THE HIT PROBLEM FOR THE MODULAR INVARIANTS OF LINEAR GROUPS

NGUYĖN H. V. HU and TRbaru0 Trần Ngoc Nam

Abstract. Let the mod 2 Steenrod algebra, $\mathcal{A}$, and the general linear group, $GL_k := GL(k, \mathbb{F}_2)$, act on $P_k := \mathbb{F}_2[x_1, \ldots, x_k]$ with $\text{deg}(x_i) = 1$ in the usual manner. We prove that, for a family of some rather small subgroups $G$ of $GL_k$, every element of positive degree in the invariant algebra $P^G_k$ is hit by $\mathcal{A}$ in $P_k$.

In other words, $(P^G_k)^+ \subset \mathcal{A}^+ \cdot P_k$, where $(P^G_k)^+$ and $\mathcal{A}^+$ denote respectively the submodules of $P_k^G$ and $\mathcal{A}$ consisting of all elements of positive degree.

This family contains most of the parabolic subgroups of $GL_k$. It should be noted that the smaller the group $G$ is the harder the problem turns out to be. Remarkably, when $G$ is the smallest group of the family, the invariant algebra $P^G_k$ is a polynomial algebra in $k$ variables, whose degrees are fixed while $k$ increases.

It has been shown in [3] that, for $G = GL_k$, the inclusion $(P^G_k)^+ \subset \mathcal{A}^+ \cdot P_k$ is equivalent to a weak algebraic version of the long-standing conjecture stating that the only spherical classes in $Q_0S^0$ are the elements of Hopf invariant one and those of Kervaire invariant one.

1. Introduction

Let $P_k := \mathbb{F}_2[x_1, \ldots, x_k]$ be the polynomial algebra over the field of two elements, $\mathbb{F}_2$, in $k$ variables $x_1, \ldots, x_k$, each of degree 1. It is equipped with the usual structure of module over $GL_k := GL(k, \mathbb{F}_2)$ by means of substitutions of variables. The mod 2 Steenrod algebra, $\mathcal{A}$, acts upon $P_k$ by use of the formula

$$Sq^j(x_i) = \begin{cases} x_i, & j = 0, \\ x_i^2, & j = 1, \\ 0, & \text{otherwise}, \end{cases}$$

and subject to the Cartan formula

$$Sq^n(fg) = \sum_{j=0}^{n} Sq^j(f) Sq^{n-j}(g),$$

for $f, g \in P_k$.

Let $G$ be a subgroup of $GL_k$. Then $P_k$ possesses the induced structure of $G$-module. Denote by $P^G_k$ the subalgebra of all $G$-invariants in $P_k$. Since the action of $GL_k$ and that of $\mathcal{A}$ on $P_k$ commute with each other, $P^G_k$ is also an $\mathcal{A}$-module.

In [3], the first named author is interested in the homomorphism

$$j_G : \mathbb{F}_2 \otimes (P^G_k) \rightarrow (\mathbb{F}_2 \otimes P_k)^G$$

1The work was supported in part by the National Research Program, No1.4.2.
22000 Mathematics Subject Classification. Primary 55S10, Secondary 55Q45
3Key words and phrases. Steenrod algebra, Invariant theory, Dickson invariant, Mui invariant.

1
induced by the identity map on $P_k$. He also sets up the following conjecture for $G = GL_k$ and shows that it is equivalent to a weak algebraic version of the long-standing conjecture stating that the only spherical classes in $Q_0S^0$ are the elements of Hopf invariant one and those of Kervaire invariant one.

Conjecture 1.1. ([3]) $j_{GL_k} = 0$ in positive degrees for $k > 2$.

This has been established for $k = 3$ in [3] and then for arbitrary $k > 2$ in [6]. That the conjecture is no longer valid for $k = 1$ and $k = 2$ is respectively shown in [3] to be an exposition of the existence of the Hopf invariant one and the Kervaire invariant one classes.

In the present paper, we are interested in the following problem: Which subgroup $G$ of $GL_k$ possesses $j_G = 0$ in positive degrees? It should be noted that, as observed in the introduction of [3],

$$j_G = 0 \text{ in positive degrees } \iff (P_k^G)^+ \subset \mathcal{A}^+ \cdot P_k,$$

where $(P_k^G)^+$ and $\mathcal{A}^+$ denote respectively the submodules of $P_k^G$ and $\mathcal{A}$ consisting of all elements of positive degree. Therefore, the smaller the group $G$ is the harder the problem turns out to be. For instance, we have understood that $j_G \neq 0$ for $G = \{1\}$, $G = GL_1$ or $G = GL_2$. Furthermore, let $T_k$ be the Sylow 2-subgroup of $GL_k$ consisting of all upper triangular matrices with entries 1 on the main diagonal.

Then $j_{T_k} \neq 0$, indeed $V_1 = x_1$ is a $T_k$-invariant, however $x_1 \notin \mathcal{A}^+ \cdot P_k$.

The problem we are interested in is closely related to the hit problem of determination of $\mathbb{F}_2 \otimes P_k$. This problem has first been studied by F. Peterson [11], R. Wood [16], W. Singer [14], and S. Priddy [12], who show its relationships to several classical problems in cobordism theory, modular representation theory, Adams spectral sequence for the stable homotopy of spheres, stable homotopy type of classifying spaces of finite groups. The tensor product $\mathbb{F}_2 \otimes P_k$ has explicitly been computed for $k \leq 3$ (see [9]). It seems unlikely that an explicit description of $\mathbb{F}_2 \otimes P_k$ for general $k$ will appear in the near future. There is also another approach, the qualitative one, to the problem. By this we mean giving conditions on elements of $P_k$ to show that they go to zero in $\mathbb{F}_2 \otimes P_k$, i.e. belong to $\mathcal{A}^+ \cdot P_k$. Peterson’s conjecture [11], which has been established by Wood [16], claims that $\mathbb{F}_2 \otimes P_k = 0$ in certain degrees. Recently, W. Singer, K. Monks, and J. Silverman have refined Wood’s method to show that many more monomials in $P_k$ are in $\mathcal{A}^+ \cdot P_k$. (See Silverman [13] and references therein.)

In this paper, we prove that $j_G = 0$ in positive degrees, or equivalently $(P_k^G)^+ \subset \mathcal{A}^+ \cdot P_k$, for a family of some rather small groups $G$. This family contains most of the parabolic subgroups of $GL_k$.

Observing the obstructions of the Hopf invariant one and the Kervaire invariant one classes, it seems necessary to make the hypothesis that $G \supset GL_3$ in order to get $j_G = 0$ in positive degrees. Let us consider the subgroup

$$G_1 \cdot G_2 := \{ \begin{pmatrix} A & * \\ 0 & B \end{pmatrix} \mid A \in G_1, B \in G_2 \} \subset GL_k,$$

where $G_1$ is a subgroup of $GL_n$ and $G_2$ is a subgroup of $GL_{k-n}$ for $n \leq k$. We are especially interested in the case $G_1 = GL_n$ and $G_2 = 1_{k-n}$, the unit subgroup of $GL_{k-n}$. We suppose $n > 2$ so that $GL_3 \subset GL_n \cdot 1_{k-n}$. Here is an interpretation of
Theorem 1.3. Theorem 1.2. Theorem 1.2.

where deg \( n > 1 \) is the smallest group among all the ones of the form \( GL_n \cdot 1_{k-n} \) for \( n > 2 \). Being applied to this group, the main theorem shows that

\[
\mathbb{F}_2[Q_{3,0}, Q_{3,1}, Q_{3,2}, V_4(x_4), ..., V_4(x_k)]^+ \subset \mathcal{A}^+ \cdot P_k,
\]

where \( \deg Q_{3,0} = 7, \deg Q_{3,1} = 6, \deg Q_{3,2} = 4, \deg V_4(x_i) = 8 \) for \( 3 < i \leq k \). This gives a large family of elements, which are hit by \( \mathcal{A} \) in \( P_k \). Remarkably, the degrees of all the generators of this polynomial algebra are small and do not depend on \( k \).

Let us now study the parabolic subgroup of \( GL_k \):

\[
GL_{k_1, \ldots, k_m} = \left\{ \begin{pmatrix} A_1 & & * \\ & A_2 & \\ & & \ddots \\ 0 & & A_m \end{pmatrix} \mid A_i \in GL_{k_i} \text{ with } k_1 + \cdots + k_m = k \right\}.
\]

It is easily seen that \( GL_{k_1} \cdot 1_{k-k_1} \) is a subgroup of \( GL_{k_1, \ldots, k_m} \). Therefore, we have

Corollary 1.4. \( j_{GL_{k_1, \ldots, k_m}} = 0 \) in positive degrees if and only if \( k_1 > 2 \).
Let $G$ be a subgroup of $GL_k$ and $\omega \in GL_k$. It is easily seen that $P_k^G \omega^{-1} = \omega P_k^G$. As the action of $GL_k$ on $P_k$ commutes with that of $A$. Theorem 1.3 and Corollary 1.4 also claim that $j_G = 0$ for any subgroup $G$, which is conjugate either to $GL_n \bullet 1_{k-n}$ with $n > 2$ or to $GL_{k_1, \ldots, k_m}$ with $k_1 > 2$.

Note that $GL_k$ is a special case of the parabolic subgroup $GL_{k_1, \ldots, k_m}$ with $k = k_1$ and $m = 1$. Hence we obtain an alternative proof for Conjecture 1.1:

**Corollary 1.5.** ([6]) $j_{GL_k} = 0$ in positive degrees if and only if $k > 2$.

The readers are referred to [4] and [5] for some problems, which are related to the main theorem and Corollary 1.5. Additionally, the problem of determination of $\mathbb{F}_2 \otimes (P^G_k)$ and its applications have been studied by Huynh - Peterson [7], [8].

The paper contains 5 sections and is organized as follows. We determine the algebra of $GL_n \bullet 1_{k-n}$-invariants in Section 2 and study the action of $A$ on this algebra for $n = 3$ in Section 3. The main theorem and its corollaries are proved in Section 4 assuming the truth of Lemma 4.2 as a key tool. Finally, we show this lemma in Section 5 and then complete the proof of the main theorem.

## 2. The Invariant Algebra of $GL_n \bullet 1_{k-n}$

The action of $GL_k$ on $P_k = \mathbb{F}_2[x_1, \ldots, x_k]$ is precisely described as follows. For every $\omega = (\omega_{ij})_{k \times k} \in GL_k$ and any $f \in P_k$, one defines

$$(\omega f)(x_1, \ldots, x_k) = f(\omega x_1, \ldots, \omega x_k),$$

where $\omega x_1, \ldots, \omega x_k$ are given by

$$\omega x_j = \sum_{1 \leq i \leq k} \omega_{ij} x_i \quad (1 \leq j \leq k).$$

Then, each subgroup $G$ of $GL_k$ possesses the induced action on $P_k$.

Using the notations given in the introduction, we get the following theorem, which is also numbered as Theorem 1.2.

**Theorem 2.1.** For $k \geq n$,

$$\mathbb{F}_2[x_1, \ldots, x_k]^{GL_n \bullet 1_{k-n}} = \mathbb{F}_2[Q_{n,0}, \ldots, Q_{n,n-1}, V_{n+1}(x_{n+1}), \ldots, V_{n+1}(x_k)].$$

We prove this theorem by three lemmata.

**Lemma 2.2.** The polynomials $Q_{n,0}, \ldots, Q_{n,n-1}, V_{n+1}(x_{n+1}), \ldots, V_{n+1}(x_k)$ are $GL_n \bullet 1_{k-n}$-invariants.

**Proof.** The polynomials $Q_{n,0}, \ldots, Q_{n,n-1}$ depend only on $x_1, \ldots, x_n$ but not on $x_{n+1}, \ldots, x_k$. On the other hand, the action of $A$ on $x_1, \ldots, x_n$, where $E_{k-n}$ denotes the unit $(k-n) \times (k-n)$-matrix, is exactly the same as that of $A \in GL_n$. Therefore, according to Dickson [1], $Q_{n,0}, \ldots, Q_{n,n-1}$ are $GL_n \bullet 1_{k-n}$-invariants.

Note that $V_{n+1}(x_i)$ can be re-written as follows

$$V_{n+1}(x_i) = \prod_{x \in V_n} (x + x_i) \quad (n < i \leq k),$$
where $V_n$ denotes the $F_2$-vector space spanned by $x_1, \ldots, x_n$. For a given matrix $\omega \in GL_n \cdot 1_{k-n}$, setting $a := \omega_1 x_1 + \cdots + \omega_n x_n$ and we get
\[
\omega x_i = (\omega_1 x_1 + \cdots + \omega_n x_n) + x_i = a + x_i \quad (n < i \leq k).
\]
Obviously, the map $\omega |_{V_n} : V_n \to V_n$ is bijective. Then, so is the map $V_n \to V_n$, which brings $x$ to $y = \omega x + a$. Thus, we obtain
\[
\omega V_{n+1}(x_i) = \prod_{x \in V_n} (\omega x + \omega x_i) = \prod_{x \in V_n} (\omega x + a + x_i) = \prod_{y \in V_n} (y + x_i) = V_{n+1}(x_i),
\]
for $n < i \leq k$. This means $V_{n+1}(x_{n+1}), \ldots, V_{n+1}(x_k)$ are $GL_n \cdot 1_{k-n}$-invariants. The lemma is proved. \hfill $\Box$

**Lemma 2.3.** The polynomials $Q_{n,0}, \ldots, Q_{n,n-1}, V_{n+1}(x_{n+1}), \ldots, V_{n+1}(x_k)$ are algebraically independent.

**Proof.** The lemma is shown by induction on $k \geq n$.

For $k = n$, from Dickson [1], $Q_{n,0}, \ldots, Q_{n,n-1}$ are algebraically independent. Suppose inductively that the lemma holds for $k-1 \geq n$. Assume that we are given an algebraic identity
\[
f(Q_{n,0}, \ldots, Q_{n,n-1}, V_{n+1}(x_{n+1}), \ldots, V_{n+1}(x_k)) = 0,
\]
where $f$ is a polynomial in the indicated variables. We think of $f$ as a polynomial in the variable $V_{n+1}(x_k)$:
\[
f = \sum_{j=0}^{q} f_j(Q_{n,0}, \ldots, Q_{n,n-1}, V_{n+1}(x_{n+1}), \ldots, V_{n+1}(x_{k-1})) V_{n+1}^j(x_k).
\]
Recall that $Q_{n,0}, \ldots, Q_{n,n-1}, V_{n+1}(x_{n+1}), \ldots, V_{n+1}(x_{k-1})$ do not depend on $x_k$, while $V_{n+1}(x_k)$ is a polynomial of degree $2^n$ in $x_k$. Now we consider $f$ to be a polynomial in $x_k$. Its leading coefficient, which corresponds to the monomial $x_k^{2^n}$, is nothing but $f_q(Q_{n,0}, \ldots, Q_{n,n-1}, V_{n+1}(x_{n+1}), \ldots, V_{n+1}(x_{k-1}))$. Thus, by the algebraic independence of $x_1, \ldots, x_k$, we get
\[
f_q(Q_{n,0}, \ldots, Q_{n,n-1}, V_{n+1}(x_{n+1}), \ldots, V_{n+1}(x_{k-1})) = 0.
\]
Iteratedly, consider the coefficients of the monomials $x_k^{2^n(j-1)}, \ldots, x_k^{2^n \cdot 0}$ and we have
\[
f_j(Q_{n,0}, \ldots, Q_{n,n-1}, V_{n+1}(x_{n+1}), \ldots, V_{n+1}(x_{k-1})) = 0 \quad (0 \leq j \leq q).
\]
Hence, applying the inductive hypothesis to $f_0, \ldots, f_q$, we conclude that they all are the zero polynomial. Therefore, so is $f$.

The lemma is proved. \hfill $\Box$

**Lemma 2.4.** Every $GL_n \cdot 1_{k-n}$-invariant polynomial $g(x_1, \ldots, x_k)$ is a polynomial in the variables $Q_{n,0}, \ldots, Q_{n,n-1}, V_{n+1}(x_{n+1}), \ldots, V_{n+1}(x_k)$.

**Proof.** The lemma is also proved by induction on $k \geq n$.

For $k = n$, it is due to Dickson [1]. Suppose inductively that the lemma is true for $k-1 \geq n$. We start by an observation, which is actually due to H. Müi [10],
claiming that if a $GL_n \bullet 1_{k-n}$-invariant polynomial admits $x_k$ as a factor, then it also admits $V_{n+1}(x_k)$ as a factor.

Let $g_0$ be the sum of all monomials in $g$ which are not divisible by $x_k$. Then $g - g_0$ has $x_k$ as a factor and therefore admits $V_{n+1}(x_k)$ as a factor. Suppose

$$g - g_0 = g'V_{n+1}^p(x_k),$$

where $g'$ is not divisible by $x_k$. Since $g_0$ does not depend on $x_k$, it is a $GL_n \bullet 1_{k-1-n}$-invariant in $\mathbb{F}_2[x_1, \ldots, x_{k-1}]$. By means of the inductive hypothesis, $g_0$ is a polynomial in $Q_{n, 0}, \ldots, Q_{n, n-1}, V_{n+1}(x_{n+1}), \ldots, V_{n+1}(x_{k-1})$.

Denote by $\text{deg}_{x_k} g$ the degree of $g$ regarded as a polynomial in $x_k$. It is clear that $\text{deg}_{x_k} g' < \text{deg}_{x_k} g$. By downward induction on $\text{deg}_{x_k} g'$ and using the above argument we can show that $g'$ is a polynomial in $Q_{n, 0}, \ldots, Q_{n, n-1}, V_{n+1}(x_{n+1}), \ldots, V_{n+1}(x_k)$.

As a consequence, $g = g_0 + g'V_{n+1}^p(x_k)$ is a polynomial in $Q_{n, 0}, \ldots, Q_{n, n-1}, V_{n+1}(x_{n+1}), \ldots, V_{n+1}(x_k)$. The lemma follows.

Combining Lemmata 2.2, 2.3 and 2.4, Theorem 2.1 is completely proved.

3. THE $A$-ACTION ON $GL_3 \bullet 1_{k-3}$-INVARANTS

From now on, we set $H = GL_3 \bullet 1_{k-3}$ for $k \geq 3$. The fundamental $H$-invariants $Q_{3, 0}, Q_{3, 1}, Q_{3, 2}, V_4(x_4), \ldots, V_4(x_k)$ will respectively be denoted by $Q_0, Q_1, Q_2, W_4, \ldots, W_k$ for brevity. Then, by Theorem 1.2, we get

$$P_k^H = \mathbb{F}_2[Q_0, Q_1, Q_2, W_4, \ldots, W_k],$$

with $\text{deg} Q_0 = 7, \text{deg} Q_1 = 6, \text{deg} Q_2 = 4, \text{deg} W_4 = \cdots = \text{deg} W_k = 8$. The action of $A$ on $P_k^H$ is given by the following formulas, which are special cases of the ones in Hrgn [2].

**Proposition 3.1.** ([2]) The only non-zero $Sq^i X$’s, where $X$ is one of the invariants $Q_0, Q_1, Q_2, W_4, \ldots, W_k$, are:

(i) $Sq^0 Q_0 = Q_0, Sq^2 Q_0 = Q_0 Q_2, Sq^6 Q_0 = Q_0 Q_1, Sq^7 Q_0 = Q_0^2, Sq^1 Q_1 = Q_1, Sq^3 Q_1 = Q_0, Sq^5 Q_1 = Q_0 Q_2, Sq^6 Q_1 = Q_1^2, Sq^2 Q_2 = Q_2, Sq^4 Q_2 = Q_1, Sq^7 Q_2 = Q_0, Sq^4 Q_2 = Q_2^2, Sq^6 W_r = W_r, Sq^4 W_r = Q_2 W_r, Sq^5 W_r = Q_1 W_r, Sq^6 W_r = Q_0 W_r, Sq^3 W_r = W_r^2 \quad (4 \leq r \leq k)$.  

(ii) $Sq^0 Q_0 = Q_0, Sq^2 Q_0 = Q_0 Q_2, Sq^6 Q_0 = Q_0 Q_1, Sq^7 Q_0 = Q_0^2, Sq^1 Q_1 = Q_1, Sq^3 Q_1 = Q_0, Sq^5 Q_1 = Q_0 Q_2, Sq^6 Q_1 = Q_1^2, Sq^2 Q_2 = Q_2, Sq^4 Q_2 = Q_1, Sq^7 Q_2 = Q_0, Sq^4 Q_2 = Q_2^2, Sq^6 W_r = W_r, Sq^4 W_r = Q_2 W_r, Sq^5 W_r = Q_1 W_r, Sq^6 W_r = Q_0 W_r, Sq^3 W_r = W_r^2 \quad (4 \leq r \leq k)$.  

**Definition 3.2.** Each monomial in the variables $Q_0, Q_1, Q_2, W_4, \ldots, W_k$ of $P_k^H$ is called an $H$-monomial. Given an $H$-monomial $R$, let $i_0(R), i_1(R), i_2(R), i_4(R), \ldots, i_k(R)$ be respectively the powers of $Q_0, Q_1, Q_2, W_4, \ldots, W_k$ in $R$. Set

$$h(R) := i_0(R) + i_1(R) + i_2(R) + i_4(R) + \cdots + i_k(R).$$

Let $s(R)$ denote the minimal non-negative integer with $2^{s(R)}$ missing in the dyadic expansion of $i_2(R)$.

**Lemma 3.3.** Let $R \in P_k^H$ be an $H$-monomial and $i$ a non-negative integer.

(i) If $h(R) = 1$, then

$$Sq^{4i}(R) = RQ_2^4 + \sum S,$

where each term $S$ is an $H$-monomial with $i_2(S) < i_2(R) + i$. 

Proof. (i) According to Proposition 3.1, if \( X \) is one of the fundamental \( H \)-invariants \( Q_0, Q_1, Q_2, W_4, \ldots, W_k \), then

\[ Sq^4 X = XQ_2. \]

Hence, using the Cartan formula, we get

\[ Sq^{4i}(R) = \binom{h(R)}{i} RQ_2^i + \sum S, \]

where each term \( S \) is an \( H \)-monomial with \( i_2(S) < i_2(R) + i \).

(ii) We write \( R = R_1 \ldots R_h \), where \( h = h(R) \) and \( R_p \) is one of the fundamental \( H \)-invariants \( Q_0, Q_1, Q_2, W_4, \ldots, W_k \), for \( 1 \leq p \leq h \). Using again the Cartan formula and Proposition 3.1, we have

\[ Sq^i(R) = \sum_{j_1 + \cdots + j_h = i} Sq^{j_1}(R_1) \cdots Sq^{j_h}(R_h) \]

\[ = \sum_{h(S)=h(R)} S + \sum_{h(T)>h(R)} T. \]

As \( deg \ Q_2 = 4 \) is the smallest number of the degrees of \( Q_0, Q_1, Q_2, W_4, \ldots, W_k \), the degree information shows that

\[ h(R) < h(T) \leq h(R) + i/4, \]

for every \( T \) in the sum.

Consider an arbitrary term \( S = Sq^{j_1}(R_1) \cdots Sq^{j_h}(R_h) \) in the sum. As \( h(S) = h(R) \), we can see that \( j_p = 0 \) for every \( p \) with \( R_p \) being one of the invariants \( Q_0, W_4, \ldots, W_k \). Suppose the contrary that \( i_2(S) \geq i_2(R) \). (Then, we have actually \( i_2(S) = i_2(R) \) because of \( h(S) = h(R) \).) By Proposition 3.1, \( j_p = 0 \) for every \( p \) with \( R_p = Q_2 \). So, \( j_p \) could be non-zero just only in the case \( R_p = Q_1 \). Furthermore, as \( h(S) = h(R) \) and by Proposition 3.1, if \( j_p \neq 0 \) then \( j_p = 1 \). Therefore,

\[ i = j_1 + \cdots + j_h \leq i_2(R). \]

This contradicts to the hypothesis that \( i > i_1(R) \).

The lemma is proved. \( \square \)

**Lemma 3.4.** Suppose \( R \) is an \( H \)-monomial in \( P_k \) and \( n \) is a non-negative integer such that \( i_2(R) \equiv 2^n - 1 \) (mod \( 2^n \)) and \( \left( \frac{h(R)}{2^{n-1}} \right) = 0 \). Then

\[ R = Sq^{2^{n+1}}(\overline{R}Q_2^{i_2(R) - 2^{n-1}}) + \sum S, \]

where \( \overline{R} := R/Q_2^{i_2(R)} \) and each term \( S \) in the sum is an \( H \)-monomial with \( s(S) < n \).
Proof. We have
\[ h(R) = h(\overline{R}Q_2^{i_2(R)}) = h(R) + i_2(R) \equiv h(R) + 2^n - 1 \pmod{2^n}. \]

Hence \( h(R) + 2^n - 1 \equiv h(R) - 2^{n-1} \pmod{2^n} \). As \( \left( \frac{h(R)}{2^{n-1}} \right) = 0 \), the term \( 2^{n-1} \) occurs in the 2-adic expansion of \( h(R) - 2^{n-1} \). Thus
\[
\left( \frac{h(\overline{R}Q_2^{2^{n-1}-1})}{2^{n-1}} \right) = \left( \frac{h(R) + 2^{n-1} - 1}{2^{n-1}} \right) = \left( \frac{h(R) - 2^{n-1}}{2^{n-1}} \right) = 1.
\]

Applying Lemma 3.3 (i) to \( \overline{R}Q_2^{2^{n-1}-1} \) and \( i = 2^{n-1} \), we get
\[ Sq^{2^{n+1}}(\overline{R}Q_2^{2^{n-1}-1}) = \overline{R}Q_2^{2^{n-1}} + \sum S', \]
where each \( S' \) is an \( H \)-monomial in \( P_k^H \) satisfying
\[ i_2(S') < i_2(\overline{R}Q_2^{2^{n-1}-1}) + 2^{n-1} = 2^n - 1. \]

This inequality implies \( s(S') < n \).

Put \( a := i_2(R) - (2^n - 1) \equiv 0 \pmod{2^n} \). By the Cartan formula and Proposition 3.1, we have
\[
Sq^{2^{n+1}}(\overline{R}Q_2^{i_2(R)-2^{n-1}}) = Sq^{2^{n+1}}(\overline{R}Q_2^{2^{n-1}-1}Q_2^a)
\]
\[ = Sq^{2^{n+1}}(\overline{R}Q_2^{2^{n-1}-1})Q_2^a + \overline{R}Q_2^{2^{n-1}-1}Sq^{2^{n+1}}(Q_2^a)
\]
\[ = (\overline{R}Q_2^{2^{n-1}} + \sum S')Q_2^a + \overline{R}Q_2^{2^{n-1}-1}Sq^{2^{n+1}}(Q_2^a)
\]
\[ = R + \sum S'Q_2^a + \overline{R}Q_2^{2^{n-1}-1}Sq^{2^{n+1}}(Q_2^a),
\]
where each term \( S'Q_2^a \) in the sum satisfies \( s(S'Q_2^a) < n \), because \( s(S') < n \) and \( a \equiv 0 \pmod{2^n} \). On the other hand, from Proposition 3.1, if \( Sq^{2^{n+1}}(Q_2^a) \neq 0 \) then it is not divisible by \( Q_2 \). Therefore
\[ s(\overline{R}Q_2^{2^{n-1}}Sq^{2^{n+1}}(Q_2^a)) = s(Q_2^{2^{n-1}-1}) = n - 1. \]

To sum up, we can write
\[ R = Sq^{2^{n+1}}(\overline{R}Q_2^{i_2(R)-2^{n-1}}) + \sum S,
\]
where each term \( S \) satisfies \( s(S) < n \).

The lemma is proved. \( \square \)

**Lemma 3.5.** Suppose \( R \) is an \( H \)-monomial in \( P_k^H \), which is not divisible by \( Q_2 \), while \( n \) and \( i \) are positive integers satisfying
\[ h(R) \equiv 0 \pmod{2^n}, \quad i_1(R) \leq 2^n - 1, \quad 2^n \leq i \leq 2^{n+1}. \]

Then
\[ Sq^i(\overline{R}Q_2^{2^n-1}) = \sum S + \sum T,
\]
where each term \( S \) is an \( H \)-monomial in \( P_k^H \) with \( s(S) < n \), while each term \( T \) is an \( H \)-monomial in \( P_k^H \) with \( i_2(T) \equiv 2^n - 1 \pmod{2^n} \) and \( \left( \frac{h(T)}{2^{n-1}} \right) = 0. \)
Proof. Note that \( i \geq 2^n > 2^n - 1 \geq i_1(R) = i_1(RQ_2^{2^n-1}) \). Applying Lemma 3.3 (ii) to \( RQ_2^{2^n-1} \) and \( i \), we get

\[
Sq^i(RQ_2^{2^n-1}) = \sum S + \sum T,
\]

where each \( S \) is an \( H \)-monomial with \( i_2(S) < i_2(RQ_2^{2^n-1}) = 2^n - 1 \), while each \( T \) is an \( H \)-monomial with

\[
h(RQ_2^{2^n-1}) < h(T) \leq h(RQ_2^{2^n-1}) + i/4.
\]

For each \( S \) in the sum, as \( i_2(S) < 2^n - 1 \), it implies \( s(S) < n \). For each \( T \) in the sum, we have

\[
h(RQ_2^{2^n-1}) = h(R) + 2^n - 1 < h(T) \leq h(R) + 2^n - 1 + i/4 \\
\leq h(R) + 2^n + (2^n - 1 - 1).
\]

Hence \( h(R) + 2^n \leq h(T) \leq h(R) + 2^n + (2^n - 1) \). Combining these inequalities with the hypothesis \( h(R) \equiv 0 \) (mod \( 2^n \)), we obtain \( \left( \frac{h(T)}{2^n-1} \right) = 0 \).

Finally, suppose \( i_2(T) = (2^n - 1) + b \), where \( b \) is an integer (that can be positive, negative or zero). If \( b \equiv 0 \) (mod \( 2^n \)) then \( i_2(T) \equiv 2^n - 1 \) (mod \( 2^n \)). Otherwise, if \( b \neq 0 \) (mod \( 2^n \)), then \( s(T) < n \) and such a \( T \) can be considered as a term in the sum \( \sum S \). The lemma is proved. \( \square \)

4. Proofs of the main theorem and its corollaries

The following two lemmata will play a key role in the proof of the main theorem.

**Lemma 4.1.** Let \( R \neq 1 \) be a product of some distinct elements in the set \( \{Q_0, Q_1, Q_2, W_4, \ldots, W_k\} \). Then \( R \in Sq^1P_k + Sq^2P_k \).

**Proof.** We write \( R = RS \) with \( R \mid Q_1Q_2 \) and \( S \mid Q_0W_4\cdots W_k \).

If \( Q_1 \not\mid R \), then from Proposition 3.1, \( Sq^1(R) = Sq^1(RS) = 0 \). Hence, by [6, Lemma 2.5], \( R \in Sq^1P_k \).

If \( R = Q_1 \), then by Proposition 3.1,

\[
R = Q_1S = Sq^2(Q_2)S = Sq^2(Q_2S) \in Sq^2P_k.
\]

Finally, if \( R = Q_1Q_2 \), then by [6, Lemma B], we have \( Q_1Q_2 = Sq^1u_1 + Sq^2u_2 \) for some elements \( u_1, u_2 \in P_k \). Then

\[
R = Q_1Q_2S = (Sq^1u_1 + Sq^2u_2)S = Sq^1(u_1S) + Sq^2(u_2S) \in Sq^1P_k + Sq^2P_k.
\]

The lemma follows. \( \square \)

We postpone the proof of the next lemma until the last section.

**Lemma 4.2.** Suppose \( R \) is an \( H \)-monomial in \( P_k^H \), \( u \neq 1 \) is an arbitrary element in \( P_k \) and \( n \) is a positive integer.

(i) If \( s(R) < n \), then \( Ru^2 \in A^+ \cdot P_k \).

(ii) If \( i_2(R) \equiv 2^n - 1 \) (mod \( 2^n \)) and \( \left( \frac{h(R)}{2^n-1} \right) = 0 \), then \( Ru^2 \in A^+ \cdot P_k \).

(iii) If \( i_2(R) = 2^n - 1 \geq i_3(R) \), \( h(R) \equiv 2^n - 1 \) (mod \( 2^n \)) and \( u \in Sq^1P_k + Sq^2P_k \), then \( Ru^2 \in A^+ \cdot P_k \).
Proof of the main theorem.
It suffices to show the theorem for the group $H = GL_3 \cdot 1_{k-3}$, as this is the smallest one of the groups $GL_n \cdot 1_{k-n}$ for $n > 2$. Moreover, using Theorem 1.2, we need only to prove that
\[(P_k^H)^+ = F_2[Q_0, Q_1, Q_2, W_1, \ldots, W_k]^+ \subset A^+ \cdot P_k\]
for every $k > 2$.

Suppose $R$ is an $H$-monomial of positive degree in $P_k^H$. We need to show that $R \in A^+ \cdot P_k$. Let $n := s(S)$. Then, by definition, $i_2(R) \equiv 2^n - 1 \pmod{2^{n+1}}$.

Let us consider the following four cases.

Case 1: $Q_2^2$ divides $R$.
Combining this with the hypothesis $i_2(R) \equiv 2^n - 1 \pmod{2^{n+1}}$, it implies $Q_2^2$ dividing $R$. Denoting $\overline{R} := R/Q_2^2$, we have $i_2(\overline{R}) = i_2(R) - 2^{n+1} \equiv 2^n - 1 \pmod{2^{n+1}}$. Thus $s(\overline{R}) = n < n + 1$. Applying Lemma 4.2 (i) to the triple $(\overline{R}, Q_2, n + 1)$, we get $R = \overline{R}Q_2^{n+1} \in A^+ \cdot P_k$.

Case 2: There exists $u \in \{Q_0, Q_1, W_4, \ldots, W_k\}$ such that $u^{2^{n+1}}$ divides $R$.
Setting $\overline{R} := R/u^{2^{n+1}}$, we have $s(\overline{R}) = s(R) = n < n + 1$. Applying Lemma 4.2 (i) to the triple $(\overline{R}, u, n + 1)$, we get $R = \overline{R}u^{2^{n+1}} \in A^+ \cdot P_k$.

Case 3: $i_0(R)$, $i_1(R)$, $i_2(R)$, $i_4(R)$, \ldots, $i_k(R)$ all are $\leq 2^{n+1} - 1$ and there exists $u \in \{Q_0, Q_1, Q_2, W_4, \ldots, W_k\}$ such that $u^{2^n}$ divides $R$.
By Case 1, $u \not\equiv Q_2$. Furthermore, since $i_2(R) \leq 2^{n+1} - 1$ and $i_2(R) \equiv 2^n - 1 \pmod{2^{n+1}}$, it implies $i_2(R) = 2^n - 1$.
We investigate the following three sub-cases.

Case 3a: $n = 0$. Then, by Lemma 4.1, $R \in Sq^1P_k + Sq^2P_k$.

Case 3b: $n \geq 1$ and there exists $m$ with $0 < m \leq n$ and $\left( \frac{h(R)}{2^{m-1}} \right) = 0$. Obviously $i_2(R) \equiv 2^m - 1 \pmod{2^m}$. Put $\overline{R} := R/u^{2^m}$ and we have $\left( \frac{h(\overline{R})}{2^{m-1}} \right) = 0$. Applying Lemma 4.2 (ii) to the triple $(\overline{R}, u, m)$, we get $R = \overline{R}u^{2^m} \in A^+ \cdot P_k$.

Case 3c: $n \geq 1$ and $\left( \frac{h(R)}{2^{m-1}} \right) = 1$ for every $m$ with $0 < m \leq n$. It implies $h(R) \equiv 2^n - 1 \pmod{2^n}$. We write uniquely $R$ in the form $R = \overline{R}v^{2^n}$, where $v \neq 1$ is a certain product of distinct elements in the set $\{Q_0, Q_1, W_4, \ldots, W_k\}$ (consequently, $i_2(v) = 0$), and $\overline{R}$ is a certain $H$-monomial with $i_0(\overline{R})$, $i_1(\overline{R})$, $i_2(\overline{R})$, $i_4(\overline{R})$, \ldots, $i_k(\overline{R})$ all $\leq 2^n - 1$. Observe that
\[
i_2(\overline{R}) = i_2(R) - 2^n i_2(v) = 2^n - 1 \geq i_1(\overline{R}),
\]
\[
h(\overline{R}) = h(R) - 2^n h(v) \equiv 2^n - 1 \pmod{2^n}.
\]
By Lemma 4.1, $v \in Sq^1P_k + Sq^2P_k$. Applying Lemma 4.2 (iii) to the triple $(\overline{R}, v, n)$, we get $R = \overline{R}v^{2^n} \in A^+ \cdot P_k$.

Case 4: $i_0(R)$, $i_1(R)$, $i_2(R)$, $i_4(R)$, \ldots, $i_k(R)$ all are $\leq 2^n - 1$. 


In particular, \(i_2(R) = 2^n - 1\), since \(i_2(R) \equiv 2^n - 1 \pmod{2^{n+1}}\). It should be noted that \(n > 0\), otherwise \(R = 1\) with degree 0. We also examine the following three sub-cases.

**Case 4a**: \(n = 1\). Then, by Lemma 4.1, \(R \in Sq^1 P_k + Sq^2 P_k\).

**Case 4b**: \(n \geq 2\) and there exists \(m\) with \(0 < m < n\) and \(\left(\begin{array}{c} h(R) \\ 2^{m-1} \end{array}\right) = 0\). It is obvious that \(i_2(R) \equiv 2^m - 1 \pmod{2^m}\). Put \(\overline{R} := R/Q_2^m\) and we have

\[
\left(\begin{array}{c} h(\overline{R}) \\ 2^{m-1} \end{array}\right) = \left(\begin{array}{c} h(R) - 2^m \\ 2^{m-1} \end{array}\right) = \left(\begin{array}{c} h(R) \\ 2^{m-1} \end{array}\right) = 0.
\]

Applying Lemma 4.2 (ii) to the triple \((\overline{R}, Q_2, m)\), we get \(R = \overline{R}Q_2^m \in \mathcal{A}^+ \cdot P_k\).

**Case 4c**: \(n \geq 2\) and \(\left(\begin{array}{c} h(R) \\ 2^{m-1} \end{array}\right) = 1\) for every \(m\) with \(0 < m < n\). It implies \(h(R) \equiv 2^{n-1} - 1 \pmod{2^{n-1}}\). Write uniquely \(R\) in the form \(R = \overline{R}u^{2^{n-1}}\), where \(u \neq 1\) is a certain product of distinct elements in the set \(\{Q_0, Q_1, Q_2, W_4, \ldots, W_k\}\) with \(i_2(u) = 1\), and \(\overline{R}\) is a certain \(H\)-monomial with \(i_2(\overline{R})\) for \(k = 1\), \(i_2(\overline{R})\), \(i_4(\overline{R})\), \ldots, \(i_k(\overline{R})\) all \(\leq 2^{n-1} - 1\). Note that

\[
i_2(\overline{R}) = i_2(R) - 2^{n-1}i_2(u) = 2^n - 1 - 2^{n-1} = 2^{n-1} - 1 \geq i_1(\overline{R}),
\]

\[
h(\overline{R}) = h(R) - 2^{n-1}h(u) = 2^{n-1} - 1 \pmod{2^{n-1}}.
\]

By Lemma 4.1, we have \(u \in Sq^1 P_k + Sq^2 P_k\). Applying Lemma 4.2 (iii) to the triple \((\overline{R}, u, n - 1)\), we obtain \(R = \overline{R}u^{2^{n-1}} \in \mathcal{A}^+ \cdot P_k\).

The main theorem is completely proved. \(\square\)

**Proof of Corollary 1.4.** Note that \(GL_{k_1 \cdot 1_{k-1}}\) is a subgroup of \(GL_{k_1 \ldots k_m}\). So, by the main theorem, we have

\[
(P_k^{GL_{k_1 \ldots k_m}})^+ \subset (P_k^{GL_{k_1 \cdot 1_{k-1}}})^+ \subset \mathcal{A}^+ \cdot P_k,
\]

for \(k_1 > 2\).

If \(k_1 = 1\), then it is easily seen that

\[
Q_{1,0} \in (F_2[x_1]^{GL_1})^+ \subset (P_k^{GL_{k_1 \ldots k_m}})^+.
\]

However, \(Q_{1,0} = x_1 \notin \mathcal{A}^+ \cdot P_k\).

Finally, if \(k_1 = 2\), then we observe that

\[
Q_{2,1} \in (F_2[x_1, x_2]^{GL_2})^+ \subset (P_k^{GL_{k_1 \ldots k_m}})^+,
\]

while \(Q_{2,1} = x_1^2 + x_2^2 + x_1x_2 \notin \mathcal{A}^+ \cdot P_k\).

The corollary is proved. \(\square\)

Since the general linear group \(GL_k\) is a special case of the parabolic subgroup \(GL_{k_1 \ldots k_m}\) with \(k = k_1\) and \(m = 1\), Corollary 1.5 follows.

### 5. Proof of Lemma 4.2

The lemma is proved by induction. Its starting case is handled by the following lemma.

**Lemma 5.1.** Suppose \(R\) is an \(H\)-monomial in \(P_k^H\) with \(s(R) = 0\), and \(u \neq 1\) is an arbitrary element in \(P_k\). Then

\[
Ru^2 \in Sq^1 P_k + Sq^2 P_k.
\]
Proof. We consider the following two cases.

Case 1: $i_1(R) \equiv 0 \pmod{2}$.

By Proposition 3.1, we have

$$S(q^1Ru^2) = Sq^1(R)u^2 = 0.$$ 

So, using [6, Lemma 2.5], we get

$$Ru^2 \in Sq^1P_k.$$ 

Case 2: $i_1(R) \equiv 1 \pmod{2}$.

Put $S = R/Q_1Q_2^0$ with $i_2 = i_2(R)$. Since $s(R) = 0$, the number $i_2$ is even. Then we have

$$Ru^2 = (SQ_1^2u^2)Q_1 = (SQ_1^2u^2)Sq^2(Q_2) = Sq^2(SQ_2^2u^2Q_2) + Sq^2(SQ_2^2u^2)Q_2 = Sq^2(SQ_2^2u^2Q_2) + Sq^2(SQ_2^2u^2)Q_2.$$ 

It is easy to see that $Sq^2(Su^2) = Sq^2(Su^2)Q_2 + S(Sq^1u^2).$ Combining this with the fact $i_1(S) = i_1(Sq^2S) \equiv 0 \pmod{2}$, we obtain $Sq^1(Sq^2(Su^2)) = 0$. Then, by [6, Lemma 2.5], this gives $Sq^2(Su^2) = Sq^1v$ for some $v \in P_k$. Therefore

$$Sq^2(Su^2)Q_2^0 = Sq^1vQ_2^0 = Sq^1(vQ_2^0).$$ 

So, in any case, we have $Ru^2 \in Sq^1P_k + Sq^2P_k$.

The lemma is proved. $\square$

Proof of Lemma 4.2. The proof is divided into three steps.

Step 1: If 4.2 (i) and 4.2 (ii) are valid for every $n \leq N$, then so is 4.2 (iii) for every $n \leq N$.

Suppose $u = Sq^1v_1 + Sq^2v_2$ for some $v_1, v_2 \in P_k$. We have

$$Ru^2 = R(Sq^1v_1 + Sq^2v_2)^2 = R(Sq^1v_1)^2 + R(Sq^2v_2)^2 = Sq^2(Rv_1^2 + Sq^2(Rv_1^2)) + Sq^2(Rv_2^2) + Sq^2(Rv_2^2).$$

Therefore

$$Sq^2(Rv_1^2 + Sq^2(Rv_1^2)) + Sq^2(Rv_2^2) + Sq^2(Rv_2^2) = Sq^2(Rv_1^2) + Sq^2(Rv_2^2) + Sq^2(Rv_2^2).$$

Note that

$$Sq^2(Rv_1^2) = Sq^2[R(Sq^1v_2)^2] + R(Sq^1v_2)^2 = Sq^2[R(Sq^1v_2)^2],$$

Thus

$$Ru^2 + Sq^2(Rv_1^2 + Sq^2(Rv_2^2)) = (as Sq^1v_1 = 0).$$

Set $\overline{R} = R/Q_2^0$. Obviously, $\overline{R}$ is an $H$-monomial in $P_k^H$ that is not divisible by $Q_2$ with $h(\overline{R}) = h(R) - (2^n - 1) \equiv 0 \pmod{2^n}$ and $i_1(\overline{R}) = i_1(R) \leq 2^n - 1$.

Using Lemma 3.5, we get

$$Sq^2(R) = Sq^2(\overline{R}Q_2^{2n-1}) = \sum S_1, \sum T_1,$$

$$Sq^2+1(R) = Sq^2+1(\overline{R}Q_2^{2n-1}) = \sum S_2, \sum T_2.$$
where each term $S_1$ or $S_2$ is an $H$-monomial with $s(S_1) < n$ and $s(S_2) < n$, while each term $T_1$ or $T_2$ is an $H$-monomial with $i_2(T_1) = i_2(T_2) \equiv 2^n - 1 \pmod{2^n}$ and

\[
\left( \frac{h(T_1)}{2^{n-1}} \right) = \left( \frac{h(T_2)}{2^{n-1}} \right) = 0.
\]

Hence

\[
Ru^2n + \sum S_1v_1^2n + \sum S_2v_2^2n + \sum T_1v_1^2n + \sum T_2v_2^2n \in A^+ \cdot P_k.
\]

From the hypothesis, Lemma 4.2 (i) is valid for the triples $(S_1, v_1, n)$ and $(S_2, v_2, n)$; that means that $S_1v_1^2n$ and $S_2v_2^2n$ are in $A^+ \cdot P_k$ for every $S_1, S_2$. Also by the hypothesis, Lemma 4.2 (ii) holds for the triples $(T_1, v_1, n)$ and $(T_2, v_2, n)$, so $T_1v_1^2n$ and $T_2v_2^2n$ both belong to $A^+ \cdot P_k$ for every $T_1, T_2$. Therefore $Ru^2n \in A^+ \cdot P_k$.

Step 1 is proved.

**Step 2:** If 4.2 (i) holds for every $n \leq N$, then so does 4.2 (ii) for every $n \leq N$.

Applying Lemma 3.4, we obtain

\[
R = Sq^{2n+1}(\overline{R}) + \sum S,
\]

where $\overline{R} := R/Q_2^{2}(R)$ and each term $S$ in the sum is an $H$-monomial with $s(S) < n$

So

\[
Ru^2n = Sq^{2n+1}(\overline{R}u^2n) + \sum Su^2n.
\]

Since $s(S) < n$, by the hypothesis, Lemma 4.2 (i) holds for the triple $(S, u, n)$, that means $Su^2n \in A^+ \cdot P_k$ for every $S$ in the sum.

Set $\tilde{R} := \overline{R}Q_2^{2}(R)$. By the Cartan formula, we get

\[
Sq^{2n+1}(\tilde{R})u^2n = Sq^{2n+1}(Ru^2n) + Sq^{2n}(\tilde{R})(Sq^1u)^2n + \tilde{R}(Sq^2u)^2n
\]

\[
= Sq^{2n+1}(\tilde{R}u^2n) + Sq^{2n}[\tilde{R}(Sq^1u)^2n] + \tilde{R}(Sq^2u)^2n
\]

\[
= Sq^{2n+1}(\tilde{R}u^2n) + Sq^{2n}[\tilde{R}(Sq^1u)^2n] + \tilde{R}(Sq^2u)^2n.
\]

Thus

\[
Sq^{2n+1}(\tilde{R})u^2n + \tilde{R}(Sq^2u)^2n \in A^+ \cdot P_k.
\]

It is easy to see that $s(\tilde{R}) = s(Q_2^{2}(R)) = n - 1 < n$. So, from the hypothesis, Lemma 4.2 (i) holds for the triple $(\tilde{R}, (Sq^2u)^2n, n - 1)$; that means $\tilde{R}(Sq^2u)^2n \in A^+ \cdot P_k$. Hence $Sq^{2n+1}(\tilde{R})u^2n \in A^+ \cdot P_k$. Finally, we have

\[
Ru^2n = Sq^{2n+1}(\tilde{R})u^2n + \sum Su^2n \in A^+ \cdot P_k.
\]

Step 2 is proved.

**Step 3:** 4.2 (i) is valid for every $n$.

This is proved by induction on $n$.

For $n = 1$, from the hypothesis $s(R) < 1$ it yields $s(R) = 0$. By Lemma 5.1, $Ru^2n \in Sq^1P_k + Sq^2P_k$. So Lemma 4.2 (i) holds for $n = 1$.

Now let $n > 1$ and suppose inductively that 4.2 (i) has been proved for every smaller value of $n$. By Steps 1 and 2 above, 4.2 (ii) and 4.2 (iii) are also valid for every smaller value of $n$. We consider the following three cases.

**Case 1:** $s(R) = 0$. 

Then, by Lemma 5.1,
\[ Ru^{2^n} = R(u^{2^{n-1}})^2 \in \mathcal{A}^+ \cdot P_k. \]

**Case 2:** There exists an integer \( m \) with \( 0 \leq m < s(R) \) and \( \left( \frac{h(R)}{2^m} \right) = 0. \)

Combining the facts \( m < s(R) < n \) and \( i_2(R) \equiv 2^{s(R)} - 1 \pmod{2^{s(R)+1}} \), we get \( m + 1 < n \) and \( i_2(R) \equiv 2^{m+1} - 1 \pmod{2^{m+1}} \). Since \( m + 1 < n \) and by the inductive hypothesis, we can apply Lemma 4.2 (ii) to the triple \((R, u^{2^{n-m-1}}, m+1)\) and have \( Ru^{2^n} = R(u^{2^{n-m-1}})^2 2^{m+1} \in \mathcal{A}^+ \cdot P_k. \)

**Case 3:** \( s(R) > 0 \) and \( \left( \frac{h(R)}{2^m} \right) = 1 \) for every \( m \) with \( 0 \leq m < s(R) \).

It implies \( h(R) \equiv 2^{s(R)} - 1 \pmod{2^{s(R)}} \). Set \( p := s(R) > 0 \). We write uniquely \( R \) in the form \( R = RS^p \), where \( S \) and \( S \) are certain \( H \)-monomials with \( i_0(R), i_1(R), i_2(R), \ldots, i_k(R) \) all \( \leq 2^p - 1 \).

Note that \( i_2(R) \equiv i_2(R) \pmod{2^p} \), as \( p = s(R) \). Combining this with the fact \( i_2(R) \leq 2^p - 1 \), we obtain \( i_2(R) = 2^p - 1 \). Since \( p = s(R) \), so \( 2^p \) does not occur in the dyadic expansion of \( i_2(R) = i_2(R) + 2p_i_2(S) = 2p - 1 + 2p_i_2(S) \).

Hence, it implies \( s(S) = 0 \).

Applying Lemma 5.1 to the \( H \)-monomial \( S \) and \( v := u^{2^{n-p-1}} \neq 1 \), we get \( Sv^2 \in Sq^1 P_k + Sq^2 P_k \).

On the other hand, we observe that
\[ h(R) = h(R) - 2^ph(S) \equiv h(R) \pmod{2^p} \Rightarrow 2^p - 1 \pmod{2^p}, \]
\[ i_2(R) = 2^p - 1 \geq i_1(R). \]

Using the inductive hypothesis together with the assumption \( p = s(R) < n \), we can apply Lemma 4.2 (iii) to the triple \((R, Sv^2, p)\) and get
\[ Ru^{2^n} = R(Sv^2)^2 2^n \in \mathcal{A}^+ \cdot P_k. \]

Step 3 is proved. Therefore, Lemma 4.2 follows. \( \square \)

**References**


Department of Mathematics
Vietnam National University, Hanoi
334 Nguyễn Trãi Street, Hanoi, Vietnam
Email address:
Nguyễn H. V. Hùng: nhvhung@hotmail.com
Trần Ngọc Nam: trngnam@hotmail.com