**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

**Kapitel:** §2. Examples where the ground field is irrelevant

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

**Nutzungsbedingungen**

Die ETH-Bibliothek ist die Anbieterin der digitalisierten Zeitschriften auf E-Periodica. Sie besitzt keine Urheberrechte an den Zeitschriften und ist nicht verantwortlich für deren Inhalte. Die Rechte liegen in der Regel bei den Herausgebern beziehungsweise den externen Rechteinhabern. Das Veröffentlichen von Bildern in Print- und Online-Publikationen sowie auf Social Media-Kanälen oder Webseiten ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. Mehr erfahren

**Conditions d'utilisation**

L'ETH Library est le fournisseur des revues numérisées. Elle ne détient aucun droit d'auteur sur les revues et n'est pas responsable de leur contenu. En règle générale, les droits sont détenus par les éditeurs ou les détenteurs de droits externes. La reproduction d'images dans des publications imprimées ou en ligne ainsi que sur des canaux de médias sociaux ou des sites web n'est autorisée qu'avec l'accord préalable des détenteurs des droits. En savoir plus

**Terms of use**

The ETH Library is the provider of the digitised journals. It does not own any copyrights to the journals and is not responsible for their content. The rights usually lie with the publishers or the external rights holders. Publishing images in print and online publications, as well as on social media channels or websites, is only permitted with the prior consent of the rights holders. Find out more

**Download PDF:** 27.04.2026

**ETH-Bibliothek Zürich, E-Periodica, https://www.e-periodica.ch**

## § 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

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

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*

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

*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

$$x_1x_2 = y_1y_2 = x_1y_2 + x_2y_1 = 0$$

and $x_1y_2 - x_2y_1 = 0$ 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:

$$Q = <a, b : a^4 = 1, b^2 = a^2, ab = b^3a> .$$

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 $\omega$, 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 $B$.