§3. The group of quaternion units

Objekttyp: **Chapter**

Zeitschrift: **L'Enseignement Mathématique**

Band (Jahr): **33 (1987)**

Heft 1-2: **L'ENSEIGNEMENT MATHÉMATIQUE**

PDF erstellt am: **26.09.2024**

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 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 $M = \text{rad } K[Q]$. 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 $x_1y_2 + x_2y_1 \neq 0$.
Now

$$\begin{aligned} u \cdot v &= (x_1x_2+y_1y_2+x_2y_1)(1+c) \\ &\quad + (x_1y_2+x_2y_1)(1+i+j+k) \bmod M^3 , \\ v \cdot u &= (x_1x_2+y_1y_2+x_1y_2)(1+c) \\ &\quad + (x_1y_2+x_2y_1)(1+i+j+k) \bmod M^3 . \end{aligned}$$

Therefore,

$$u \cdot v + v \cdot u = (x_1y_2+x_2y_1)(1+c) \bmod M^3 \neq 0 \bmod M^3 ,$$

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 $u^2 = (x_1^2+y_1^2+x_1y_1)(1+c) \bmod M^3$.

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 $x_1^2 + y_1^2 + x_1y_1$ represents 0 non-trivially in K and $w = y_1/x_1$ is a primitive cube root of unity in K.