International Electronic Journal of Algebra
Volume 7 (2010) 59-77

MODULE HOMOMORPHISMS OF GROUP ALGEBRAS OF CYCLIC p-GROUPS IN CHARACTERISTIC p

Vahid Shirbisheh

Received: 8 January 2009; Revised: 22 July 2009
Communicated by Sait Halıcıoğlu

Abstract. Given a prime number p, we study the module theory of $F[G]$, where F is a field of characteristic p and G is a cyclic p-group. We describe a construction of the set of all injective homomorphisms between two finitely generated $F[G]$-modules in terms of their numerical invariants. We also give a conceptual characterization of injective $F[G]$-homomorphisms. Finally, we characterize all submodules of a given finitely generated $F[G]$-module. These results were applied to describe all solutions of a specific type of Galois embedding problems in [8].

Mathematics Subject Classification (2000): 13M99, 20D15
Keywords: module theory, group algebras, cyclic p-groups, Galois embedding problems

1. Introduction

The main motivation of this paper comes from Galois theory, specifically Galois embedding problems with finite abelian kernels of exponent p, where p is an odd prime number, see [7,8]. Consider *the inverse Galois problem of a group H over a field D*, that is finding a Galois extension K/D such that $H \simeq Gal(K/D)$. Sometimes, it is possible to reduce this problem to a simpler problem known as a *Galois embedding problem* that can be formulated as follows: Assume that we have a surjection $\pi : H \twoheadrightarrow G$ of groups and E/D is a solution for the inverse Galois problem of G over D, i.e. $G \simeq Gal(E/D)$. The Galois embedding problem associated with the surjection π over the field extension E/D is the problem of finding an embedding of the field extension E/D into a Galois extension K/D such that $H \simeq Gal(K/D)$ and the restriction of elements of $Gal(K/D)$ to E corresponds to the surjection π. Then, the Galois group $Gal(K/E)$ corresponds to the kernel of π which we denote by N. Thereby, one may consider groups in the group extension $1\to N\to H\to G\to 1$ correspondingly as Galois groups of the following tower of field extensions:

$$\begin{tikzcd} K \arrow[d, dash] \arrow[d, bend left=60, dash, "Gal(K/E)"] \arrow[dd, bend right=60, dash, "Gal(K/D)"'] \\ E \arrow[d, dash] \arrow[d, bend left=60, dash, "Gal(E/D)"] \\ D \end{tikzcd}$$

Here, N is called the *kernel of the Galois embedding problem*. The tools developed in this paper enable us to study Galois embedding problems with finite abelian kernels of exponent p over cyclic Galois extensions E/D of degree p. To explain the idea, let E/D be such an extension, i.e. $G = Gal(E/D) \simeq \mathbb{Z}/p\mathbb{Z}$. The Galois action of G on $E^\times$ induces an action of G on $E^\times/E^{\times p}$. Since $E^\times/E^{\times p}$ is a group of exponent p, one can consider the Galois module structure of $E^\times/E^{\times p}$ as an $\mathbb{F}_p[G]$-module structure. This $\mathbb{F}_p[G]$-module structure was studied in [3,4] and in more general setting in [5]. Using a relative version of Kummer theory as formulated in the following theorem, we can identify the $\mathbb{F}_p[G]$-module structure of finitely generated submodules of $E^\times/E^{\times p}$ with the $\mathbb{F}_p[G]$-module structure of their associated Kummer extensions.

Theorem 1.1. *Let E/D be a cyclic extension of degree p^l with Galois group G and let D contain a primitive pth root of unity. Let B be a subgroup of $E^\times$ containing $E^{\times p}$ and invariant under the Galois action of G. If $B/E^{\times p}$ is a finitely generated submodule of $E^\times/E^{\times p}$, then it has the same $\mathbb{F}_p[G]$-module structure as $Gal(E_B/E)$, where E_B is the Kummer extension associated with B as shown in the following diagram:*

$$\begin{tikzcd} E_B \arrow[d, dash] \arrow[d, bend left=60, dash, "Gal(E_B/E)"] \arrow[dd, bend right=60, dash, "Gal(E_B/D)"'] \\ E \arrow[d, dash] \arrow[d, bend left=60, dash, "G"] \\ D \end{tikzcd} \tag{1}$$

For the proof of the above theorem and necessary definitions and notations see [7], although it appeared briefly in [6] too. It was shown in [9] that E_B is Galois over D. Therefore, knowing all finitely generated $\mathbb{F}_p[G]$-submodules of $E^\times/E^{\times p}$ amounts to characterizing all finite Kummer extensions of E of exponent p, which are also Galois over D. These extensions are all possible answers of the Galois embedding problems associated with the group extensions $1 \to N \to H \to G \to 1$ over E/D, where N, the kernel of the Galois embedding problem, is a finite abelian group of exponent p. If the group $E^\times/E^{\times p}$ is finite, for instance when E is a p-adic field, one can apply the results of the present paper to describe all $\mathbb{F}_p[G]$-submodules of $E^\times/E^{\times p}$, hence all solvable Galois embedding problems with finite abelian kernels of exponent p over the field extension E/D.

Although, for our application in [8], we only need to consider the group algebra of the cyclic group $\mathbb{Z}/p\mathbb{Z}$ over $\mathbb{F}_p$, we prove all statements in a slightly more general setting. In this paper, we assume p is a prime number and G is the cyclic group of order $q = p^l$ for some positive integer l and F is a field of characteristic p.

Here, we summarize the content of this paper. In the rest of this section, we describe all ideals of the group algebra $F[G]$ and all indecomposable $F[G]$-modules (Proposition 1.2). We also introduce some notations and two sets of numerical invariants for finitely generated $F[G]$-modules. In Section 2, we describe some criteria in terms of linear algebra over F to determine when $F[G]$-homomorphisms between two finitely generated $F[G]$-modules are injective or surjective (Lemmas 2.1 and 2.5). In Section 3, we address the problem of the existence of injective and surjective $F[G]$-homomorphisms with respect to numerical invariants of the $F[G]$-modules under consideration (Propositions 3.1 and 3.2). As the main result of this section, we develop a constructive method to characterize all injective homomorphisms between two finitely generated $F[G]$-modules (Theorem 3.12). In Section 4, we propose a conceptual framework to study $F[G]$-modules and $F[G]$-homomorphisms. This section is concluded with a characterization of all injective $F[G]$-homomorphisms in terms of a specific family of linear maps between finite dimensional vector spaces over F (Theorem 4.6). Finally, in the last section, we use the results of Sections 1, 2 and 3 to characterize all submodules of a given finitely generated $F[G]$-module in terms of its numerical invariants (Theorem 5.5). The reader can modify most of the statements of this paper and their proofs to generalize them to the case that $F[G]$-modules are not necessarily finitely generated, although this condition is necessary in Sections 3 and 5.

Let G be generated by σ. In the group algebra $F[G]$, we set $x = \sigma - 1$ and define $A := F[x]/x^q$. Then, we have the following basic observations:

Proposition 1.2. (i) *$F[G] \simeq A$.*

(ii) *Every polynomial in A whose constant term is nonzero is invertible.*

(iii) *Every ideal of A is of the form $\langle x^m \rangle$ for some $0 \le m \le q$.*

(iv) *Let B be an indecomposable $F[G]$-module of dimension m over F. Then, $0 \le m \le q$ and $B \simeq \langle x^{q-m} \rangle \simeq A/\langle x^m \rangle$.*

Proof. (i) Since the characteristic of F is p, we have $\sigma^q - 1 = (\sigma - 1)^q$. Thus, $F[G] \simeq \frac{F[\sigma]}{\langle \sigma^q - 1 \rangle} \simeq \frac{F[\sigma]}{\langle (\sigma-1)^q \rangle} = \frac{F[x+1]}{\langle x^q \rangle} \simeq \frac{F[x]}{\langle x^q \rangle}$.

(ii) For a given polynomial $h(x) = 1 + c_1 x + \cdots + c_n x^n$, set $g(x) = h(x) - 1$. Then using the fact that $g(x)^q = 0$, we have

$$\begin{aligned} h(x)(1 - g(x) + g(x)^2 - \cdots \pm g(x)^q) &= (1 + g(x))(1 - g(x) + g(x)^2 - \cdots \pm g(x)^q) \\ &= 1 - g(x)^q \\ &= 1. \end{aligned}$$

This shows $h(x)$ is invertible and so is every polynomial with nonzero constant term.

(iii) It is well known that A is a principal ideal domain. Let I be an ideal of A generated by a polynomial $P(x) = a_m x^m + a_{m+1} x^{m+1} + ... + a_n x^n$, where $a_m \neq 0$ and $m \leq n \leq q - 1$. If $n > m$, write $P(x) = x^m(a_m + a_{m+1} x + ... + a_n x^{n-m})$. By Part (ii), $a_m + a_{m+1} x + ... + a_n x^{n-m}$ has an inverse, say $Q(x)$. Thus, we have $x^m = P(x)Q(x) \in I$. On the other hand, $P(x) \in \langle x^m \rangle$. These facts prove that $I = \langle x^m \rangle$.

(iv) Let B be an indecomposable $F[G]$-module whose dimension over F is m. By Part (i), B is an A-module, and since B is finite dimensional, it is finitely generated. On the other hand, by the decomposition theorem of principal ideal domains, [2, page 402], B is isomorphic to a direct sum of cyclic A-modules. Now, since B is indecomposable, its decomposition has exactly one cyclic module which is isomorphic to A/I for some ideal I of A. By Part (iii), we have $B \simeq A/\langle x^m \rangle$ where $0 \leq m \leq q$. The map defined by $1 \mapsto x^{q-m}$ gives an isomorphism from $A/\langle x^m \rangle$ onto $\langle x^{q-m} \rangle \subseteq A$. $\square$

In the above proposition, we used the same notation for x and the class of x in A, and we will keep using this notation in the rest of this paper. The proof of Part (iv) of the above proposition has been taken from [1].

Now, we set up the notations that will be used in the rest of this paper. Consider two fixed finitely generated $F[G]$-modules decomposed into direct sums of cyclic modules as follows:

$$\begin{aligned} M &= B_1 \oplus \cdots \oplus B_r \\ L &= C_1 \oplus \cdots \oplus C_s, \end{aligned}$$

where $B_i = \langle x^{q-l_i} \rangle$ has dimension l_i and $C_j = \langle x^{q-k_j} \rangle$ has dimension k_j for some $1 \leq l_i, k_j \leq q$. Whenever it is useful, we will also assume that summands of each $F[G]$-module are in decreasing order with respect to their dimensions over F. Therefore, for given finitely generated $F[G]$-modules M and L, positive integers $(l_1, \cdots, l_r)$ and $(k_1, \cdots, k_s)$ are complete sets of invariants of M and L respectively.

Example 1.3. Let $q = 3^2$ and $M = \langle x\rangle \oplus \langle x^3\rangle \oplus \langle x^5\rangle \oplus \langle x^5\rangle \oplus \langle x^6\rangle$. Then $r = 5$ and the numerical invariants $(8, 6, 4, 4, 3)$ determine the $F[G]$-module structure of M up to isomorphism.

There is yet another set of invariants for a finitely generated $F[G]$-module. For $k = 1, \cdots, q$, let k_M (resp. k_L) be the number of cyclic summands of M (resp. L) of dimension greater than or equal to k. We also denote the direct sum of such summands of M (resp. L) by $M_{(k)}$ (resp. $L_{(k)}$). We always have $1_M = r$ and $M_{(1)} = M$. Clearly, the q-tuple $(1_M, \cdots, q_M)$ (resp. $(1_L, \cdots, q_L)$) is another complete set of invariants of M (resp. L). It has two advantages. First, it has the constant length q. In other words, it encodes the order of the group G as well. Second, its components are in a decreasing order.

Example 1.4. Let M be as Example 1.3. Then, one easily computes $(1_M, \cdots, 9_M) = (5, 5, 5, 4, 2, 2, 1, 1, 0)$. Moreover, we have $M_{(1)} = M_{(2)} = M_{(3)} = \langle x\rangle \oplus \langle x^3\rangle \oplus \langle x^5\rangle \oplus \langle x^5\rangle \oplus \langle x^6\rangle$, $M_{(4)} = \langle x\rangle \oplus \langle x^3\rangle \oplus \langle x^5\rangle \oplus \langle x^5\rangle$, $M_{(5)} = M_{(6)} = \langle x\rangle \oplus \langle x^3\rangle$, $M_{(7)} = M_{(8)} = \langle x\rangle$ and $M_{(9)} = 0$.

Remark 1.5. Assume the numerical invariant $(l_1, \cdots, l_r)$ of M is given. As in Example 1.4, one can compute the numerical invariant $(1_M, \cdots, q_M)$ by the formula $k_M = \sum_{l_i \geq k} 1$ for all $1 \leq k \leq q$. Moreover, we have $M_{(k)} = \oplus_{l_i \geq k} \langle x^{q-l_i}\rangle$ for all $1 \leq k \leq q$.

Conversely, let the numerical invariant $(1_M, \cdots, q_M)$ of M be given. Then, the number r of cyclic summands of M is the greatest integer appearing in the q-tuple $(1_M, \cdots, q_M)$. l_1 is the place of the last nonzero component of $(1_M, \cdots, q_M)$, i.e. $l_1 = k$ if and only if $k_M \neq 0$ and $(k+1)_M = 0$ (provided that $k + 1 \leq q$). Then, $l_1 = l_2 = \cdots = l_{n_1}$, where $n_1 = k_M$. Now, let k'_M be the first distinct number before k_M in the sequence $(1_M, \cdots, q_M)$. Then, $l_{n_1+1} = \cdots = l_{n_1+n_2} = k'$, where $n_2 = k'_M - k_M$. In this way, one can inductively compute the numerical invariants $(l_1, \cdots, l_r)$ using the numerical invariants $(1_M, \cdots, q_M)$, as in the next example.

Example 1.6. Let M be an $F[G]$-module that $(1_M, \cdots, q_M) = (10, 9, 6, 6, 6, 5, 5, 2)$. Then, $|G| = q = 8 = 2^3$ and so $p = 2$. Moreover, $r = 10$ and one easily computes $(l_1, \cdots, l_{10}) = (8, 8, 7, 7, 7, 5, 2, 2, 2, 1)$. Hence,

$$M = \left(\bigoplus_{j=1}^{2} \langle 1\rangle\right) \oplus \left(\bigoplus_{j=1}^{3} \langle x\rangle\right) \oplus \langle x^3\rangle \oplus \left(\bigoplus_{j=1}^{3} \langle x^6\rangle\right) \oplus \langle x^7\rangle.$$

Remark 1.7. The above discussion suggests that all statements regarding M and L could be stated in terms of at least one of these two types of numerical invariants.

Let $\varphi : M \to L$ be an $F[G]$-homomorphism. We use the same notation for the restriction of φ to each summand of M. For $i = 1, ..., r$ (resp. $j = 1, ..., s$), let b_i (resp. c_j) be the generator of B_i (resp. C_j) in M (resp. in L) defined by $(0, ..., 0, \overbrace{x^{q-l_i}}^{i\,th\,place}, 0, ..., 0)^t$ (resp. $(0, ..., 0, \overbrace{x^{q-k_j}}^{j\,th\,place}, 0, ..., 0)^t$). We sometimes consider M and L respectively as submodules of A^r and A^s in the obvious way.

Remark 1.8. We note that $x^{l_i} b_i = 0$ in B_i, and so, the image of B_i under φ is annihilated by x^{l_i}. Thus, it is contained in $\left(\oplus_{j=1}^{s} \langle x^{q-l_i} \rangle\right) \cap L$ (as a submodule of A^s).

2. Injectivity and surjectivity of homomorphisms

For an $F[G]$-module K, let K^G denote the submodule of G-invariant elements of K. Although, the following lemma holds in greater generality in terms of socles of modules the present formulation is sufficient for our purpose.

Lemma 2.1. *Let $\varphi : M \to L$ be an $F[G]$-homomorphism and let $\widetilde{\varphi} : M^G \to L^G$ denote the restriction of φ to M^G. Then, φ is injective if and only if $\widetilde{\varphi}$ is injective.*

Proof. Assume φ is not injective. Then $\varphi(m) = 0$ for some non zero $m \in M$. Let n be the largest integer such that $x^n m \neq 0$. Then $(\sigma - 1)(x^n m) = x(x^n m) = x^{n+1} m = 0$, so $x^n m \in M^G$ and we have $\widetilde{\varphi}(x^n m) = \varphi(x^n m) = x^n \varphi(m) = 0$. This shows $\widetilde{\varphi}$ is not injective too. The converse is clear. □

We will see in Lemma 2.5 that the above lemma can be considered as a statement dual to Nakayama's lemma. In the following, we associate a linear map to every $F[G]$-homomorphism between two finitely generated $F[G]$-modules. This linear map can be thought of as the restriction of the homomorphism to fixed submodules as Lemma 2.1. This allows us to reduce the study of injective $F[G]$-homomorphisms to the linear algebra problem of determining one-to-one linear maps between vector spaces over F.

Definition 2.2. Let $\varphi : M \to L$ be an $F[G]$-homomorphism. We define a linear map $\overline{\varphi} : F^r \to F^s$ by setting $\overline{\varphi}(e_i) := x^{l_i - 1} \varphi(b_i)$ and extending it linearly, where $\{e_1, ... e_r\}$ is the standard basis of F^r.

Remark 2.3. In the above definition, we considered the isomorphism $F^s \simeq \langle x^{q-1} \rangle^s$ for the target of $\overline{\varphi}$.

Remark 2.4. As before, let $\widetilde{\varphi}$ denote the restriction of φ to M^G with L^G as its target. Then, $\widetilde{\varphi}$ as an F-linear map is the same as $\overline{\varphi}$. To see this, we first note that $M^G = B_1^G \oplus \cdots \oplus B_r^G$. On the other hand, for $i = 1, \cdots, r$, B_i^G is generated by $x^{l_i-1}b_i = (0, ..., 0, \overbrace{x^{q-1}}^{i\,th\,place}, 0, ..., 0)^t$, and so it has dimension 1 over F. Thus, we have $\widetilde{\varphi}(x^{l_i-1}b_i) = \varphi(x^{l_i-1}b_i) = x^{l_i-1}\varphi(b_i) = \overline{\varphi}(e_i)$.

Although the interpretation of $\overline{\varphi}$ as the restriction of φ to M^G is simpler, the way we defined it in the above definition is constructive and it helps to construct injective $F[G]$-homomorphisms using some specific matrices.

Now, we give a similar criterion for surjectivity of an $F[G]$-homomorphism. Let I be the augmentation ideal of A, i.e. the ideal generated by $x = \sigma - 1$ in A. For an $F[G]$-module K, we set $K_G = K/IK$. For every $F[G]$-homomorphism $\varphi : M \to L$, we have $\varphi(IM) \subseteq IL$. Thus, φ induces a map $\widehat{\varphi} : M_G \to L_G$ defined by $\widehat{\varphi}(m + IM) := \varphi(m) + IL$. Since L is finitely generated and I is nilpotent the following lemma follows from Nakayama's lemma:

Lemma 2.5. *$\varphi : M \to L$ is surjective if and only if $\widehat{\varphi} : M_G \to L_G$ is surjective.*

Proof. Obviously, the surjectivity of φ implies the surjectivity of $\widehat{\varphi}$.

Conversely, let $\widehat{\varphi}$ be surjective and let $R = \varphi(M)$. Then, by surjectivity of $\widehat{\varphi}$, we have $L = R + IL$. By Nakayama's lemma $R = L$. Therefore, φ is surjective. $\square$

The above lemma holds in greater generality in terms of radicals of modules, but the above formulation is adequate for our purpose. The map $\widehat{\varphi}$, as a linear map over F, can be constructed as follows:

Definition 2.6. Let $\varphi : M \to L$ be an $F[G]$-homomorphism. We associate a linear map $\underline{\varphi} : F^r \to F^s$ with φ by setting

$$\underline{\varphi}(e_j) := \begin{pmatrix} a_{1j}x^{k_1-1} \\ \vdots \\ a_{sj}x^{k_s-1} \end{pmatrix},$$

where $\{e_1, ...e_r\}$ is the standard basis of F^r and $\varphi(b_j) = \begin{pmatrix} a_{1j} \\ \vdots \\ a_{sj} \end{pmatrix}$. We used the isomorphism $\left(\langle x^{q-1}\rangle\right)^s \simeq F^s$ for the target of $\underline{\varphi}$.

Remark 2.7. The maps $\widehat{\varphi}$ and $\underline{\varphi}$ are equal as F-linear maps. To see this, we first note that $M_G = M/IM = B_1/IB_1 \oplus \cdots \oplus B_r/IB_r$ and each B_j/IB_j is one dimensional and generated by b_j. Thus, we have

$$\begin{aligned}\widehat{\varphi}(b_j+IM) &= \varphi(b_j)+IL\\ &= \left[\sum_{i=1}^{s}\begin{pmatrix}0\\ \vdots\\ a_{ij}\\ \vdots\\ 0\end{pmatrix}\leftarrow (i\,th\,place)\right]+(IC_1\oplus\cdots\oplus IC_s)\\ &= \sum_{i=1}^{s}\begin{pmatrix}0\\ \vdots\\ a_{ij}\\ \vdots\\ 0\end{pmatrix}+IC_i.\end{aligned}$$

This shows that all terms of degree more than $q-k_i$ in the ith component of $\widehat{\varphi}(b_j+IM)$ can be considered zero. On the other hand, there is no term of degree less than $q-k_i$ in the ith component of $\widehat{\varphi}(b_j+IM)$. Thus, the ith component of $\widehat{\varphi}(b_j+IM)$ as an element of F is equal to the coefficient of x^{q-k_i} in a_{ij}. This is exactly the ith component of $\underline{\varphi}(e_j)$ as an element of F, because terms with degree greater than x^{q-k_i} in a_{ij} vanish due to the factor x^{k_i-1} and again there is no term of degree less that $q-k_i$ in a_{ij}.

3. Characterization of injective homomorphisms

From linear algebra, we know that there is an injective linear map from F^r into F^s if and only if $r\leq s$. By Lemma 2.1, this is a necessary condition for the existence of an injective homomorphism from M into L too. But, it is not sufficient, e.g. A cannot be embedded into $\langle x\rangle$. Here, we describe a sufficient condition for the existence of injective homomorphisms between two given finitely generated $F[G]$-modules. Afterwards, we shall describe the set of all injective $F[G]$-homomorphisms between them in terms of the cartesian product of two specific families of matrices.

Proposition 3.1. *There is at least one injective homomorphism from M into L if and only if $k_M\leq k_L$ for $k=1,...,q$.*

Proof. Assume the components of M and L are in decreasing order with respect to their dimension over F. Let $\varphi: M\to L$ be an injective homomorphism. For $k=1,\cdots,q$, let ι_k denote the natural embedding of $M_{(k)}$ into M. Then, $\varphi\iota_k: M_{(k)}\to L$ is injective too. If $l_i\geq k$, then according to Definition 2.2, $\overline{\varphi\iota_k}(e_i)=\overline{\varphi}(e_i)=x^{l_i-1}\varphi(b_i)$. Therefore, if C_j has dimension less than k, the jth component of $x^{l_i-1}\varphi(b_i)$ is zero. So, for $1 \leq i \leq r$, if $l_i \geq k$, then only first k_L components of $\overline{\varphi\iota_k}(e_i)$ can be nonzero. Now, by Lemma 2.1, the injectivity of $\overline{\varphi\iota_k}$ implies that $k_M \leq k_L$. Conversely, let $k_M \leq k_L$ for $k = 1, \cdots, q$. Then, $r \leq s$ and it is easy to see that $l_i \leq k_i$ for $1 \leq i \leq r$. Therefore, one can embed summands of M into summands of L correspondingly. This gives us an injective homomorphism from M into L. $\square$

The following proposition answers the same question about the existence of surjective homomorphisms between two finitely generated $F[G]$-modules:

Proposition 3.2. *There is at least one surjective homomorphism from M onto L if and only if $k_M \geq k_L$ for $k = 1, ..., q$.*

Proof. Let $k_M \geq k_L$ for $k = 1, ..., q$. Then, one notes that if $j \geq i$ then $\langle x^{q-i}\rangle \simeq \frac{\langle x^{q-j}\rangle}{\langle x^{q-j+i}\rangle}$. This means that any cyclic module can be considered as a quotient of cyclic modules of higher dimensions. For the converse, namely, when there is a surjective homomorphism $\varphi : M \to L$, one can consider the composition of φ with natural surjections $\pi_k : L \to L_{(k)}$. Then the statement follows from Lemma 2.5 and Remark 2.7. $\square$

In Definition 2.2, we associated a linear map $\overline{\varphi}$ to every homomorphism φ. Then, using Lemma 2.1, we were able to determine when φ is injective by studying the injectivity of $\overline{\varphi}$. Now, we are going in the reverse direction, namely, we start with a linear map T between two vector spaces over F and an $F[G]$-homomorphism S of specific form and we construct an $F[G]$-homomorphism $\Phi_{T,S}$. Afterwards, we will explain the necessary condition on T that implies the injectivity of $\Phi_{T,S}$. This also means that the injectivity of $\Phi_{T,S}$ has nothing to do with S. It provides us with a method, based on linear algebra over F, to construct all injective homomorphisms between two $F[G]$-modules using F-linear maps.

Definition 3.3. Let $M_{sr}(F)$ (resp. $M_{sr}(I)$) denote the set of all $s \times r$ matrices with entries in F (resp. $I = \langle x\rangle \subseteq A$). For given $T = (t_{ij}) \in M_{sr}(F)$ and $S = (s_{ij}) \in M_{sr}(I)$, we define an $s \times r$ matrix $\Phi_{T,S}$ with entries in A as follows:

$$\Phi_{T,S} := ((t_{ij} + s_{ij})x^{n_{ij}}),$$

where n_{ij}'s are defined by

$$n_{ij} := \begin{cases} l_j - k_i & if \quad l_j > k_i \\ 0 & if \quad l_j \leq k_i \end{cases}$$

and are called the *correction numbers associated with M and L*. Further, $x^{n_{ij}}$'s are called the *correction powers associated with M and L*.

Lemma 3.4. *If we consider elements of M and L as column vectors with respect to the cyclic decompositions of M and L, then the matrix multiplication by $\Phi_{T,S}$ (from left) defines an $F[G]$-homomorphism from M into L.*

Proof. Clearly, $\Phi_{T,S}$ is an $F[G]$-homomorphism from A^r into A^s. We must show that the restriction of $\Phi_{T,S}$ to M (considered as a submodule of A^r) maps elements of M into L (considered as a submodule of A^s). It is enough to check this for some b_j, the generator of the jth cyclic summand of M. By definition, we have

$$\Phi_{T,S}(b_j) = \begin{pmatrix} (t_{1j} + s_{1j})x^{n_{1j}}x^{q-l_j} \\ \vdots \\ (t_{sj} + s_{sj})x^{n_{sj}}x^{q-l_j} \end{pmatrix}. \tag{2}$$

If we denote the least degree of terms occurring in the ith component of 2 by d_i, then by the definition of correcting numbers we always have $d_i \geq q - k_i$. Thus, the ith component of 2 belongs to C_i, the ith cyclic summand of L. This shows that $\Phi_{T,S}(b_j) \in L$. □

It is seen in the above discussion that $\Phi_{T,S}$ becomes a homomorphism from M into L because of the correction powers, hence the name. In the following example, we illustrate the content of the above definition and lemma.

Example 3.5. Assume $q = 3^2$, $F = \mathbb{F}_3$, $M = \langle x \rangle \oplus \langle x^5 \rangle$ and $L = \langle 1 \rangle \oplus \langle x^2 \rangle \oplus \langle x^7 \rangle$. Then, $r = 2$, $s = 3$, $l_1 = 8$, $l_2 = 4$, $k_1 = 9$, $k_2 = 7$, $k_3 = 2$ and the matrix (n_{ij}) of correcting numbers is

$$\begin{pmatrix} 0 & 0 \\ 1 & 0 \\ 6 & 2 \end{pmatrix}.$$

For $T = \begin{pmatrix} 2 & 1 \\ 1 & 0 \\ 0 & 1 \end{pmatrix}$ and $S = \begin{pmatrix} x^2 + 2x & x^3 \\ x^5 & x^8 + x^6 \\ x^4 + 2x^2 & x^7 \end{pmatrix}$, we have

$$\Phi_{T,S} = \begin{pmatrix} x^2 + 2x + 2 & x^3 + 1 \\ x^6 + x & x^8 + x^6 \\ 2x^8 & x^2 \end{pmatrix},$$

$$\Phi_{T,S}(b_1) = \Phi_{T,S} \begin{pmatrix} x \\ 0 \end{pmatrix} = \begin{pmatrix} x^3 + 2x^2 + 2x \\ x^7 + x^2 \\ 0 \end{pmatrix} \in L,$$

$$\Phi_{T,S}(b_2) = \Phi_{T,S} \begin{pmatrix} 0 \\ x^5 \end{pmatrix} = \begin{pmatrix} x^8 + x^5 \\ 0 \\ x^7 \end{pmatrix} \in L.$$

We also note that some terms in some entries of S vanish during the process of defining $\Phi_{T,S}$ and have no effect in $\Phi_{T,S}$. For instance, by replacing S with $S' = \begin{pmatrix} x^2+2x & x^3 \\ x^5 & x^8+x^6 \\ 2x^2 & 0 \end{pmatrix}$, we still get the same homomorphism. In other words, $\Phi_{T,S} = \Phi_{T,S'}$. We address this issue in Lemma 3.10 and Definition 3.11.

Definition 3.6. (i) For $j = 1, ..., r$ and $i = 1, ..., s$, *the* (i, j)*th correcting coefficient associated with* M *and* L is defined by

$$m_{ij} := \begin{cases} 1 & if \quad l_j \leq k_i \\ 0 & if \quad l_j > k_i \end{cases}$$

(ii) Let $T = (t_{ij}) \in M_{sr}(F)$. *The correction of* T *with respect to* M *and* L is the matrix defined by $T^c := (m_{ij}t_{ij})$.

Remark 3.7. We note that $m_{ij} = 1$ if $n_{ij} = 0$ and $m_{ij} = 0$ if $n_{ij} \neq 0$.

Example 3.8. With assumptions of Example 3.5, the matrix (m_{ij}) of correcting coefficient and correction of T are respectively

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \\ 0 & 0 \end{pmatrix}, \quad \begin{pmatrix} 2 & 1 \\ 0 & 0 \\ 0 & 0 \end{pmatrix}.$$

Lemma 3.9. $\overline{\Phi_{T,S}} = T^c$.

Proof. Let T and S be as Definition 3.3. Then, we have

$$\Phi_{T,S}(b_j) = x^{q-l_j} \begin{pmatrix} x^{n_{1j}}t_{1j} \\ \vdots \\ x^{n_{sj}}t_{sj} \end{pmatrix} + x^{q-l_j} \begin{pmatrix} x^{n_{1j}}s_{1j} \\ \vdots \\ x^{n_{sj}}s_{sj} \end{pmatrix}. \tag{3}$$

Thus, considering the standard basis $\{e_1, \cdots, e_r\}$ for F^r, the jth column of $\overline{\Phi_{T,S}}$ is equal to $x^{l_j-1}\Phi_{T,S}(b_j) = x^{q-1} \begin{pmatrix} x^{n_{1j}}t_{1j} \\ \vdots \\ x^{n_{sj}}t_{sj} \end{pmatrix} + x^{q-1} \begin{pmatrix} x^{n_{1j}}s_{1j} \\ \vdots \\ x^{n_{sj}}s_{sj} \end{pmatrix}$. Due to the fact that each entry of S comes from I, the second term is zero. Hence, Remarks 2.3 and 3.7, the jth column of $\overline{\Phi_{T,S}}$ is equal to $\begin{pmatrix} m_{1j}t_{1j} \\ \vdots \\ m_{sj}t_{sj} \end{pmatrix}$ and this is exactly the jth column of T^c in the standard basis. $\square$

The above lemma shows that in order to construct injective homomorphism between two $F[G]$-modules using Definition 3.3, only those matrices $T \in M_{sr}(F)$

are needed that are injective after correction. We denote the subset of $M_{sr}(F)$ consisting of all matrices that are *injective after correction with respect to M and L* by $Iac(M, L)$.

Like entries of T, some terms of some entries of S may vanish during the construction of $\Phi_{T,S}$, so they have no effect in the value of $\Phi_{T,S}$.

Lemma 3.10. *A term in the (i, j)th entry of S has effect in the value of $\Phi_{T,S}$ if and only if its degree is less than $\min\{l_j, k_i\}$.*

Proof. First, we note that $\min\{l_j, k_i\} = l_j - n_{ij}$. Let T and S be as Lemma 3.9. Then, 3 shows that to compute $\Phi_{T,S}(b_j)$, we multiply $x^{q-l_j+n_{ij}}$ to s_{ij}, so terms of degree greater than or equal to $l_j - n_{ij}$ in s_{ij} vanish and consequently they have no effect in the value of $\Phi_{T,S}$. □

Definition 3.11. A matrix $S \in M_{sr}(I)$ is called *non-vanishing with respect to M and L*, if the degree of the (i, j)th entry of S is less than $l_j - n_{ij}$ for all $i = 0, \cdots, s$ and $j = 1, \cdots, r$. The subset of $M_{sr}(I)$ consisting of all non-vanishing matrices with respect to M and L is denoted by $Nvm(M, L)$.

The set of all injective $F[G]$-homomorphisms from M into L is denoted by $Hom_G^{inj}(M, L)$.

Theorem 3.12. *(i) Every $F[G]$-homomorphism from M into L is equal to $\Phi_{T,S}$ for some $T \in M_{sr}(F)$ and $S \in Nvm(M, L)$.*

(ii) There is a bijective correspondence between $Hom_G^{inj}(M, L)$ and the cartesian product $Iac(M, L) \times Nvm(M, L)$.

Proof. (i) Let φ be an $F[G]$-homomorphism from M into L. Let $\varphi = (f_{ij})$ denote the matrix form of φ corresponding to the generating set $\{b_j\}_{j=1}^r$ of M. We know that $\varphi(b_j) \in (\langle x^{q-l_j}\rangle)^s \cap L = \oplus_{i=1}^s \langle x^{q-h_{ij}}\rangle$, where $h_{ij} = \min\{l_j, k_i\}$. So, we have $\varphi(b_j) = \begin{pmatrix} x^{q-h_{1j}} P_{1j}(x) \\ \vdots \\ x^{q-h_{sj}} P_{sj}(x) \end{pmatrix}$ for some polynomials $P_{ij}(x) \in A$. On the other hand, we have $\varphi(b_j) = (f_{ij})b_j = \begin{pmatrix} f_{1j}x^{q-l_j} \\ \vdots \\ f_{sj}x^{q-l_j} \end{pmatrix}$. Thus, for $i = 1, ..., s$ and $j = 1, ..., r$, we have $x^{q-l_j} f_{ij} = P_{ij}(x)x^{q-h_{ij}}$. If $l_j > k_i$, then $h_{ij} = k_i$, $q - k_i > q - l_j$, and $n_{ij} = l_j - k_i$. Thus, we have $f_{ij}x^{q-l_j} = P_{ij}(x)x^{q-k_i} = P_{ij}(x)x^{q-l_j}x^{l_j-k_i} = P_{ij}(x)x^{q-l_j}x^{n_{ij}}$. In the case that $l_j \leq k_i$ we have $h_{ij} = l_j$ and $n_{ij} = 0$. Thus, we again obtain

$$f_{ij}x^{q-l_j} = P_{ij}(x)x^{q-l_j}x^{n_{ij}}. \tag{4}$$

Therefore, 4 holds in both cases. The factor x^{q-l_j} in both sides of 4 allows us to assume $P_{ij}(x)$ and f_{ij} have no term of degree more than $l_j - 1$, because those terms will vanish and have no effect in the value of φ. Therefore, we can assume that

$$f_{ij} = P_{ij}(x)x^{n_{ij}}, \tag{5}$$

where both sides of 5 have no term of degree more than $l_j - 1$. This is equivalent to saying that $P_{ij}(x)$ has no term of degree more than $l_j - n_{ij} - 1$. This shows that if $T = (t_{ij})$ and $S = (s_{ij})$ are defined as follows

$$t_{ij} := \textit{the constant term of } P_{ij}(x),$$

and

$$s_{ij} := P_{ij}(x) - t_{ij},$$

then $(t_{ij}) \in M_{sr}(F)$ and $(s_{ij}) \in Nvm(M, L)$ and $\varphi = \Phi_{T,S}$.

(ii) Let $\varphi \in Hom_G^{inj}(M, L)$. Then, by Part (i) there exist $T \in M_{sr}(F)$ and $S \in Nvm(M, L)$ such that $\varphi = \Phi_{T,S}$. Since φ is injective, $\overline{\varphi} = \overline{\Phi_{T,S}} = T^c$ is injective. Thus, T is injective after correction.

Conversely, let $T \in Iac(M, L)$, then due to the fact that $\overline{\Phi_{T,S}} = T^c$ and T^c is injective, $\Phi_{T,S}$ has to be an injective $F[G]$-homomorphism for any matrix $S \in M_{sr}(\langle x \rangle)$. It is easy to see that this correspondence is bijective. □

Remark 3.13. In the case that F is a finite field, for instance $\mathbb{F}_p$, one can use the above discussion to write an algorithm to list all injective $F[G]$-homomorphisms.

4. A conceptual characterization of homomorphisms

In this section, we propose a framework to decompose an $F[G]$-module into q layers corresponding to different powers of x that annihilate each layer. Each layer of an $F[G]$-module would be a vector space over F. This approach provides us with a conceptual description of injective $F[G]$-homomorphisms between two $F[G]$-modules in terms of a specific family of F-linear maps between different layers of two $F[G]$-modules. One will see that this section is the continuation of the idea of Lemma 2.1.

Definition 4.1. For any finitely generated $F[G]$-module M, we define $M_0 := 0$, $M_1 := Ann(x)$, and for $2 \leq i \leq q$, let M_i be a complement subspace for $Ann(x^{i-1}) = M_1 \oplus \cdots \oplus M_{i-1}$ in $Ann(x^i)$. A decomposition $M \simeq M_1 \oplus \cdots \oplus M_q$ of M into direct sum of F-linear subspaces obtained in this way is called a *q-grading of M*. Whenever we have a q-grading of M, we will denote the ith component of an element $m \in M$ by m_i.

The name “grading” comes from the fact that $A = A_1 \oplus \cdots \oplus A_q$, where A_i is generated by x^{q-i} as an F-linear subspace of A, (and of course, in this case, we have $A_iA_j \subseteq A_{i+j}$, which makes no sense in general q-gradings). In this section, we denote the F-vector space generated by an element a in an $F[G]$-module by $\langle\langle a\rangle\rangle$.

Remark 4.2. With notations of Section 1, define $M_i := \bigoplus_{j=1}^{r}\langle\langle x^{q-i}\rangle\rangle \cap B_j$ for $1 \leq i \leq q$. Then the decomposition $M \simeq M_1 \oplus \cdots \oplus M_q$ is a q-grading for M. This is called the *q-grading associated with the decomposition* $M \simeq B_1 \oplus \cdots \oplus B_r$. It is clear that the jth summand of M_i is $\langle\langle x^{q-i}\rangle\rangle$ if $i \leq l_j$, otherwise it is zero. Therefore, some of the summands of M_i vanish for larger i's. Thus, the dimensions of M_i's are decreasing. We formalize this observation as follows.

For $2 \leq i \leq q$, we have $Ann(x^{i-1}) \subseteq Ann(x^i)$ and

$$M_i \simeq \frac{Ann(x^i)}{Ann(x^{i-1})}.$$

This isomorphism gives rise to the following inclusions for $2 \leq i \leq q$:

$$\begin{array}{rcl} \iota_i^{i-1} : M_i & \hookrightarrow & M_{i-1} \\ m + Ann(x^{i-1}) & \mapsto & xm + Ann(x^{i-2}) \end{array} \tag{6}$$

The above remark motivates the following definition.

Definition 4.3. (i) Let V be a finite dimensional vector space over F. A sequence consisting of $q-1$ inclusions ending to V as follows

$$V_q \xhookrightarrow{\iota_q^{q-1}} V_{q-1} \xhookrightarrow{\iota_{q-1}^{q-2}} \cdots \xhookrightarrow{\iota_2^1} V_1 = V$$

is called a *q-filtration of* V and is denoted by $(V_1, \cdots, V_q)$ or simply by V_*. Since $V = V_1$, we may omit V from the name of a q-filtration. The composition of n consecutive inclusions starting from V_m is denoted by $\iota_m^{m-n} : V_m \hookrightarrow V_{m-n}$, whenever it makes sense.

(ii) The sequence $(M_1, \cdots, M_q)$ defined in Definition 4.1 and Remark 4.2 is a q-filtration of the F-vector space $Ann(x) \leq M$ and it is called the *q-filtration associated with the q-grading $M \simeq M_1 \oplus \cdots \oplus M_q$ of M.*

(iii) A *q-homomorphism from a q-filtration $(V_1, \cdots, V_q)$ into another q-filtration* $(W_1, \cdots, W_q)$ is a family of F-linear maps $T_j : V_{j+1} \to W_1$ for $j = 0, \cdots, q-1$ such that $T_j\iota_{j+i}^{j+1}(V_{j+i}) \subseteq \iota_i^1(W_i)$, for all $j = 0, \cdots, q-1$ and for all $1 \leq i \leq q-j-1$. It is denoted by $T_* = \{T_j\}$. It is called *injective* if T_0 is injective. The set of all q-homomorphisms (resp. injective q-homomorphisms) from V_* into W_* is denoted by $Hom_q(V_*, W_*)$ (resp. $Hom_q^{inj}(V_*, W_*)$).

(iv) Let $\varphi : M \rightarrow L$ be an $F[G]$-homomorphism and let $(M_1, \cdots, M_q)$ (resp. $(L_1, \cdots, L_q)$) be the q-filtration associated with a q-grading of M (resp. L). For $j = 0, \cdots, q-1$, define $\varphi_j : M_{j+1} \rightarrow L_1$ by $m \mapsto \varphi(m)_1$. Since φ is an $F[G]$-homomorphism, $\{\varphi_j\}$ is a q-homomorphism from M_* into L_*. It is called the *q-grading of φ with respect to q-filtrations $M_* = (M_1, \cdots, M_q)$ and $L_* = (L_1, \cdots, L_q)$* and is denoted by φ_*. Despite the fact that the map

$$\varphi \mapsto \varphi_* \tag{7}$$

depends on q-filtrations M_* and L_*, we denote it simply by

$$\alpha : Hom_{F[G]}(M, L) \rightarrow Hom_q(M_*, L_*).$$

The following proposition follows immediately from the above definition:

Proposition 4.4. *Let V_* and W_* be two q-filtrations. Then $Hom_q(V_*, W_*)$ with following operations is an $F[G]$-module:*

$$\begin{aligned} \lambda\{T_j\} + \{S_j\} &:= \{\lambda T_j + S_j\}, \quad \forall \lambda \in F, \forall T_*, S_* \in Hom_q(V_*, W_*), \\ x\{T_j\} &:= \{U_j\}, \quad \forall T_* \in Hom_q(V_*, W_*), \end{aligned}$$

where $U_0 := 0$ and $U_j := T_{j-1}\iota^j_{j+1}$ for $1 \leq j \leq q-1$.

Example 4.5. With the assumptions of Example 3.5, we have

$$M_i = \begin{cases} \langle\langle x^{q-i}\rangle\rangle \oplus \langle\langle x^{q-i}\rangle\rangle & for \quad i = 1, \cdots, 4 \\ \langle\langle x^{q-i}\rangle\rangle \oplus 0 & for \quad i = 5, \cdots, 8 \\ 0 \oplus 0 & for \quad i = 9 \end{cases}$$

$$L_i = \begin{cases} \langle\langle x^{q-i}\rangle\rangle \oplus \langle\langle x^{q-i}\rangle\rangle \oplus \langle\langle x^{q-i}\rangle\rangle & for \quad i = 1, 2 \\ \langle\langle x^{q-i}\rangle\rangle \oplus \langle\langle x^{q-i}\rangle\rangle & for \quad i = 3, \cdots, 7 \\ \langle\langle x^{q-i}\rangle\rangle & for \quad i = 8, 9 \end{cases}$$

In order to explain how q-homomorphisms are related to $F[G]$-homomorphisms, we added zero spaces at the end of some of M_i's in the above formulas. All inclusions ι^i_{i+1} for all i's and for all M_{i+1}'s and L_{i+1}'s is the multiplication by x.

Let φ be $\Phi_{T,S} = \begin{pmatrix} x^2 + 2x + 2 & x^3 + 1 \\ x^6 + x & x^8 + x^6 \\ 2x^8 & x^2 \end{pmatrix}$ as Example 3.5. Then, one easily checks that the associated q-homomorphism $\{\varphi_j\}$ is computed as follows:

$$\varphi_0 \begin{pmatrix} \alpha x^8 \\ \beta x^8 \end{pmatrix} = \left(\varphi \begin{pmatrix} \alpha x^8 \\ \beta x^8 \end{pmatrix}\right)_1 = \begin{pmatrix} 2\alpha x^8 + \beta x^8 \\ 0 \\ 0 \end{pmatrix}_1 = \begin{pmatrix} 2\alpha x^8 + \beta x^8 \\ 0 \\ 0 \end{pmatrix},$$

$$\varphi_1\begin{pmatrix}\alpha x^7\\ \beta x^7\end{pmatrix}=\left(\varphi\begin{pmatrix}\alpha x^7\\ \beta x^7\end{pmatrix}\right)_1=\begin{pmatrix}2\alpha x^8+2\alpha x^7+\beta x^7\\ \alpha x^8\\ 0\end{pmatrix}_1=\begin{pmatrix}2\alpha x^8\\ \alpha x^8\\ 0\end{pmatrix}.$$

Hence, $\varphi_0=\begin{pmatrix}2&1\\0&0\\0&0\end{pmatrix}$, $\varphi_1=\begin{pmatrix}2&0\\1&0\\0&0\end{pmatrix}$ and similarly we obtain $\varphi_2=\begin{pmatrix}1&0\\0&0\\0&1\end{pmatrix}$,
$\varphi_3=\begin{pmatrix}0&1\\0&0\\0&0\end{pmatrix}$, $\varphi_4=\varphi_5=\varphi_7=\begin{pmatrix}0&0\\0&0\\0&0\end{pmatrix}$, $\varphi_6=\begin{pmatrix}0&0\\1&1\\0&0\end{pmatrix}$, $\varphi_8=\begin{pmatrix}0&0\\0&1\\2&0\end{pmatrix}$.
From this computation, it is clear that for $0\le i\le q-1$, the entry (r,s)th of φ_i is equal to the coefficient of x^i in the entry (r,s)th of φ.

As we observed in the above example, q-homomorphisms carry all information contained in $F[G]$-homomorphisms. We formulate this fact in the following theorem.

Theorem 4.6. *Let $M_*=(M_1,\cdots,M_q)$ (resp. $L_*=(L_1,\cdots,L_q)$) be the q-filtration associated with a q-grading of M (resp. L). Then, the map α, see 7, is an $F[G]$-isomorphism from $Hom_{F[G]}(M,L)$ onto $Hom_q(M_*,L_*)$, which maps the set of injective $F[G]$-homomorphisms onto the set of injective q-homomorphisms.*

Proof. First, we show α is an $F[G]$-homomorphism. For $\varphi,\psi\in Hom_{F[G]}(M,L)$ and $\lambda\in F$, it is clear that $(\varphi+\lambda\psi)_*=\varphi_*+\lambda(\psi_*)$. Let $U_*=\{U_j\}=(x\varphi)_*=\alpha(x\varphi)$. If $m\in M_1$, then we have $U_0(m)=(x\varphi(m))_1=(\varphi(xm))_1=0$. If $j=1,\cdots,q-1$ and $m\in M_{j+1}$, then we have $U_j(m)=(x\varphi(m))_1=(\varphi(xm))_1=\varphi_{j-1}(xm)=\varphi_{j-1}\iota^j_{j+1}$. This shows that $(x\varphi)_*=U_*=\{U_j\}=x\varphi_*=x\{\varphi_j\}$ as defined in Proposition 4.4.

Now, we prove α is an isomorphism. Let $\varphi\neq 0$. Then $(\varphi(m))_k\neq 0$ for some $k=1,\cdots,q$ and some $m\in M$. In other words, $\varphi(m)$ has a non-zero component in L_k. So, $x^{k-1}\varphi(m)=\varphi(x^{k-1}m)$ has a non-zero component in L_1. Thus, $(\varphi(x^{k-1}m))_1\neq 0$ and this implies that there exist $0\le j\le q-1$ and $m'\in M_{j+1}$ such that $\varphi_j(m')\neq 0$. Thus, $\varphi_j\neq 0$, and so $\varphi_*\neq 0$. Therefore, α is injective. For given $T_*\in Hom_q(M_*,L_*)$, we define $\varphi\in Hom_{F[G]}(M,L)$ such that $T_*=\alpha(\varphi)$ (with respect to M_* and L_*). For $m\in M$, define

$$\varphi(m):=(\sum_{j=0}^{q-1}T_j(m_{j+1}),\sum_{j=0}^{q-2}T_j(m_{j+2}),\cdots,T_0(m_q)),\forall\, m\in M,$$

where $m=m_1+\cdots+m_q$ with respect to the filtration M_* of M and the components of the right hand side of the above formula is considered with respect to the filtration L_*. Now, we compute φ_j for $j=0,\cdots,q-1$. For $m\in M_{j+1}$, we have $\varphi_j(m)=$

$(\varphi(m))_1 = \sum_{j=0}^{q-1} T_j(m_{j+1})$. Since, $m = m_{j+1} \in M_{j+1}$ the above sum reduces to $T_j(m)$ which shows $T_* = \varphi_* = \alpha(\varphi)$. Thus α is surjective. It is straightforward that φ_0 is the same map as $\widetilde{\varphi}$, the restriction of φ to M^G. Therefore, the last statement follows from Lemma 2.1. □

5. Submodules of an $F[G]$-module

Let M and L satisfy the condition of Proposition 3.1. Moreover, let ψ be an $F[G]$-automorphism of M and let φ be an injective $F[G]$-homomorphism from M into L. Then, we have $Im(\varphi\psi) = Im(\varphi)$, and so images of φ and $\varphi\psi$ define the same submodule of L isomorphic to M. Conversely, let $Im(\varphi_1) = Im(\varphi_2)$ for two injective $F[G]$-homomorphisms from M into L. We define $\psi : M \to M$ by $\psi(m) := \varphi_2^{-1}\varphi_1(m)$ for $m \in M$. It is clear that ψ is a bijection. Therefore, if we prove that it is an $F[G]$-homomorphism, then it is an $F[G]$-automorphism of M and we have $\varphi_2\psi = \varphi_1$. To show ψ is an $F[G]$-homomorphism, let $m \in M$, then $\varphi_2\varphi_2^{-1}(x\varphi_1(m)) = x\varphi_1(m) = x\varphi_2\varphi_2^{-1}(\varphi_1(m)) = \varphi_2(x\varphi_2^{-1}(\varphi_1(m)))$. Now, due to the fact that φ_2 is injective we have $\varphi_2^{-1}(x\varphi_1(m)) = x\varphi_2^{-1}(\varphi_1(m))$. Thus, $\psi(xm) = \varphi_2^{-1}\varphi_1(xm) = \varphi_2^{-1}(x\varphi_1(m)) = x\varphi_2^{-1}(\varphi_1(m)) = x\psi(m)$. Similarly, one checks that $\psi(m + m') = \psi(m) + \psi(m')$. Therefore, ψ is an $F[G]$-automorphism.

We define the action of $Aut_G(M)$, the group of all $F[G]$-automorphisms of M, on $Hom_G^{inj}(M, L)$, the set of injective homomorphisms from M into L, by $(\psi, \varphi) \mapsto \varphi\psi^{-1}$ for $\psi \in Aut_G(M)$ and $\varphi \in Hom_G^{inj}(M, L)$. It follows from the above discussion that the images of two injective $F[G]$-homomorphisms from M into L are the same if and only if they are in the same orbit of this action. Therefore, we obtain a description of the set of all submodules of L isomorphic to M as follows:

Proposition 5.1. *Let M and L satisfy the condition of Proposition 3.1. Then, there is a bijection between the set of all submodules of L isomorphic to M and*

$$\frac{Hom_G^{inj}(M, L)}{Aut_G(M)},$$

the set of all orbits of the action of $Aut_G(M)$ on $Hom_G^{Inj}(M, L)$.

One notes that the above proposition holds for more general algebras and their finitely generated modules. Now, by letting M vary through all isomorphic classes of submodules of L, we can parameterize all submodules of L.

Corollary 5.2. *Let $S(L)$ denote the set of all classes of submodules of L up to isomorphism. Then, the set of all submodules of L can be parameterized by*

$$\bigcup_{M \in S(L)} \frac{Hom_G^{inj}(M, L)}{Aut_G(M)}.$$

We describe $S(L)$ in terms of numerical invariants $k_1, \cdots, k_s$ of L.

Definition 5.3. As before, let s be the number of summands of L. We set

$$D^s := \{(n_1, \cdots, n_s) \in \mathbb{Z}^s; 0 \le n_i \le q, \, \forall i = 1, \cdots, s\}.$$

Let $\mathcal{L} = (n_1, \cdots, n_s) \in D^s$. As Remark 1.5, for all $k = 1, \cdots, q$, we define

$$k_{\mathcal{L}} := \sum_{n_i \ge k} 1 = |\{n_i \, ; \, n_i \ge k\}|.$$

Then $D(L)$ as a subset of D^s is defined as follows:

$$D(L) := \{\mathcal{L} = (n_1, \cdots, n_s) \in D^s; n_j \le n_i \, \forall \, i < j, \, and \, k_{\mathcal{L}} \le k_L \, \forall \, k = 1, \cdots, q\}$$

Now, let $M = B_1 \oplus \cdots \oplus B_r$ be a submodule of L. By assuming that cyclic components of M are in decreasing order with respect to their dimensions, Proposition 3.1 asserts that $\mathcal{L}(M) = (l_1, \cdots, l_r, \overbrace{0, \cdots, 0}^{s-r \, times})$ is an element of $D(L)$. We also note that if $M \simeq M'$, then $\mathcal{L}(M) = \mathcal{L}(M')$. Conversely, for $\mathcal{L} = (n_1, \cdots, n_s) \in D(L)$, we define a submodule of L by $M(\mathcal{L}) := \langle x^{q-n_1} \rangle \oplus \cdots \oplus \langle x^{q-n_s} \rangle$. This shows that $M \mapsto \mathcal{L}(M)$ is a bijective correspondence between $S(L)$ and $D(L)$ with the inverse $\mathcal{L} \mapsto M(\mathcal{L})$.

Example 5.4. Let $q = 3$ and $L = \langle 1 \rangle \oplus \langle x \rangle \oplus \langle x^2 \rangle$. Then, $s = 3$, $(k_1, k_2, k_3) = (3, 2, 1)$, $(1_k, 2_k, 3_k) = (3, 2, 1)$ and elements of $D(L)$ are $(0, 0, 0), (1, 0, 0), (1, 1, 0), (1, 1, 1), (2, 0, 0), (2, 1, 0), (2, 1, 1), (3, 0, 0), (3, 1, 0), (3, 1, 1), (3, 2, 0), (3, 2, 1)$.

We conclude this paper with the following theorem which characterizes all submodules of a finitely generated $F[G]$-module L.

Theorem 5.5. *There is a bijective correspondence between the set of all submodules of L and the following set:*

$$\bigcup_{\mathcal{L} \in D(L)} \frac{Hom_G^{inj}(M(\mathcal{L}), L)}{Aut_G(M(\mathcal{L}))}. \tag{8}$$

We note that all ingredients of 8 depend only on q and $k_1, \cdots, k_s$, which are invariants of L. Therefore, similar to Remark 3.13, when F is a finite field, one can use the constructions of the present section and Section 3 to write an algorithm to generate all the submodules of a finitely generated $F[G]$-module.

Acknowledgment. I would like to thank Ján Mináč, Ajneet Dhillon and John Swallow for their valuable comments and many helpful discussions. I would also like to thank referees for their suggestions and comments.

References

[1] G. Bhandari, Milnor K-theory as Galois modules in characteristic p, PhD thesis, The University of Western Ontario, 2005.

[2] P. Bhattacharya, S. K. Jain and S. R. Nagpaul, Basic Abstract Algebra, Second edition, Cambridge University Press, 1994.

[3] D. K. Faddeev, *On the structure of the reduced multiplicative group of a cyclic extension of a local field,* Izv. Akad. Nauk SSSR Ser. Mat., 24 (1960), 145–152.

[4] J. Mináč and J. Swallow, *Galois module structure of pth-power class of extensions of degree p*, Israel J. Math., 138 (2003), 29–42.

[5] J. Mináč, A. Schultz, J. Swallow, *Galois module structure of pth-power classes of cyclic extensions of degree* p^n, Proc. London Math. Soc., 3, 92 (2006), 307–341.

[6] J. Mináč, A. Schultz and J. Swallow, *Automatic realizations of Galois groups with cyclic quotient of order* p^n, J. Thor. Nombres Bordeaux, 20(2) (2008), 419–430.

[7] V. Shirbisheh, *A relative version of Kummer theory*, (arXiv:08081760).

[8] V. Shirbisheh, *Galois embedding problems with abelian kernels of exponent p,* VDM Verlag Dr. Mueller, ISBN: 978-3-639-14067-5, 2009.

[9] W. C. Waterhouse, *The normal closure of certain Kummer extensions,* Canad. Math. Bull., 37 (1994), 133–139.

Vahid Shirbisheh
Department of Mathematics
Faculty of Sciences
The University of Golestan
Gorgan, P.O. Box: 155
Golestan, Iran
e-mail: shirbisheh@gmail.com