon g \in H_j\}$ for some $i \in [\![1, r]\!]$. Since X is a Weiss H-orbit over S, it follows that there exists some $xg'H_i \in X$ such that $G_{xg'H_j} \subseteq H_j$. We have that $G_{xg'H_i} = H_i^{xg'}$. Therefore $H_i^{xg'} \subseteq H_j$. From Proposition 12 we have that $i = j$. Therefore $xg'H_j g'^{-1} x^{-1} \subseteq H_j$. Since $|g'H_j g'^{-1}| = |H_j|$, it follows that $g'H_j g'^{-1} = H_j$. Therefore $g' \in N_G\,(H_j)$. We have that

$$X = \{gg'H_j\colon g \in H_j\} = \{gH_j g'\colon g \in H_j\} = \{g'H_j\}.$$

Hence

$$\begin{aligned} F\widehat{S} &= \sum_{j=1}^{r} \sum_{X \in W} a_j(X)\,\mathrm{Tr}_{G/H_j}(\widehat{X}) + F\widehat{S} \\ &= \sum_{j=1}^{r} \sum_{g' \in N_G(H_j)} a_j\,(\{g'H_j\})\,\mathrm{Tr}_{G/H_j}\,(g'H_j) + F\widehat{S}. \end{aligned}$$

Then $\sum_{j=1}^{r}\sum_{g'\in N_G(H_j)} a_j(\{g'H_j\})\operatorname{Tr}_{G/H_j}(g'H_j) \in F\widehat{S}$. Since $\operatorname{Tr}_{G/H_j}(g'H_j) = \sum_{z\in G/H_j} zH_j$, it follows that

$$\sum_{j=1}^{r}\sum_{g'\in N_G(H_j)} a_j(\{g'H_j\})\operatorname{Tr}_{G/H_j}(g'H_j) = \sum_{j=1}^{r}\sum_{z\in G/H_j}\sum_{g'\in N_G(H_j)} a_j(\{g'H_j\})zH_j.$$

Therefore, the element $\sum_{j=1}^{r}\sum_{z\in G/H_j}\sum_{g'\in N_G(H_j)} a_j(\{g'H_j\})zH_j$ belongs to $F\widehat{S}$.

We obtain that the element $\sum_{g'\in N_G(H_j)} a_j(\{g'H_j\})$ is independent of j. We set

$$a(f) := \sum_{g'\in N_G(H_j)} a_j(\{g'H_j\}) \in F.$$

From (25) it follows that

$$\widehat{f}(v_j) = \pi\bigg(\sum_{X\in W} a_j(X)(\widehat{X} + F\widehat{S})\bigg) = \sum_{g'\in N_G(H_j)} a_j(\{g'H_j\})\pi(H_j + F\widehat{S}) = a(f)v_j.$$

Hence $\widehat{f}(v_j) = a(f)v_j$. That is, $\widehat{f}$ is the multiplication by $a(f)$. Therefore $A \cong F$. ∎

PROPOSITION 13: *With the conditions and notations of Propositions 8 and 9, let $H_i = G_i$. Let*

$$M := \frac{\bigoplus_{i\in A_2} k[G/G_i]}{ke^*_{A_2}}.$$

Then, as $k[G]$-modules,

$$W := \Omega^{\#}(M) \cong \frac{k[G]^{|A_2|-1+d_{G/\widehat{H}}}}{M}$$

and W is an indecomposable $k[G]$-module. Furthermore, as k-module we have that $W \cong k^a$ where

$$a = |G|d_{G/\widehat{H}} + \sum_{i\in A_2}\left(|G| - \frac{|G|}{|G_i|}\right) + 1 - |G|.$$

Proof: From Propositions 1, 9 and 12 we have that M is an indecomposable $k[G]$-module. We have that any injective $k[G]$-component N of M satisfies $N \cong k[G]^b$ for some $b \in \mathbb{N}_0$. Since $\mathcal{N}(M) = 0$ it follows that $b = 0$ ([15], Proposition 1). Therefore $M \cong M^{(1)}$. From Proposition 2-(c) we have that $\Omega^{\#}(M)$ is an indecomposable $k[G]$-module.

The $k[G]$-sequence

$$0 \longrightarrow M \longrightarrow k[G]^{|A_2|-1+d_{G/\widehat{H}}} \longrightarrow \Omega^{\#}(M) \longrightarrow 0 \tag{27}$$

is exact (Proposition 6-(c)). The result follows. ∎

THEOREM 1: *Let L/K be a finite Galois p-extension of algebraic function fields of one variable with Galois group $G = \mathrm{Gal}(L/K)$ and field of constants an algebraically closed field k of characteristic p. Let $\Omega_L^s(0)$ be the $k[G]$-module of the semisimple holomorphic differentials of L. Let $P_1, \dots, P_r$ be the ramified primes in L/K and let $G_1, \dots, G_r$ be their decomposition groups respectively. For each $i \in [\![1, r]\!]$ we define $\widehat{G_i} := \langle gG_ig^{-1} \mid g \in G\rangle$ the normal closure of the subgroup G_i in G, $\widehat{H} := \widehat{G_1} \cdots \widehat{G_r}$ and $d_{G/\widehat{H}}$ the minimal number of generators of the group $G/\widehat{H}$. Reordering the indices and taking conjugates if necessary, let $1 \leq i_1 < i_2 < \cdots < i_{s-1} < i_s = r$ be such that*

$$\begin{array}{ccc} G_1, & \dots, & G_{i_1-1} \subseteq G_{i_1} \\ G_{i_1+1}, & \dots, & G_{i_2-1} \subseteq G_{i_2} \\ & \vdots & \\ G_{i_{s-1}+1}, & \dots, & G_{i_s-1} \subseteq G_{i_s} = G_r \end{array}$$

and such that satisfy the condition: If for $1 \leq j, k \leq s$, there exists some $g \in G$ such that $G_{i_j}^g = gG_{i_j}g^{-1} \subseteq G_{i_k}$, then $j = k$. Let $A_2 := \{i_1, i_2, \dots, i_s\}$ and $A_1 := [\![1, r]\!] - A_2$. Then the modular decomposition in terms of indecomposable $k[G]$-modules of $\Omega_L^s(0)$ is given by

$$\Omega_L^s(0) \cong k[G]^{r_K - d_{G/\widehat{H}}} \oplus \bigoplus_{i \in A_1} I_{G,G_i} \oplus \Omega(\ker(\Phi_0)),$$

where

$$I_{G,G_i} = \left\{ \sum_{g \in G} a_g g \in k[G]\colon \sum_{g \in \sigma} a_g = 0 \ \forall \sigma \in G/G_i \right\},$$

Φ_0 is the restriction of Φ on the module $\bigoplus_{i \in A_2} k[G/G_i]$, where Φ is as in (3). We have that

$$\ker(\Phi_0) = \left\{ \left(\sum_{\sigma \in G/G_{i_1}} a_\sigma \sigma, \dots, \sum_{\sigma \in G/G_{i_s}} a_\sigma \sigma \right)\colon \sum_{i \in A_2} \sum_{\sigma \in G/G_i} a_\sigma = 0 \right\},$$

$$\Omega(\ker(\Phi_0)) \cong \Omega(\mathbb{X}(M)), \quad \text{where } M = \frac{\bigoplus_{i \in A_2} k[G/G_i]}{k e_{A_2}^*},$$

$$ke^*_{A_2} = \left\{ \Big(\sum_{\sigma \in G/G_{i_1}} x\sigma, \ldots, \sum_{\sigma \in G/G_{i_s}} x\sigma \Big) \in \bigoplus_{i \in A_2} k[G/G_i] \colon x \in k \right\}.$$

The indecomposable $k[G]$*-module*

$$W := \Omega(\ker(\Phi_0)) \cong \frac{k[G]^{|A_2|-1+d_{G/\widehat{H}}}}{M}$$

satisfies $W \cong k^a$ *as* k*-module, where*

$$a = |G| d_{G/\widehat{H}} + \sum_{i \in A_2} \Big(|G| - \frac{|G|}{|G_i|} \Big) + 1 - |G|.$$

Proof: From Proposition 6-(e) we have that as $k[G]$-modules

$$\mathbb{X}(\Omega^s_L(0)) \cong k[G]^u \oplus \Omega^\# \Big(\frac{\bigoplus_{i=1}^r k[G/G_i]}{ke^*} \Big)$$

for some $u \geq 0$. From Propositions 2-(d), 6, 7, 8 and 9 we obtain

$$\mathbb{X}(\Omega^s_L(0)) \cong k[G]^{\tau_K - d_{G/\widehat{H}}} \oplus \bigoplus_{i \in A_1} \frac{k[G]}{k[G/G_i]} \oplus \Omega^\#(M). \tag{28}$$

Therefore

$$\mathbb{X}(\mathbb{X}(\Omega^s_L(0))) \cong \mathbb{X}(k[G]^{\tau_K - d_{G/\widehat{H}}}) \oplus \mathbb{X}\Big(\bigoplus_{i \in A_1} \frac{k[G]}{k[G/G_i]} \Big) \oplus \mathbb{X}(\Omega^\#(M)).$$

From the argument used to prove Proposition 6-(a) it follows that $\mathbb{X}(\ker(\Phi_0)) \cong M$. Therefore, from Proposition 5 and ([6], Lemma 3.5) we have that as $k[G]$-modules

$$\mathbb{X}(\Omega^\#(M)) \cong \mathbb{X}(\Omega^\#(\mathbb{X}(\ker(\Phi_0)))) \cong \mathbb{X}(\mathbb{X}(\Omega(\ker(\Phi_0)))) \cong \Omega(\ker(\Phi_0)). \tag{29}$$

From Propositions 2-(d), 5 we have that

$$\mathbb{X}\Big(\frac{k[G]}{k[G/G_i]} \Big) \cong \Omega\left(\mathbb{X}(k[G/G_i])\right) \cong \Omega(k[G/G_i]).$$

From [16] and [17] we have that $I_{G,G_i} \cong \Omega(k[G/G_i])$ and that I_{G,G_i} is an indecomposable $k[G]$-module.

From ([6], Corollary 3.4, Lemmas 3.5 , 3.6), (28) and (29) we obtain that

$$\Omega^s_L(0) \cong k[G]^{\tau_K - d_{G/\widehat{H}}} \oplus \bigoplus_{i \in A_1} I_{G,G_i} \oplus \Omega(\ker(\Phi_0)).$$

Finally, from Propositions 1, 12, 13 and ([6], Lemma 3.5) we have that the $k[G]$-module $\mathbb{X}(\Omega^\#(M)) \cong \Omega(\ker(\Phi_0))$ is an indecomposable $k[G]$-module. ∎

References

[1] F. W. Anderson and K. R. Fuller, *Rings and Categories of Modules*, Graduate Texts in Mathematics **13**, Springer-Verlag, Berlin–Heidelberg–New York, 1974.

[2] C. Chevalley, *Introduction to the Theory of Algebraic Functions of One Variable*, Mathematical Surveys No. **6**, American Mathematical Society, 1951.

[3] C. W. Curtis and I. Reiner, *Methods of Representation Theory with Applications to Finite Groups and Orders*, Pure and Applied Mathematics, Wiley-Interscience, New York, Vol. I, 1981; Vol. II, 1987.

[4] K. Iwasawa, *Algebraic Functions*, Translations of Mathematical Monographs, Vol. 118, American Mathematical Society, 1993.

[5] G. Karpilovsky, *Group Representations*, North-Holland Mathematics Studies, **175** Vol. I, North-Holland, Amsterdam–London–New York–Tokyo, 1992.

[6] G. Karpilovsky, *Group Representations*, North-Holland Mathematics Studies, **175** Vol. II, North-Holland, Amsterdam–London–New York–Tokyo, 1992.

[7] G. Karpilovsky, *Topics in Field Theory*, North-Holland Mathematics Studies, **155**, North-Holland, Amsterdam, 1992.

[8] S. Nakajima, *Equivariant form of the Deuring–Šafarevič formula for Hasse–Witt invariants*, Mathematische Zeitschrift **190** (1985), 559–566.

[9] Sudarshan K. Sehgal, *Topics in Group Rings*, Pure and Applied Mathematics, Vol. 50, Marcel Dekker, New York, 1978.

[10] J.-P. Serre, *Local Fields*, Graduate Texts in Mathematics **67**, Springer-Verlag, New York, 1979.

[11] J.-P. Serre, *Sur la topologie des variétés algébriques en caractéristique p*, Symposium Internacional de Topología Algebraica, Universidad Autónoma de México y UNESCO, 1956, pp. 24–53.

[12] D. Subrao, *The p-rank of Artin–Schreier curves*, Manuscripta Mathematica **16** (1975), 169–193.

[13] J. Tate, *Genus change in inseparable extensions of function fields*, Proceedings of the American Mathematical Society **3** (1951), 400–406.

[14] R. Valentini, *Some p-adic Galois representations for curves in characteristic p*, Mathematische Zeitschrift **192** (1986), 541–545.

[15] R. Valentini, *Representations of automorphisms on differentials of function fields of characteristic p*, Journal für die Reine und Angewandte Mathematik **335** (1982), 164–179.

[16] G. Villa and M. Madan, *Structure of semisimple differentials and p-class groups in $\mathbb{Z}_p$-extensions*, Manuscripta Mathematica **57** (1987), 315–350.

[17] G. Villa and M. Madan, *Integral representations of p-class groups in $\mathbb{Z}_p$-extensions, semisimple differentials and Jacobians*, Archiv der Mathematik **56** (1991), 254–269.