VNU. JOURNAL OF SCIENCE, Nat. Sci., t .XV, n^{0}5 - 1999

SPLITTING $B(Z/p)^n_+$ FROM THE MULTIPLICATIVE GROUP OF THE SUBFIELDS OF FINITE FIELDS*

Nguyen Gia Dinh

Department of Mathematics, College of Sciences, Hue University

Abstract. *Let p be a prime number, F_{p^n} the field of p^n elements, K a subfield of F_{p^n} and $K^* = K \setminus \{0\}$ the multiplicative group of K. By using representation theory and explicit idempotents in the group ring $F_p[K^*]$, we give a splitting of $B(Z/p)^n_+$ into stable wedge summands and a condition so that each of these summands does not contain indecomposable summands*

I. INTRODUCTION

The current tendency of algebraic topology is to survey the stable splittings of topolog spaces, especially classifying spaces. That is exactly one of the causes giving an impulse stronger t the research on cohomology and representation of groups. Since 1984, with Carlsson's solution c the Segal Conjecture [1], the most significant recent development in homotopy theory, the algebrai topologists have been interested more and more in the problem of finding a stable splitting

$$BP_+ \simeq X_1 \vee X_2 \vee \ldots \vee X_N$$

nto wedge summands, completed at p, where p is a fixed prime number, P is an abelian p-grour and BP_+ is its classifying space with a disjoint basepoint. A decomposition of the identity i $Z/p[\mathrm{Aut}(P)]$ into orthogonal idempotents induces a stable splitting of BP_+ [6]. Harris and Kuh have shown that splitting questions about an arbitrary abelian p-group can be reduced to specia case of an elementary abelian p-group [8].

Let F_{p^n} be the field of p^n elements, K a subfield of F_{p^n} and $K^* = K \setminus \{0\}$ the multiplicativ group of K. By some way, we can consider K^* as a subgroup of $GL_n(Z/p)$ (=Aut$(Z/p)^n$). Stabl splitting of a G-topology space X depends mainly partially on the action of group G. In this paper we give a stable splitting of $B(Z/p)^n_+$ from K^* when $B(Z/p)^n_+$ is considered as a space on whicl the action of K^* is the restriction of the action of $F^*_{p^n}$. Here, $F^*_{p^n}$ acts naturally on $(Z/p)^n$ by identifying F_{p^n} with $(Z/p)^n$ as a vector space. Moreover, we also give a condition so that each o the wedge summands of this splitting does not contain indecomposable summands.

* The paper was partially supported by the National Fundamental Research Program N^o 1.4.2

II. MAIN RESULTS

Proposition 2.1. *If K is a subfield of the field F_{p^n} then K^* can be considered as a subgroup* ($GL_n(Z/p)$.

Proof. In F_{p^n}, choose an element ω so that ω generates the cyclic group $F_{p^n}^*$ and $\{\omega, \phi(\omega), \dots, \phi^{n-1}$ forms a basis for F_{p^n} over F_p ([4]), where $\phi(a) = a^p$ is the Frobenius. Let $p(x) = a_0 + a_1x + \cdots$ $a_{n-1}x^{n-1} + x^n$ be the minimal polynomial for ω. Let

$$\theta = \begin{pmatrix} 0 & 0 & \dots & 0 & -a_0 \\ 1 & 0 & \dots & 0 & -a_1 \\ 0 & 1 & \dots & 0 & -a_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & 1 & -a_{n-1} \end{pmatrix}$$

be the $n \times n$ matrix over F_p representing multiplication by ω in the basis $\{1, \omega, \dots, \omega^{n-1}\}$. Sin ω is a generator of $F_{p^n}^*$, we see that θ has order $p^n - 1$ in $GL_n(Z/p)$. Therefore, we can conside

$$F_{p^n}^* \quad = . < \theta > \quad \subseteq GL_n(Z/p) .$$

Given a subfield K of the field F_{p^n}. Then $K = F_{p^m}$ with $m \mid n$ and $(p^m - 1) \mid (p^n - 1)$. F $F_{p^n} = F_p(\omega)$ and $F_{p^n}^* =< \theta >$, we have

$$K \;=\; F_p(\omega^{n/m}) \text{ and } K^* =< \theta^r >,$$

where $r = \frac{p^n-1}{p^m-1}$.

Notation 2.2 We let $C_m =< c >$ act on $Z/(p^n - 1)$ by $c(u) = up^{n/m}$ (mod $p^n - 1$). L $[u]$ be the orbit containing u under the action of C_m. On the set $(Z/(p^n - 1))/C_m$, the action $C_r =< a >\cong (Z/(p^n - 1))/(Z/(p^m - 1))$ is given by $a([u]) = [u + p^m - 1]$. Let $V_u(m) = \cup_{h=0}^{r-1} a^h([u$ For each $V_u(m)$, we choose u to be the smallest element of $V_u(m)$. Then $V_u(m)$ is exactly the s consisting of the elements of $Z/(p^n - 1)$ in form $up^l + h(p^m - 1)$ with $0 \le l \le m-1$, $0 \le h \le r-1$ a the set consisting of such representatives u is $I(m)$. Here, $I(m)$, $J_u(m)$ and $z_u(m)$ are determin as follows: We let $C_m =< \phi >$ act on $Z/(p^m - 1)$ by $\phi(u) = up$. Let $J_u(m)$ be the orbit containi u, and let $I(m)$ be a set consisting of one element from each orbit. The cardinality of $J_u(m)$ $z_u(m)$, where $z_u(m)$ is the smallest positive exponent k with $up^k \equiv u$ (mod $p^m - 1$).

Harris has proved the elements ([7],3.5,4.4)

$$f_u(m) = \sum_{v \in J_u(m)} e_v(m) \ , \ u \in I(m) \ , \ \text{where } \ e_v(m) = - \sum_{k=0}^{p^m-2} \omega^{-kvr}\theta^{kr}$$

form a primitive orthogonal set of idempotents with $\sum f_u(m) = 1$ in $F_p[K^*]$. In order to give splitting of $B(Z/p)^n_+$ from K^*, each $f_u(m)$ have to be expressed as a sum of primitive orthogor idempotents

$$e_j = - \sum_{k=0}^{p^n-2} \omega^{-kj}\theta^k \ , \ j \in Z/(p^n - 1) \ ,$$

in $F_{p^n}[F_{p^n}^*]$ (see [4]). We have the following main lemma:

emma 2.3. *For $m \mid n$ and $u \in I(m)$, we have*

$$f_u(m) = \sum_{j\in V_u(m)} e_j = \sum_{l=0}^{z_u(m)-1} \sum_{j\equiv up^l (\mathrm{mod}\ p^m-1)} e_j.$$

roof. We have

$$\sum_{j\in V_u(m)} e_j = -\sum_{l=0}^{z_u(m)-1}\sum_{v=0}^{p^n-2}\sum_{h=0}^{r-1} \omega^{-v(up^l+h(p^m-1))}\theta^v,$$

here $r = \frac{p^n-1}{p^m-1}$, $r \equiv 1 (\mathrm{mod}\ p)$, and

$$\sum_{h=0}^{r-1} \omega^{-v(up^l+h(p^m-1))} = \begin{cases} 0 & \text{if } r \nmid v, \\ r\omega^{-vup^l} & \text{if } r \mid v. \end{cases}$$

ence

$$\sum_{j\in V_u(m)} e_j = \sum_{l=0}^{z_u(m)-1} \left(-\sum_{k=0}^{p^m-2} \omega^{-kup^l r}\theta^{kr}\right) = \sum_{l=0}^{z_u(m)-1} e_{up^l}(m) = f_u(m).$$

heorem 2.4. *For $m \mid n$, let $\widehat{Z}_{n,m}(u) = f_u(m)B(Z/p)^n_+$. Then*

$$B(Z/p)^n_+ \simeq \bigvee_{u\in I(m)} \widehat{Z}_{n,m}(u),$$

$$\widehat{Z}_{n,m}(u) \simeq \bigvee_{i\in I\cap V_u(m)} \widehat{Y}_n(i) \simeq \bigvee_{j\in V_u(m)} Y_n(j),$$

here $\widehat{Y}_n(i) = f_i(n)B(Z/p)^n_+$ and $Y_n(j)$ is the Campbell-Selick.

The Campbell-Selick summands are described in details in [2] and [7].)

roof. From Lemma 2.3, we have

$$f_u(m) = \sum_{i\in I\cap V_u(m)} f_i.$$

ere the $f_u(m)$'s ($u \in I(m)$) form an orthogonal set of idempotents with $\sum f_u(m) = 1$ in $_p[GL_n(Z/p)]$. Hence, the proof of the Theorem is completed. ◇

In [8], Harris and Kuhn follow the constructions of the irreducible representations S_λ (resp. $_\lambda$) for $\lambda \in \Lambda$ (resp. $\lambda \in \Lambda'$) of $F_p[M_n(Z/p)]$ (resp. $F_p[GL_n(Z/p)]$) as given by James and Kerber [9] chapter 8 - in particular, exercise 8.4 of their book, where

$$\Lambda = \{(\lambda_1, \dots, \lambda_n) \mid 0 \le \lambda_k \le p-1, 1 \le k \le n\},$$

$$\Lambda' = \{(\lambda_1, \dots, \lambda_n) \mid 0 \le \lambda_k \le p-1, 1 \le k \le n-1, 0 \le \lambda_n \le p-2\}.$$

Denote the stable summand of $B(Z/p)^n_+$ corresponding to $S_{(\lambda)}$ (resp. $S'_{(\lambda)}$) by $X_{(\lambda)}$ (resp. $X'_{(\lambda)}$
The X_λ's are the indecomposable summands of $B(Z/p)^n_+$ and the X'_λ's are splitted over the X_λ

(2.5)
$$X'_{(\lambda_1,\dots,\lambda_n)} \simeq X_{(\lambda_1,\dots,\lambda_n)}, \text{ if } 0 < \lambda_n < p-1 \text{ and}$$
$$X'_{(\lambda_1,\dots,\lambda_{n-1},0)} \simeq X_{(\lambda_1,\dots,\lambda_{n-1},0)} \vee X_{(\lambda_1,\dots,\lambda_{n-1},p-1)}.$$

For each $\lambda \in \Lambda'$, $i \in I$, let a'_{λ_i} be the number of times the representation $F_p[F^*_{p^n}]f_i(n)$ occu in a composition series for $\mathrm{Res}^{GL_n(Z/p)}_{F^*_{p^n}} S'_\lambda$. Then for $j \in J_i$, Harris has proved that ([7], 4 6):

(2.6)
$$Y_n(j) \simeq \bigvee_{\lambda\in\Lambda'} a'_{\lambda_i} X'_\lambda .$$

One of the fundamental problems that has been being intersted in at present in the problem finding a stable splitting of $B(Z/p)^n_+$ is to determine a'_{λ_i}.

Lemma 2.7 ([5]). *The eigenvalues for the action of θ on the Weyl module W^α are $\omega^{\beta(T)}$ whe T is a semistandard α-tableau of content $(\beta_1,\dots,\beta_n)$ and $\beta(T) \equiv (\sum_{k=1}^n p^{k-1}\beta_k)$ (mod $p^n - 1$*

Here, the notions of Weyl module and semistandard α-tableau of content $(\beta_1,\dots,\beta_n)$ c be found in [8].

Lemma 2.8 ([5]). *The eigenvalues for the action of θ on $S_{(\lambda)}$ are ω^j with $j \equiv m_\lambda$(mod $p -$ where $m_\lambda = \lambda_1 + 2\lambda_2 + \dots + n\lambda_n$ with $\lambda = (\lambda_1,\dots,\lambda_n)$.*

From Theorem 2.4, (2.5), (2.6), Lemma 2.7 and Lemma 2.8, we have the following theore

Theorem 2.9. *If $m_\lambda \not\equiv u$ (mod $p-1$) then X_λ is not a summand of $\widehat{Z}_{n,m}(u)$, so it is not summand of $Y_n(j)$ for each $j \in V_u(m)$.*

For $\lambda = (\lambda_1,\dots,\lambda_n)$ where $\lambda_i = 0$ or $p-1$, $m_\lambda \equiv 0$ (mod $p-1$) and we have the tolowi corollary:

Corollary 2.10. *$X_{(\lambda_1,\dots,\lambda_n)}$ for $\lambda_i = 0$ or $p-1$, for example $X_{(p-1,\dots,p-1,p-1)}$ and $X_{(p-1,\dots,p-1,}$ are the summands of $\bigvee_{j\equiv 0(\mathrm{mod}\ p-1)} Y_n(j)$.*

REFERENCES

1. G. Carlsson. Equivariant stable homotopy and Segal's Burnside ring conjecture, *Ann. Mat* **120**(1984), 189-224..
2. H.E.A.Campbell and P.S.Selick. Polynomial algebras over the Steenrod algebra, *Comme Math. Helv.* , **65** (1990), 171-180.
3. H.Davenport. Bases for finite fields, *J.London Math.Soc.* , **65**(1968), 21-39.
4. Nguyen Gia Dinh. Modular representation of some linear groups over a finite field, *Viet. Math.*, Vol. **24**, No.2 (1996), 143-154.
5. Nguyen Gia Dinh. On certain stable wedge summands of $B(Z/p)^n_+$, Acta mathematica Vi namica, Vol.**21**, No.1 (1996), 1-13.
6. J.C. Harris, *Stable splittings of classifying spaces*, Ph.D. thesis, University of Chicago, 1985.

. J.C. Harris, *On certain stable wedge summands of* $B(Z/p)^n_+$, Can. J. Math., 44(1) (1992), 104-118.

. J.C. Harris and N.J. Kuhn, *Stable decompositions of classifying spaces of finite abelian p-groups*, Math. Proc. Camb. Phil. Soc., 103 (1988), 427-449.

. G. James and A. Kerber, *The Representation Theory of Symmetric Group*, Encyclopedia of Math. and its Applications,16,Addison-Wesley, 1981.

ẠP CHÍ KHOA HỌC ĐHQGHN, KHTN, t.XV, n°5 - 1999

PHÂN RÃ $B(Z/P)^N_+$ TỪ NHÓM NHÂN TÍNH CỦA CÁC TRƯỜNG CON TRONG CÁC TRƯỜNG HỮU HẠN

Nguyễn Gia Định

Khoa Toán - Đại học KH - Đại học Huế

Giả sử p là một số nguyên tố, F_{p^n} là trường của p^n các phần tử, K là trường con của F_{p^n} à $K^* = K \setminus \{0\}$ nhóm nhân tính của K. Bằng cách sử dụng lý thuyết biểu diễn và các lũy đẳng ên trong vành nhóm $F_p[K^*]$, chúng ta đưa ra sự phân hoạch của $B(Z/p)^n_+$ thành các hạng tử ọng số ổn định và điều kiện để mỗi trong các hạng tử này không chứa các hạng tử không khai iển được.