Mathematica Balkanica

Mathematical Society of South-Eastern Europe
A quarterly published by
the Bulgarian Academy of Sciences – National Committee for Mathematics

Mathematica Balkanica

New Series Vol. 12, 1998, Fasc. 3-4

On the Minimal Idempotents of Twisted Group Algebras of Cyclic 2-Groups [1]

Jordan Epitropov, Todor Mollov, Nako Nachev

Presented by Bl. Sendov

For a field K of the second kind with respect to 2 and of characteristic different from 2, we consider the decomposition of the binomials $x^{2^n} - a$ into a product of irreducible factors over K and find the explicit form of the minimal idempotents of the twisted group algebra $K^t\langle g\rangle$ of a cyclic 2-group $\langle g\rangle$ over K.

AMS Subj. Classification: 16S35, 20D20; 12E99

Key Words: minimal idempotents, twisted group algebras, cyclic 2-groups

Introduction

The starting point of a lot of investigations on twisted group algebras is to find the minimal idempotents of the twisted group algebra K^tG, where G is a cyclic group and K is a field. When $\langle g\rangle$ is a cyclic p-group, p is an odd prime and K is a field of characteristic different from p, Nachev and Mollov [3] have found the explicit form of the minimal idempotents of $K^t\langle g\rangle$. For $p = 2$, additional difficulties arise which are connected with the decomposition of the polynomial $x^{2^n} - a$ into irreducible factors over the field K. The purpose of the present paper is to find the explicit form of the minimal idempotents of $K^t\langle g\rangle$ when $\langle g\rangle$ is a cyclic 2-group and K is a field of the second kind with respect to 2 (and of characteristic different from 2). We shall mention that the semisimplicity of the twisted group algebra $K^t\langle g\rangle$ in this case is a well known fact (see e.g. [1] or [4]).

The paper is organized as follows. In Section 1 we give some notations, definitions and preliminary results. Section 2 deals with the decomposition of an arbitrary polynomial $x^{2^n} - a$ in irreducible factors over a field K of the second

[1] Supported by the National Scientific Fund of the Ministry of Education, Science and Technologies of Bulgaria under Contract MM431/94

kind with respect to 2. In Section 3 we find the explicit form of the minimal idempotents of the twisted group algebra $K^t\langle g\rangle$ of an arbitrary cyclic 2-group $\langle g\rangle$ over a field K of the second kind with respect to 2.

1. Notations, definitions and preliminary results

Let p be a prime, K be a field of characteristic different from p and $\bar{K}$ be the algebraic closure of K. We denote by ε_n a p^n-th primitive root of 1 in $\bar{K}$. The field K is called a field of the first kind with respect to p [5, p. 684], if $K(\varepsilon_i) \neq K(\varepsilon_2)$ for some $i > 2$. Otherwise, K is called a field of the second kind with respect to p. An equivalent definition is the following. If the Sylow p-subgroup $K(\varepsilon_2)_p$ of the multiplicative group $K(\varepsilon_2)^*$ is cyclic, then K is of the first kind with respect to p and if $K(\varepsilon_2)_p$ is the quasicyclic group $\mathbb{Z}(p^\infty)$ then K is a field of the second kind with resect to p. Typical examples of fields of the first and of the second kind with respect to any prime p are $\mathbb{Q}$ and $\mathbb{R}$, respectively. Let K^* be the multiplicative group of K and let G be a multiplicative group. A twisted group algebra K^tG of G over K [5, p. 13] is an associative K-algebra with basis $\{\bar{x} \mid x \in G\}$ and with multiplication defined on the basis by

$$\bar{x}\bar{y} = \gamma(x,y)\overline{xy},\ \gamma(x,y) \in K^*.$$

We denote by KG the ordinary group algebra of G over K. It is well known that if $G = \langle g\rangle$ is a cyclic group then $K^t\langle g\rangle$ is a commutatitve algebra. If the group $\langle g\rangle$ is of order n, then $\bar{g}^n = a$ for some $a \in K^*$. Obviously this equality determines the twisted group algebra $K^t\langle g\rangle$. We define

$$K^n = \{a^n \mid a \in K\},\ n \in \mathbb{N}.$$

Clearly K^n is closed with respect to the multiplication and especially $K^{p^n} \supseteq K^{p^{n+1}}$.

The following definition is well known [6, §44, p. 142].

Definition 1.1. Let α belong to the finite extension L of the field K and let $f(x) = x^n + a_1x^{n-1} + \ldots + a_n$ be the minimal polynomial of α over K. The element

$$N(\alpha) = (-1)^n a_n^{(L:K)/n}$$

is called the norm of α (in L over K).

Clearly, $N(\alpha) = (\alpha_1 \ldots \alpha_n)^{(L:K)/n}$, where $\alpha_1, \ldots, \alpha_n$ are the zeros of the polynomial $f(x)$, i.e. all the conjugate elements of α over K. It is well known that $N(\alpha\beta) = N(\alpha)N(\beta)$ for $\alpha, \beta \in L$ and if $a \in K$ then $N(a) = a^{(L:K)}$.

In order to demonstrate that some special binomials are indecomposable over the field K, we mention the following theorem.

Theorem 1.2 ([2], Th. 16.6, p. 225) *The binomial $x^n - a$, $a \in K$, is irreducible over K if and only if $a \notin K^p$ for all primes p dividing n and $a \notin -4K^4$ whenever $4|n$.*

Throughout this paper, the base field K is of the second kind with respect to 2 and of characteristic different from 2. If $a \in K$ and n is a fixed positive integer, then we denote by $H_n(a)$ the greatest integer s in the interval $[0,n]$ such that $a \in K(\varepsilon_2)^{2^s}$. As usually we assume that 0 and 1 are the trivial idempotents of an algebra.

2. Decomposition of special binomials over a field in irreducible factors

If it is not explicitly stated, in this section we assume that $K \neq K(\varepsilon_2)$, i.e. $-1 \notin K^2$.

Lemma 2.1. *For every $n \geq 2$ the only conjugated over K element $\bar{\varepsilon}_n$ of ε_n is ε_n^{-1}.*

Proof. Since ε_n is a root of the equation $x^{2^{n-1}} + 1 = 0$ over K, we obtain that $\bar{\varepsilon}_n$ is a root of the same equation. Hence $\bar{\varepsilon}_n \in \langle\varepsilon_n\rangle$ and $\varepsilon_n\bar{\varepsilon}_n \in K \cap \langle\varepsilon_n\rangle = \{-1,1\}$, i.e. $\bar{\varepsilon}_n = t\varepsilon_n^{-1}$, where $t \in \{-1,1\}$. Besides

$$\varepsilon_n + \varepsilon_n^{-1} = (\varepsilon_{n+1} + t\varepsilon_{n+1}^{-1})^2 - 2t = (\varepsilon_{n+1} + \bar{\varepsilon}_{n+1})^2 - 2t \in K.$$

Therefore $\varepsilon_n + \varepsilon_n^{-1} \in K$ and $\varepsilon_n\varepsilon_n^{-1} = 1 \in K$, which shows that $\bar{\varepsilon}_n = \varepsilon_n^{-1}$.

Lemma 2.2. *Let $\alpha \in K(\varepsilon_2)$. Then the following conditions are equivalent.*

(i) $\alpha \in K$;
(ii) $\bar{\alpha} = \alpha$, where $\bar{\alpha}$ is the conjugated of α;
(iii) $N(\alpha) = \alpha^2$.

Proof. The equivalence of (i) and (ii) is obvious. The equivalence of (ii) and (iii) follows from the equality $\alpha^2 = N(\alpha) = \alpha\bar{\alpha}$.

Lemma 2.3. *The polynomial $f(x) = x^{2^n} - a$, $a \in K$, $n \geq 2$, is irreducible over K if and only if $a \notin K^2 \cup (-K^4)$.*

Really since $4 = (\varepsilon_3 + \varepsilon_3^{-1})^4 = (\varepsilon_3 + \bar{\varepsilon}_3)^4 \in K^4$, then $4K^4 = K^4$. Then the proof of the lemma follows from Theorem 1.2.

Lemma 2.4. *Let $\alpha \in K(\varepsilon_2)$. Then $\alpha^{2^n} \in K$ if and only if $\alpha = a\varepsilon_{n+1}^l$, $a \in K$, $l \in \mathbb{Z}$.*

Proof. Let $\alpha^{2^n} \in K$. By Lemma 2.2 we see that $(N(\alpha))^{2^n} = N(\alpha^{2^n}) = \alpha^{2^{n+1}}$. Therefore we obtain $N(\alpha) = \alpha^2\varepsilon_n^{-l} = (\alpha\varepsilon_{n+1}^{-l})^2$ for some $l \in \mathbb{Z}$. On the other hand, by Lemma 2.1 we have that $N(\varepsilon_{n+1}^{-l}) = 1$. Hence $N(\alpha\varepsilon_{n+1}^{-l}) = N(\alpha) = (\alpha\varepsilon_{n+1}^{-l})^2$ and by Lemma 2.2 it follows that $\alpha\varepsilon_{n+1}^{-l} \in K$, i.e. $\alpha = a\varepsilon_{n+1}^{l}$. The inverse statement of the lemma is obvious.

Lemma 2.5. *For every $n \in \mathbb{N}$ it holds*

$$K \cap K(\varepsilon_2)^{2^n} = K^{2^n} \cup (-K^{2^n}).$$

Proof. Let $u \in K \cap K(\varepsilon_2)^{2^n}$. Then $u = \alpha^{2^n}$, $\alpha \in K(\varepsilon_2)$ and, by Lemma 2.4, $\alpha = b\varepsilon_{n+1}^{l}$, $b \in K, l \in \mathbb{Z}$. Therefore

$$u = \alpha^{2^n} = b^{2^n}(-1)^l \in K^{2^n} \cup (-K^{2^n}),$$

i.e.

$$K \cap K(\varepsilon_2)^{2^n} \subseteq K^{2^n} \cup (-K^{2^n}).$$

The opposite inclusion is obvious.

Lemma 2.6. *The equality $K^{2^n} \cap (-K^{2^m}) = 0$ holds for arbitrary $m, n \in \mathbb{N}$.*

Proof. The equality $K^2 \cap (-K^2) = 0$ follows from the fact that $\varepsilon_2 \notin K$. Moreover $K^{2^n} \cap (-K^{2^m}) \subseteq K^2 \cap (-K^2) = 0$.

Lemma 2.7. *The polynomial $f(x) = x^{2^n} - \alpha$, $\alpha \in K(\varepsilon_2)$, $n \in \mathbb{N}$, is irreducible over $K(\varepsilon_2)$ if and only if $\alpha \notin K(\varepsilon_2)^2$.*

For $n \geq 2$ the proof follows from Lemma 2.3 applied to $K(\varepsilon_2)$ bearing in mind that $-K(\varepsilon_2)^4 \subseteq K(\varepsilon_2)^2$.

For $n \geq 1$ the proof follows from Theorem 1.2 applied to the field $K(\varepsilon_2)$.

Let $a \in K^*$ and $n \in \mathbb{N}$. We denote by $H_n(a)$ the greatest integer s in the interval $[0, n]$ such that $a \in K(\varepsilon_2)^{2^s}$. Lemma 2.5 gives immediately that the integer $H_n(a)$ coincides with the greatest integer $s \in [0, n]$ such that $a \in K^{2^s} \cup (-K^{2^s})$. If $a \in K^{2^s}$, then we call the element a of *the first kind* and if $a \in -K^{2^s}$, then we call a an element of *the second kind*. Clearly the integer $H_n(a)$ always exists and is uniquely determined, by Lemma 2.6 the kind of a is also completely determined. We call the integer $H_n(a)$ the *n-height* of a in K^*.

Theorem 2.8. *Let K be a field of the second kind with respect to 2 and of characteristic different from 2, let $f(x) = x^{2^n} - a$ be a polynomial over K, $a \neq 0$, $n \in \mathbb{N}$, and let $H_n(a) = s$. Then*

1) If $K = K(\varepsilon_2)$, then

$$f(x) = \prod_{i=0}^{2^s-1} (x^{2^{n-s}} - b\varepsilon_s^i), \ a = b^{2^s}, b \in K. \tag{1}$$

and the factors of (1) are irreducible polynomials over K.

2) If $K \neq K(\varepsilon_2)$ and 2.1) $s = 0$ or 2.2) $s = 1$ and the element a is of the second kind, then $f(x)$ is irreducible over K.

In the other cases $f(x)$ is decomposed in irreducible factors over K in the following way.

3) If $K \neq K(\varepsilon_2)$, $s \geq 1$, and a is of the first kind, then

$$(2)\qquad f(x) = (x^{2^{n-s}} - b)(x^{2^{n-s}} + b) \prod_{i=1}^{2^{s-1}-1} [x^{2^{n-s+1}} - (\varepsilon_s^i + \varepsilon_s^{-i}) b x^{2^{n-s}} + b^2],$$

$a = b^{2^s}$, $b \in K$.

4) If $K \neq K(\varepsilon_2)$, $s \geq 2$, and a is of the second kind, then

$$(3)\qquad f(x) = \prod_{i=0}^{2^{s-1}-1} [x^{2^{n-s+1}} - (\varepsilon_s^i + \varepsilon_s^{-i-1})\varepsilon_{s+1} b x^{2^{n-s}} + b^2],\ a = -b^{2^s},$$

$b \in K$.

Proof. 1) Let $K = K(\varepsilon_2)$. Obviously (1) is a decomposition of $f(x)$ over K. If $s < n$, then $b\varepsilon_s^i \notin K^2$, $-K^4 \subseteq K^2$ and by Lemma 2.7 the factors of (1) are irreducible polynomials over K. The case $s = n$ is trivial.

2) Let $K \neq K(\varepsilon_2)$ and 2.1) $s = 0$ or 2.2) $s = 1$ and a is of the second kind.

If $n = 1$, then in the case 2.1) we have $a \notin K^2$ and in the case 2.2) by Lemma 2.6 we have again $a \notin K^2$. Now Theorem 1.2 gives the irreducibility of $f(x)$ over K.

Let $n \geq 2$. If $s = 0$, then $a \notin K(\varepsilon_2)^2 \supset (-K^4)$, i.e. $a \notin K^2 \cup (-K^4)$. Therefore, by Lemma 2.3, the polynomial $f(x)$ is irreducible over K. Let $s = 1$ and the element a is of the second kind. Then, by the definition of a, it follows that $a \in (-K^2)\setminus(-K^4)$ and, by Lemma 2.6, $a \notin K^2 \cup (-K^4)$. Thus, again by Lemma 2.3, $f(x)$ is irreducible over K.

3) Let $K \neq K(\varepsilon_2)$, $s \geq 1$, and let a be of the first kind. Then $a = b^{2^s}$, $b \in K$. We obtain the decomposition (1) of the polynomial $f(x)$ over $K(\varepsilon_2)$. We shall show that all the factors of $f(x)$ in (1) are irreducible over $K(\varepsilon_2)$. Really, if $s < n$, then by the definition of $H_n(a)$ we obtain that $b \notin K(\varepsilon_2)^2$ and, since $\varepsilon_s^i = \varepsilon_{s+1}^{2i} \in K(\varepsilon_2)^2$, it follows that $b\varepsilon_s^i \notin K(\varepsilon_2)^2$. Now, by Lemma 2.7 the factors in (1) are irreducible over $K(\varepsilon_2)$. For $s = n$ the factors of (1) are of the first degree and also are irreducible over $K(\varepsilon_2)$. Grouping and multiplying the conjugated over K factors in (1), by Lemma 2.1, we obtain that the factors of (2) are with coefficients from K. Their irreducibility over K follows from the irreducibility of the factors of (1) over $K(\varepsilon_2)$.

4) Let $K \neq K(\varepsilon_2)$, $s \geq 2$, and let a be of the second kind. Then $a = -b^{2^s}$, $b \in K$, and we obtain the following decomposition of the polynomial $f(x)$ over $K(\varepsilon_2)$

$$f(x) = \prod_{i=0}^{2^s-1} (x^{2^{n-s}} - b\varepsilon_{s+1}\varepsilon_s^i). \tag{4}$$

As in the case 3) we see that (4) is a decomposition of $f(x)$ in irreducible factors over $K(\varepsilon_2)$ and (4), in view of Lemma 2.1, gives the decomposition (3) of $f(x)$ in irreducible factors over K.

3. Minimal idempotents of twisted group algebras of cyclic 2-groups

Theorem 3.1. *Let K be a field of the second kind with respect to 2 and of characteristic different from 2 and let $\langle g\rangle$ be a cyclic group of order 2^n. Let the twisted group algebra $K^t\langle g\rangle$ be defined by the equality $\bar{g}^{2^n} = a$, $a \in K^*$, and let $H_n(a) = s$. Then the minimal idempotents e_i and f_k of $K^t\langle g\rangle$ are the following.*

1) If $K = K(\varepsilon_2)$, then

$$e_i = \frac{1}{2^s}\sum_{j=0}^{2^s-1} \varepsilon_s^{-ij} b^{-j}\bar{g}^{2^{n-s}j},\ i = 0, 1, \ldots, 2^s - 1, \tag{1}$$

where $b^{2^s} = a$, $b \in K$.

2) If $K \neq K(\varepsilon_2)$ and 2.1) $s = 0$ or 2.2) $s = 1$ and the element a is of the second kind then the only minimal idempotent of $K^t\langle g\rangle$ is the unity.

3) If $K \neq K(\varepsilon_2)$, $s \geq 1$, and a is of the first kind then

$$\begin{aligned} f_k &= \frac{1}{2^s}\sum_{j=0}^{2^s-1} \delta_{kj} b^{-j}\bar{g}^{2^{n-s}j},\ k = 1, 2;\ \delta_{1j} = 1,\ \delta_{2j} = (-1)^j, \\ e_i &= \frac{1}{2^s}\sum_{j=0}^{2^s-1} (\varepsilon_s^{ij} + \varepsilon_s^{-ij}) b^{-j}\bar{g}^{2^{n-s}j},\ i = 1, 2, \ldots, 2^{s-1} - 1, \end{aligned} \tag{2}$$

where $b^{2^s} = a$, $b \in K$.

4) If $K \neq K(\varepsilon_2)$, $s \geq 2$, and a is of the second kind then

$$e_i = \frac{1}{2^s}\sum_{j=0}^{2^s-1} (\varepsilon_s^{ij+j} + \varepsilon_s^{-ij})\varepsilon_{s+1}^{-j} b^{-j}\bar{g}^{2^{n-s}j},\ i = 0, 1, \ldots, 2^{s-1} - 1, \tag{3}$$

where $-b^{2^s} = a$, $b \in K$.

Proof. Let L be the splitting field of the polynomial $f(x) = x^{2^n} - a$ over K. It is well known, that the minimal idempotents of the group algebra $L\langle g\rangle$ are

$$e_\beta = \frac{1}{2^n}\sum_{i=0}^{2^n-1} \beta^{-i} g^i, \tag{4}$$

where β runs on the zeros of the polynomial $x^{2^n} - 1$. Since L is a splitting field of the polynomial $f(x)$, then there exists $\gamma \in L$, such that $\gamma^{2^n} = a$. Then the equality $\bar{g}^{2^n} = a$ implies $(\gamma^{-1}\bar{g})^{2^n} = 1$ and therefore the cyclic group $\langle\gamma^{-1}\bar{g}\rangle$ is a group basis of the twisted group algebra $L^t\langle g\rangle$, i.e. $L^t\langle g\rangle$ coincides with the group algebra $L\langle\gamma^{-1}\bar{g}\rangle$. Hence the minimal idempotents of $L^t\langle g\rangle$ are obtained from (4) by replacing g with $\gamma^{-1}\bar{g}$. So we obtain that the minimal idempotents of $L^t\langle g\rangle$ will be of the form

$$e_\beta = \frac{1}{2^n}\sum_{i=0}^{2^n-1} (\beta\gamma)^{-i}\bar{g}^i,$$

When β runs on the zeros of $x^{2^n} - 1$, $\beta\gamma$ will run on the zeros of $f(x)$. Therefore we can set $\beta\gamma = \alpha$ and the minimal idempotents of the twisted group algebra $L^t\langle g\rangle$ will be of the form

$$e_\alpha = \frac{1}{2^n}\sum_{j=0}^{2^n-1} \alpha^{-j}\bar{g}^j,$$

where α runs on the zeros of $f(x)$. From here we shall obtain the minimal idempotents of $K(\varepsilon_2)^t\langle g\rangle$ summing the minimal idempotents e_α, where α runs on the zeros of an arbitrary fixed irreducible factor of $f(x)$ over $K(\varepsilon_2)$. By Theorem 2.8 the irreducible factors of $f(x)$ over $K(\varepsilon_2)$ are of the form $\varphi_i(x) = x^{2^{n-s}} - \lambda\varepsilon_s^i$, $i = 0, 1, \ldots, 2^s - 1$, where $\lambda^{2^s} = a$, $\lambda \in K(\varepsilon_2)$. Let $\mu^{2^{n-s}} = \lambda$, $\mu \in L$. The zeros of $\varphi_i(x)$ are $\mu\varepsilon_n^i\varepsilon_{n-s}^r$, $r = 0, 1, \ldots, 2^{n-s} - 1$, and the idempotents e_i of $K(\varepsilon_2)^t\langle g\rangle$ are

$$e_i = \frac{1}{2^n}\sum_{j=0}^{2^n-1}\left(\sum_{r=0}^{2^{n-s}-1} \varepsilon_{n-s}^{-rj}\right)\mu^{-j}\varepsilon_n^{-ij}\bar{g}^j.$$

For a fixed j not divisible by 2^{n-s} the sum in the brackets is equal to zero. Therefore if we replace j by $j2^{n-s}$, $j = 0, 1, \ldots, 2^{n-s} - 1$, we shall obtain

$$e_i = \frac{1}{2^s}\sum_{j=0}^{2^s-1} \varepsilon_s^{-ij}\lambda^{-j}\bar{g}^{j2^{n-s}},\ i = 0, 1, \ldots, 2^s - 1. \tag{5}$$

Now in the case 1) for $K = K(\varepsilon_2)$ we assume $\lambda = b \in K$ and obtain the formula (1). The case 2) is clear because in this case $f(x)$ is irreducible over K. In the case 3) we have again $\lambda = b \in K$ and $e_0 = f_1 \in K^tG$, $e_{2^s-1} = f_2 \in K^tG$. The other idempotents in this case are obtained from (5) summing the pairs of conjugates over$K$. In this way the formula (2) is completely established. In the case 4) by Lemma 2.4 we have $\lambda = b\varepsilon_{s+1}$, $b \in K$. The minimal idempotents in this case are also obtained from (5) summing the pairs of conjugates over K and this gives the formula (3).

As a consequence of Theorem 3.1 one can obtain the minimal idempotents of the factor-algebra $K[x]/I$, where I is the ideal of the algebra $K[x]$ generated by the polynomial $x^{2^n} - a$, $a \in K^*$. They are obtained from the idempotents from Theorem 3.1 assuming that $\bar{g} = x + I$.

We shall note that when $\langle g \rangle$ is a cyclic 2-group and K is a field of the first kind with respect to 2 then the problem of finding the explicit form of the minimal idempotents of the twisted group algebra $K^t\langle g \rangle$ is open because of the serious problems that arrise with the decompositions of the polynomials $x^{2^n} - a$ into irreducible factors over the field K.

References

[1] A. A. B o v d i. Crossed products of semigroups and rings, *Sib. Mat. Zh.* **4**, 1963, 481-500 (In Russian).

[2] Gr. K a r p i l o v s k y. *Field Theory*, Marcel Dekker, Inc., N. York and Basel, 1988.

[3] N. A. N a c h e v, T. Zh. M o l l o v. Minimal idempotents of semisimple twisted group algebras of cyclic p-group of odd order (In Russian), *Publ. Math., Debrecen* **35**, 1988, 309-319.

[4] D. S. P a s s m a n. On the semisimplicity of twisted group algebras, *Proc. Amer. Math. Soc.* **25**, 1970, 161-166.

[5] D. S. P a s s m a n. *The Algebraic Structure of Group Rings*, Wiley-Interscience Publ., John Wiley and Sons, Inc., 1972.

[6] B. L. V a n d e r W a e r d e n. *Algebra*, I, Sechste Auflage der Modernen Algebra, Springer-Verlag, Berlin-Göttingen-Heidelberg, 1964.

Department of Algebra
University of Plovdiv
4000 Plovdiv, BULGARIA

Received: 20.12.1996