International Electronic Journal of Algebra
Published Online: February 11, 2026
DOI: 10.24330/ieja.1886803

A PROPERTY OF LEADING MONOMIALS IN MODULAR POLYNOMIAL INVARIANTS

Bekir Danış

Received: 14 April 2025; Revised: 7 October 2025; Accepted: 17 January 2026
Communicated by A. Çiğdem Özcan

Abstract. We study modular polynomial invariants of the cyclic group C_p over a field of characteristic p where p is a prime number and use the reverse lexicographic order. We focus on the leading monomial of an invariant by considering the degrees of the terminal variables. It is obtained that this degree of each terminal variable is divisible by p when only pure powers of terminal variables appear in the leading monomial. Then, we show that this divisibility also holds for the general case, that is, the degrees of the terminal variables of the leading monomial are divisible by p. After proving this property, we investigate the cyclic group C_{p^k} for a positive integer k with the same characteristic p. By noticing that the same arguments with only minor changes can be applied to this case, we get that p divides the degree of each terminal variable.

Mathematics Subject Classification (2020): 13A50
Keywords: Leading monomial, modular polynomial invariant, degree of terminal variables

1. Introduction

For a given monomial order $<$, the largest monomial appearing in a polynomial f is called the leading (or initial) monomial and denoted by $LM_<(f)$. Leading monomials are beneficial since the ideal generated by leading monomials is a monomial ideal and it inherits some properties from the original ideal. Thus, considering the ideal of leading monomials is a shortcut to figure out combinatorial and geometrical properties of an ideal.

Monomial ideals and lead-term ideals provide a connection between commutative algebra and combinatorial algebra. As a conclusion, we note that the leading monomials are not only suitable objects for the computational aspect but crucial for the combinatorial structure of an ideal as well. For detailed theory of the leading terms, we refer the reader to [5].

We include basic notations and definitions about invariant theory because the main task to be accomplished is related to the leading monomials of a modular polynomial invariant. Let V be a vector space and V^* represents the dual space of V. For an infinite field F, the coordinate ring of V is denoted by $F[V]$ and it is

$$F[V] = F[x_1, x_2, \ldots, x_n]$$

where $x_1, x_2, \ldots, x_n$ form a basis of V^*.

Let G be a group and the action of G on the coordinate ring may be defined as follows

$$(af)(v) = f(a^{-1}(v))$$

for $a \in G$, $v \in V$ and $f \in F[V]$.

The invariant ring is defined by

$$F[V]^G := \{f \in F[V] \mid g(f) = f \text{ for all } g \in G\}.$$

After the definition of the invariant ring, recall that it is a modular case if the characteristic of F divides the order of G. For a survey of results on this invariant theory, see [2] and [3].

Throughout this paper, we use reverse lexicographic order $<$ by fixing the order of the variables as $x_1 < x_2 < \cdots < x_n$. The reason for using reverse lexicographic order is that an ideal and its leading-term ideal share some important properties with this order. In other words, reverse lexicographic order enables us to catch a relation between an ideal and its initial ideal, see [4, §15.7].

Biggest variable x_n is called terminal variable and we discuss the degree of terminal variable in leading monomial of a modular polynomial invariant. In this paper, we study cyclic groups of prime order p^k in modular situation, i.e., the characteristic of F is p. We suggest [1], [2] and [7] for more background on invariants for cyclic groups.

In this study, we prove p divides the degrees of terminal variables arising in the leading monomial of a modular polynomial invariant for C_{p^k}. To reach this conclusion, we consider whether the leading monomial of an invariant consists of only pure powers of terminal variables or not with the main emphasis on a single indecomposable module.

2. Main results

Let $G = C_{p^k}$ and g be a fixed generator of the cyclic group. For a G-module V over F, there are $|G| = p^k$ indecomposable C_{p^k}-modules over the field, namely

$V_1, \dots, V_{p^k}$ and it is known

$$V = V_{r_1} \oplus V_{r_2} \oplus \cdots \oplus V_{r_s}$$

for all $1 \leq r_j \leq p^k$ when j varies from 1 to s.

By noting the isomorphism between V_{r_j} and its dual, we consider the dual basis $x_{1,j}, x_{2,j}, \dots, x_{r_j,j}$ of $V_{r_j}^*$ and the action of g on these variables is given as follows

$$g(x_{i,j}) = x_{i,j} + x_{i-1,j} \text{ for all } 1 < i \leq r_j \text{ and } g(x_{1,j}) = x_{1,j}.$$

Furthermore, it is obvious that the description of polynomial ring $F[V]$ is

$$F[V] = F[x_{i,j} \mid 1 \leq i \leq r_j \text{ and } 1 \leq j \leq s].$$

We set monomial ordering as reverse lexicographic order with

$$x_{1,j} < x_{2,j} < \cdots < x_{r_j,j} \text{ for all } 1 \leq j \leq s$$

and the ordering of the variables lying in different indecomposable modules is defined by

$$x_{r_j,j} < x_{1,j+1} \text{ for all } 1 \leq j \leq s-1.$$

We call the $x_{r_j,j}$ for all possible j varying from 1 to s as terminal variables. Alternatively, the terminal variable is the biggest variable in the basis of each indecomposable module. We pay attention to the degrees of the terminal variables occurring in leading monomials.

Firstly, we concentrate on a single indecomposable G-module V_{r_n} with $1 \leq n \leq s$ because the generalization is easily followed from single indecomposable module case. Remember that the basis elements of V_{r_n} are $x_{1,n}, x_{2,n}, \dots, x_{r_n,n}$. For notational convenience, we take

$$y_i = x_{i,n} \text{ for all } 1 \leq i \leq r_n.$$

Then, we need the following lemma from [6]. (See [6, Lemma 1].)

Lemma 2.1. *Take an element $f \in F[V]^G$ and let M be a monomial showing up in f. Suppose, we have a monomial $M_1 \neq M$ and M_1 appears in $g(M)$. Then, there exists a monomial M_2 lying in f different than both M and M_1 satisfying that M_1 appears in $g(M_2)$.*

After the statement of this lemma, we take single G-module V_{r_n} with $1 \leq n \leq s$ and $r_n > 1$ into consideration. Since $F[V_1] = F[V_1]^G$, we may disregard V_1. Recall that $y_1, \dots, y_{r_n}$ form a basis for V_{r_n} and the action of g is

$$g(y_i) = y_i + y_{i-1} \text{ for } 1 < i \leq r_n \text{ and } g(y_1) = y_1.$$

The monomial ordering is reverse lexicographic order with $y_1 < \cdots < y_{r_n}$ and we show the following proposition.

Proposition 2.2. *Let $f \in F[V_{r_n}]^G$ and $M = y_{r_n}^d$ be the leading monomial of f for a positive integer d. For notational purposes, we write $M = LM_<(f)$. Then, we get that the characteristic p divides the degree of the terminal variable, $p \mid d$.*

Proof. Suppose $p \nmid d$. Then, we apply g to M and focus on the monomials appearing in $g(M)$. We have

$$g(M) = g(y_{r_n}^d) = (y_{r_n} + y_{r_n-1})^d.$$

Since d is not equivalent to 0 in mod p, it follows that $M_1 = (y_{r_n})^{d-1} y_{r_n-1}$ appears in $g(M)$ and it is different than M. Hence, we can use the previous lemma. By Lemma 2.1, there exists a monomial M_2 arising in f different than M, M_1 such that M_1 should be seen in $g(M_2)$. Note that $M_2 < M$ and assume

$$M_2 = y_{r_n}^b y_{r_n-1}^c \text{ for } b, c \geq 0.$$

Observe that if M_2 contains a variable except that y_{r_n}, y_{r_n-1}, finding M_1 in $g(M_2)$ is not possible.

Perform g to M_2 and get

$$g(M_2) = (y_{r_n} + y_{r_n-1})^b (y_{r_n-1} + y_{r_n-2})^c \text{ if } r_n > 2$$

or we have

$$g(M_2) = (y_{r_n} + y_{r_n-1})^b (y_{r_n-1})^c \text{ for } r_n = 2.$$

Since M_1 lies in $g(M_2)$, we have two options as follows:

$$M_1 = y_{r_n}^{b-1} y_{r_n-1} \text{ with } c = 0, b = d \text{ or } M_1 = y_{r_n}^b y_{r_n-1}^c \text{ with } c = 1, b = d-1.$$

Recognize that first choice implies $M_2 = M$ and second choice implies $M_2 = M_1$. This is a contradiction and so the assertion of the proposition follows. □

In Proposition 2.2, we deal with the case of a pure power of the terminal variable y_{r_n}. Next, we extend this case to more generalized version.

Theorem 2.3. *Let $f \in F[V_{r_n}]^G$ and $M = y_{r_n}^d N = LM_<(f)$ with no y_{r_n} in N for a positive integer d. We can say that N is a monomial in the variables $y_1, \ldots, y_{r_n-1}$. Then, we have $p \mid d$.*

Before the proof of Theorem 2.3, we need a technical lemma.

Lemma 2.4. *Let $M = y_{r_n}^d N$ be a monomial appearing in an invariant with no y_{r_n} in N and $d > 0$. Assume that*

$$M_1 = (y_{r_n})^{d-1} y_{r_n - 1} N \text{ appears in } g(M).$$

For a monomial $M_2 \neq M_1$ in $F[V_{r_n}]$ with $M_2 < M$, M_1 does not appear in $g(M_2)$.

Note that we do not need the assumption that M is the leading monomial for this lemma. This assumption is necessary in the statement of Theorem 2.3.

Proof of Lemma 2.4. If we have only one variable y_{r_n}, we handle this case by the same idea used in Proposition 2.2. Take

$$M = y_{r_n}^d y_{a_r}^{b_r} y_{a_{r-1}}^{b_{r-1}} \dots y_{a_1}^{b_1} \text{ with } a_r > \dots > a_1.$$

Suppose $M_1 = (y_{r_n})^{d-1} y_{r_n - 1} y_{a_r}^{b_r} y_{a_{r-1}}^{b_{r-1}} \dots y_{a_1}^{b_1}$ lies in $g(M_2)$ and seek a contradiction. Let α be the degree of y_{a_1} in M_2 and realize that we focus on the smallest variable with respect to the reverse lexicographic order. The ordering $M_2 < M$ implies that $\alpha \geq b_1$ since there is not any variable less than y_{a_1} inside M_2. It remains to prove $\alpha \leq b_1$. On the other hand, to catch a monomial containing $y_{a_1}^{b_1}$ in $g(M_2)$, we look at the consecutive terms and compute

$$g(y_{a_1+1}^{\beta}) = (y_{a_1+1} + y_{a_1})^{\beta}$$

and

$$g(y_{a_1}^{\alpha}) = (y_{a_1} + y_{a_1-1})^{\alpha} \text{ or } g(y_{a_1}^{\alpha}) = y_{a_1}^{\alpha} \text{ if } a_1 = 1$$

in $g(M_2)$ for some power β. For all cases, the main purpose is to get a term including $y_{a_1}^{b_1}$ without $\{y_i \mid i < a_1\}$ in $g(M_2)$. Therefore, we have $\alpha \leq b_1$ and this implies $\alpha = b_1$.

Next, we choose the smallest variable distinct from y_{a_1} with respect to the reverse lexicographic order. Let γ be the degree of y_{a_2} in M_2. By $M_2 < M$, we have $\gamma \geq b_2$. On the other hand, to catch a monomial containing $y_{a_2}^{b_2}$ in $g(M_2)$, we look at the consecutive terms and compute

$$g(y_{a_2+1}^{e}) = (y_{a_2+1} + y_{a_2})^{e}$$

and

$$g(y_{a_2}^{\gamma}) = (y_{a_2} + y_{a_2-1})^{\gamma}$$

in $g(M_2)$ for some power e. For all cases, the main purpose is to get a term including $y_{a_2}^{b_2} y_{a_1}^{b_1}$ without $\{y_i \mid i < a_2\}$ in $g(M_2)$. Therefore, we have $\gamma \leq b_2$ by noting $\alpha = b_1$ and this implies $\gamma = b_2$. Proceeding in the same way, we conclude that the exponents of all variables occurring in M_2 are identical to those in M, which implies that $M_2 = M$ but it is an obvious contradiction. Thus, we verify the assertion of the lemma. □

After demonstration of this Lemma 2.4, we may precisely establish the proof of Theorem 2.3 by using Lemma 2.1.

Proof of Theorem 2.3. Suppose p does not divide d. Then, it follows that $M_1 = y_{r_n}^{d-1} y_{r_n-1} N$ appears in $g(M) - M$ with non-zero coefficient. Note that arising of M_1 in $g(M) - M$ is equivalent to occurring of M_1 in $g(M)$ with $M_1 \neq M$.

By Lemma 2.1, there is a monomial M_2 different than both M, M_1 such that M_1 shows up in $g(M_2)$. Notice that M is the leading monomial so the condition $M_2 < M$ as seen in Lemma 2.4 is satisfied. However, it is a clear contradiction with Lemma 2.4. Hence, we acquire $p \mid d$. □

After managing the single indecomposable G-module V_{r_n} case, we concentrate on

$$V = V_{r_1} \oplus V_{r_2} \oplus \cdots \oplus V_{r_s}$$

the direct sum of indecomposable G-modules for the cyclic group C_{p^k} and we attain the same divisibility property as a corollary of Theorem 2.3 with a little manipulation.

Theorem 2.5. *Let $f \in F[V]^G$ and the leading monomial of f is*

$$LM_<(f) = \prod_{1 \leq j \leq s} x_{r_j,j}^{\alpha_j} N_j$$

with no $x_{r_j,j}$ in $N_j \in F[V_{r_j}]$ for positive integers α_j. Then, we show that p divides α_j for all values of j.

Proof. By giving particular attention to the projection of f onto single indecomposable G-module V_{r_j}, it may be observed that the projection of $LM_<(f)$ onto the same G-module V_{r_j} is the biggest monomial appearing in the projected version of f onto V_{r_j}. In simpler terms, the leading monomial in the projection of f onto V_{r_j} is $x_{r_j,j}^{\alpha_j} N_j$ with no $x_{r_j,j}$ in N_j.

Otherwise, it is contradictory with that $LM_<(f)$ is the leading monomial and we would also like to point out that the projection of f onto V_{r_j} lies inside the invariant ring $F[V_{r_j}]^G$.

By using this fact with the implementation of Theorem 2.3, we gain our desired result, that is

$$p \mid \alpha_j \text{ for all } 1 \leq j \leq s.$$

□

Remark 2.6. To obtain the divisibility as in Theorem 2.5 for C_{p^k} follows a similar process to getting the same divisibility for C_p because the primary workflow is coming from the single indecomposable module case. To clarify, the number of direct summands of V does not influence the proof of Theorem 2.5.

Acknowledgement. The author would like to thank the reviewers and editors of the International Electronic Journal of Algebra.

Disclosure statement. The author reports that there are no competing interests to declare.

References

[1] D. J. Benson, Polynomial Invariants of Finite Groups, London Mathematical Society Lecture Note Series, 190, Cambridge University Press, Cambridge, 1993.

[2] H. E. A. E. Campbell and D. L. Wehlau, Modular Invariant Theory, Encyclopaedia of Mathematical Sciences, 139, Invariant Theory and Algebraic Transformation Groups, 8, Springer-Verlag, Berlin, 2011.

[3] H. Derksen and G. Kemper, Computational Invariant Theory, Invariant Theory and Algebraic Transformation Groups, I, Encyclopaedia of Mathematical Sciences, 130, Springer-Verlag, Berlin, 2002.

[4] D. Eisenbud, Commutative Algebra: With a View Toward Algebraic Geometry, Graduate Texts in Mathematics, 150, Springer-Verlag, New York, 1995.

[5] J. Herzog and T. Hibi, Monomial Ideals, Graduate Texts in Mathematics, 260, Springer-Verlag London, Ltd., London, 2011.

[6] M. Kohls and M. Sezer, *Degree of reductivity of a modular representation*, Commun. Contemp. Math., 19(3) (2017), 1650023 (12 pp).

[7] L. Smith, Polynomial Invariants of Finite Groups, Research Notes in Mathematics, 6, A K Peters, Ltd., Wellesley, MA, 1995.

Bekir Danış
Digital Transformation Office
Aydın Adnan Menderes University
Central Campus, 09010, Aydın, Turkey
e-mail: bekir.danis@adu.edu.tr