Zeitschrift: L'Enseignement Mathématique
Herausgeber: Commission Internationale de l'Enseignement Mathématique
Band: 33 (1987)
Heft: 1-2: L'ENSEIGNEMENT MATHÉMATIQUE

Artikel: SOME EXAMPLES OF GROUP ALGEBRAS WITHOUT FILTRED MULTIPLICATIVE BASIS

Autor: Paris, Luis

DOI: https://doi.org/10.5169/seals-87900

L'Enseignement Mathématique, t. 33 (1987), p. 307-314

SOME EXAMPLES OF GROUP ALGEBRAS WITHOUT FILTRED MULTIPLICATIVE BASIS

by Luis PARIS

Let R be a finite dimensional algebra over a field K. A *filtred multiplicative basis* B for R is a K-basis of R such that

MB1) $b, b' \in B$ implies $b \cdot b' \in B$ or $b \cdot b' = 0$,

MB2) $B \cap \operatorname{rad}(R)$ is a K-basis of $\operatorname{rad}(R)$, where $\operatorname{rad}(R)$ is the radical of R.

In [B.-G.-R.-S.], R. Bautista, P. Gabriel, A. V. Roiter and L. Salmereon prove that if R is of finite representation type, i.e. if there are only finitely many isomorphism classes of indecomposable R-modules, then R possesses a filtred multiplicative basis. In their introduction, they state: "It is not known to us whether general group-algebras do [have filtred multiplicative bases]".

Of course, it is well known that if K is a field of characteristic p, then the group algebra KG of the finite group G is of finite representation type if and only if the p-Sylow subgroups of G are cyclic. (See e.g. [C.-R.], page 431.)

However, if $G = C_p \times C_p$, the direct product of 2 copies of a cyclic group of order p, generated by a and b, then the set

$$B = \{(a-1)^i (b-1)^j \mid 0 \leqslant i, j \leqslant p-1\}$$

is a filtred multiplicative basis of KG for any field K of characteristic p, although the representation type of $K[C_p \times C_p]$ is infinite.

In this note we produce some less obvious examples showing that the group algebras of p-groups over an algebraically closed field of characteristic p do not necessarily admit a filtred multiplicative basis.

We also show that for the group of quaternion units Q, of order 8, and K of characteristic 2, the algebra KQ admits a filtred multiplicative basis if and only if K contains a primitive 3-rd root of unity.

This note is a condensed version of my "Travail de Diplôme" at the University of Geneva. I am grateful to Claude Cibils and Michel Kervaire for valuable suggestions and their encouragements during my work.

§ 1. Preliminary remarks

Note that if R is a finite dimensional K-algebra and B is a filtred multiplicative basis (as defined above), then $B \cap \{\text{rad}(R)\}^n$ is a K-basis of $\{\text{rad}(R)\}^n$ for all $n \geqslant 1$. Indeed, the set $B \cap \{\text{rad}(R)\}^n$ is linearly free over K since B is. By hypothesis, $B \cap \text{rad}(R)$ is a K-basis of $\text{rad}(R)$ and thus the set of products $b_1 \cdot \ldots \cdot b_n$ with $b_i \in B \cap \text{rad}(R)$ is a generator system for $\{\text{rad}(R)\}^n$. But all such products $b_1 \cdot \ldots \cdot b_n$ are either 0 or belong to $B \cap \{\text{rad}(R)\}^n$. Hence, $B \cap \{\text{rad}(R)\}^n$ generates $\{\text{rad}(R)\}^n$ over K.

The case of a finite abelian group G is easy to understand:
Let

$$G_p = <a_1> \times <a_2> \times \ldots \times <a_r>$$

be a decomposition of the p-Sylow subgroup G_p of G as a direct product of cyclic groups of orders $p^{n_1}, \ldots, p^{n_r}$ respectively. Let $G = G_p \times H$, where $|H|$ is prime to p. Then,

$$B = \{(a_1-1)^{m_1} \cdot (a_2-1)^{m_2} \ldots (a_r-1)^{m_r} \cdot h \mid 0 \leqslant m_i \leqslant n_i - 1, h \in H\}$$

is a filtred multiplicative basis of KG for any field K of characteristic p.

If we insist that the elements of B outside $\text{rad}(R)$ should be orthogonal idempotents, then we have to require that K be algebraically closed, as otherwise KH itself need not have a filtred multiplicative basis B satisfying

MB3) If $e, e' \in B \backslash \text{rad}(R)$, $e \neq e'$, then $e^2 = e$ and $e \cdot e' = 0$.

Observe that, more generally, if B_1, B_2 are filtred multiplicative bases for KG_1 and KG_2, then $B_1 \times B_2$ is a filtred multiplicative basis for $K[G_1 \times G_2]$.

In the next paragraphs we will examine examples of p-groups.

If G is a p-group, and K a field of characteristic p, then $\text{rad}(KG)$ is the augmentation ideal

$$\text{rad}(KG) = \{\sum_{g \in G} \alpha_g g \mid \sum_{g \in G} \alpha_g = 0\}$$

Note also that in that case, a filtred multiplicative basis B for KG necessarily contains 1. Indeed, $\dim_k \{KG/\text{rad}(KG)\} = 1$. If $e \in B$ is the unique element outside $\text{rad}(KG)$, then $e^2 \notin \text{rad}(KG)$ and therefore $e^2 = e$. But KG is local, thus $e = 1$. (Alternatively, $e = 1 + r$ with $r \in \text{rad}(KG)$ and $e = e^{p^N} = 1 + r^{p^N} = 1$.)

Thus for p-groups, axiom MB3) is automatically satisfied.

§ 2. EXAMPLES WHERE THE GROUND FIELD IS IRRELEVANT

Let p be a prime number (e.g. $p=2$), and let n be a natural number, $n \geqslant 4$.

Consider the group $H_n(p)$ defined by generators and relations:

$$H_n(p) = \langle a, b : a^{p^{n-1}} = 1, b^p = 1, ba = a^{1+p^{n-2}}b \rangle .$$

The group $H_n(p)$ is a finite p-group of order p^n.

PROPOSITION 1. *Let K be an arbitrary field of characteristic p. The group algebra $K[H_n(p)]$ does not possess any filtred multiplicative basis.*

Remark. In contrast, consider the dihedral group

$$D(2^n) = \langle r, s : r^{2^{n-1}} = 1, s^2 = 1, sr = r^{-1}s \rangle .$$

Both $D(2^n)$ and $H_n(2)$ are semi-direct products of $\mathbf{Z}/2^{n-1}\mathbf{Z}$ by $\mathbf{Z}/2\mathbf{Z}$.

However, a straightforward calculation shows that the set B consisting of the following elements

$$1, 1+s,$$
$$(r+s)^k, (1+s)(r+s)^k \quad \text{for} \quad k = 1, \ldots, 2^{n-2},$$
$$(r+s)^l(1+s), (1+s)(r+s)^l(1+s) \quad \text{for} \quad l = 1, \ldots, 2^{n-2}-1$$

is a filtred multiplicative basis of $K[D(2^n)]$ for any field K of characteristic 2.

We proceed to prove Proposition 1. Let $M = \operatorname{rad} K[H_n(p)]$. Recall that a, b are the generators of the defining presentation of $H_n(p)$.

LEMMA. *Let L_k be the set*

$$L_k = \{(1-a)^{k_1}(1-b)^{k_2} \mid 0 \leqslant k_1 < p^{n-1}, 0 \leqslant k_2 < p \text{ and } k_1 + k_2 = k\}.$$

Claim: The classes mod M^{k+1} *of the elements of L_k form a K-basis of M^k/M^{k+1}.*

Proof. We show first, by induction on k, that the set

$$\{(1-a)^l(1-b)^{k-l} \mid 0 \leqslant l \leqslant k\}$$

is a system of K-generators of M^k mod M^{k+1}.

If $g, g' \in H_n(p)$, the identity

$$1 - g \cdot g' = (1-g) + (1-g') - (1-g)(1-g')$$

implies that $\{(1-a),(1-b)\}$ is a system of K-generators of $M \bmod M^2$.

Suppose by induction that

$$\{(1-a)^l (1-b)^{m-l} \mid 0 \leqslant l \leqslant m\}$$

is a K-generator system of $M^m \bmod M^{m+1}$. The set of products $u_1 \cdot u_2$ with $u_1 \in M$, $u_2 \in M^m$ generates M^{m+1} over K. Thus we have by induction,

$$u_1 = \alpha_1(1-a) + \alpha_2(1-b) \bmod M^2 \quad \text{with} \quad \alpha_1, \alpha_2 \in K,$$

$$u_2 = \sum_{l=0}^{m} \beta_l (1-a)^l (1-b)^{m-l} \bmod M^{m+1} \quad \text{with} \quad \beta_l \in K.$$

Hence

$$u_1 \cdot u_2 = \sum_{l=0}^{m} \left(\alpha_1 \beta_l (1-a)^{l+1} (1-b)^{m-l} + \alpha_2 \beta_l (1-b)(1-a)^l (1-b)^{m-l}\right) \bmod M^{m+2}.$$

Now,

$$\begin{aligned}(1-b)(1-a) &= 1 - a - b + ba \\ &= 1 - a - b + ab - (ab-ba) \\ &= (1-a)(1-b) - (ab-ba).\end{aligned}$$

But

$$ab - ba \in M^{p^{n-2}} \subset M^3 \quad (\text{recall } n \geqslant 4),$$

since

$$ab - ba = ab - a^{1+p^{n-2}} b = (1-a)^{p^{n-2}} ab.$$

It follows that

$$(1-b)(1-a) = (1-a)(1-b) \bmod M^3$$

and therefore

$$(1-b)(1-a)^l (1-b)^{m-l} = (1-a)^l (1-b)^{m-l+1} \bmod M^{m+2}.$$

Consequently,

$$u_1 \cdot u_2 = \sum_{l=0}^{m} \left(\alpha_1 \beta_l (1-a)^{l+1} (1-b)^{m-l} + \alpha_2 \beta_l (1-a)^l (1-b)^{m-l+1}\right) \bmod M^{m+2}$$

and the set

$$L = \{(1-a)^{k_1}(1-b)^{k_2} \mid 0 \leqslant k_1 < p^{n-1},\ 0 \leqslant k_2 < p\}$$

is a system of K-generators of $K[H_n(p)]$.

Since

$$|L| = p^n = |H_n(p)| = \dim_K K[H_n(p)],$$

it follows that L is a K-basis of $K[H_n(p)]$.

We have just proved that

$$L_k = \{(1-a)^{k_1}(1-b)^{k_2} \mid 0 \leqslant k_1 < p^{n-1}, 0 \leqslant k_2 < p, k_1 + k_2 = k\}$$

generates $M^k \bmod M^{k+1}$.

We have to prove that L_k is linearly free over K. If $\sum_{t \in L_k} \alpha_t t = 0 \bmod M^{k+1}$ where $\alpha_t \in K$ then we can write $\sum_{t \in L_k} \alpha_t t = \sum_{\substack{s \in UL_l \\ l > k}} \beta_5 s$ where $\beta_5 \in K$. Consequently $\alpha_t = 0$ for all t in L_k because L is a K-basis of $K[H_n(p)]$.

We now come to the proof that $K[H_n(p)]$ has no filtred multiplicative basis.

We proceed by contradiction. If B were such a basis, consider

$$\{u, v\} = B \cap \{M \backslash M^2\},$$

the set of elements of B in M but outside M^2.

$\{u, v\}$ is a K-basis of $M \bmod M^2$. Also $K[H_n(p)] = K[u, v]$, the algebra generated over K by u and v.

We are going to prove:

Claim: $u \cdot v = v \cdot u$

This implies that $K[H_n(p)] = K[u, v]$ is commutative: Contradiction.

Proof of the claim. By the lemma,

$$u = x_1(1-a) + y_1(1-b) \bmod M^2$$

$$v = x_2(1-a) + y_2(1-b) \bmod M^2,$$

where $x_1, x_2, y_1, y_2 \in K$ and $x_1y_2 - x_2y_1 \neq 0$.

Now,

$$u \cdot v = x_1x_2(1-a)^2 + y_1y_2(1-b)^2 + (x_1y_2 + x_2y_1)(1-a)(1-b) \bmod M^3$$

$$v \cdot u = x_1x_2(1-a)^2 + y_1y_2(1-b)^2 + (x_1y_2 + x_2y_1)(1-a)(1-b) \bmod M^3$$

since

$$(1-a)(1-b) = (1-b)(1-a) \bmod M^3 .$$

We know that $(1-a)^2, (1-b)^2, (1-a)(1-b)$ forms a K-basis of M^2/M^3. Hence $u \cdot v \neq 0$ and $v \cdot u \neq 0 \bmod M^3$. Otherwise

$$x_1 x_2 = y_1 y_2 = x_1 y_2 + x_2 y_1 = 0$$

and $x_1 y_2 - x_2 y_1 = 0$ contrary to the fact that $\{u, v\}$ gives a basis of M/M^2.

Thus $uv, vu \in B$ satisfy $uv = vu \bmod M^3$ and $uv \neq 0$, $vu \neq 0 \bmod M^3$.

It follows that $uv = vu$. In fact more generally, if $u_1, u_2 \in B \backslash M^k$ and $u_1 = u_2 \bmod M^k$ then $u_1 = u_2$. Proof: $B \cap M^k$ is a basis of M^k, thus $u_1 - u_2 = \sum_{u \in B \cap M^k} \lambda_u u$. This is possible only if $u_1 - u_2 = 0$.

§ 3. The group of quaternion units

Let Q be defined by generators and relations:

$$Q = \langle a, b : a^4 = 1, b^2 = a^2, ab = b^3 a \rangle .$$

Set $i = a, j = b, k = ab$ and $c = a^2$. Then

$$Q = \{1, c, i, ci, j, cj, k, ck\} .$$

Proposition 2. *Let* K *be a field of characteristic* 2. *The group algebra* $K[Q]$ *possesses a filtred multiplicative basis if and only if* K *contains a primitive cube root of unity.*

Proof. If K contains a primitive cube root of unity, say ω,

let

$$B = \{1, u, v, uv, vu, u^2, v^2, u^3\} ,$$

where

$$u = \omega i + \omega^2 j + k$$
$$v = \omega^2 i + \omega j + k .$$

It is easily verified that B is a filtred multiplicative basis.

Conversely, suppose that $K[Q]$ possesses a filtred multiplicative basis B.

Observe that $\{1+i, 1+j\}$ is a K-basis of M/M^2, where again $M = \operatorname{rad} K[Q]$. Also $\{1+c, 1+i+j+k\}$ is a K-basis of M^2/M^3. Since $B \cap (M/M^2) = \{u, v\}$ must be a K-basis of M mod M^2, we have

$$u = x_1(1+i) + y_1(1+j) \bmod M^2 ,$$

$$v = x_2(1+i) + y_2(1+j) \bmod M^2 ,$$

with $x_1, y_1, x_2, y_2 \in K$ and $x_1 y_2 + x_2 y_1 \neq 0$.
Now

$$u \cdot v = (x_1 x_2 + y_1 y_2 + x_2 y_1)(1+c) + (x_1 y_2 + x_2 y_1)(1+i+j+k) \bmod M^3 ,$$

$$v \cdot u = (x_1 x_2 + y_1 y_2 + x_1 y_2)(1+c) + (x_1 y_2 + x_2 y_1)(1+i+j+k) \bmod M^3 .$$

Therefore,

$$u \cdot v + v \cdot u = (x_1 y_2 + x_2 y_1)(1+c) \bmod M^3 \neq 0 \bmod M^3 ,$$

and so $u \cdot v \neq v \cdot u$.

We must have $uv \in B \cap (M^2 \backslash M^3)$ since the $(1+i+j+k)$-coordinate of $u \cdot v$ is non-zero. Similarly $v \cdot u \in B \cap (M^2 \backslash M^3)$. But $\dim (M^2/M^3) = 2$ and so

$$B \cap (M^2 \backslash M^3) = \{uv, vu\} .$$

Consider the element $u^2 \in M^2$. Either $u^2 = uv$ or $u^2 = vu$ or $u^2 \in M^3$. But $u^2 = (x_1^2 + y_1^2 + x_1 y_1)(1+c) \bmod M^3$.

Since the $(1+i+j+k)$-coordinate of u^2 is 0, we have $u^2 \neq uv$, $u^2 \neq vu$.

Hence $u^2 \in M^3$. This implies $u^2 = 0$, and it follows that the quadratic form $x_1^2 + y_1^2 + x_1 y_1$ represents 0 non-trivially in K and $w = y_1/x_1$ is a primitive cube root of unity in K.

REFERENCES

[B.-G.-R.-S.] Bautista, R., P. Gabriel, A. V. Roiter and L. Salmeron. Representation-finite algebras and multiplicative basis. *Invent. Math. 81* (1985), 217-285.

[C.-R.] Curtis, C. W. and I. Reiner. *Representation theory of finite groups and associative algebras.* Pure and Appl. Math., vol. 11, Interscience, New York, 1962.

(Reçu le 23 juillet 1987)

Luis Paris

Université de Genève
Section de Mathématiques
2-4, rue du Lièvre, Case postale 240
CH-1211 Genève 24 (Switzerland)