On the left ideals of a crossed group algebra over finite fields

By Z. M. ABD EL MONEIM (Debrecen)

Dedicated to Professor Zoltán Daróczy on his 50 th birthday

Let G be an arbitrary group containing an infinite cyclic subgroup of finite index, K a fixed finite field with characteristic $P(\neq 2)$, and D an arbitrary finite extension field over K, $(D:K)=n$.

S. D. BERMAN and K. BUZÁSI proved (see [1]) that the investigation of finitely generated $K\,G$-modules can be reduced to the study of finitely generated modules over so-called algebras of type E over K.

All the algebras A of type E over the finite field K were described in [2]. It was shown that the algebra

$$(1) \qquad A=[D,a,b]; \quad a\lambda=\lambda a; \quad b\lambda=\lambda b; \quad b^{-1}ab=a^{-1}; \quad b^2=\xi,$$

where $\lambda\in D$, ξ is not a square, $\xi\in D^*$, contains no zero divisors. All the other algebras of type E over K are either rings of principal ideals or contain zero divisors. For the case of the real field R K. BUZÁSI asked the question: "Is the algebra (1) a principal left ideal ring?" (see [4]). If the answer is positive, then by results of S. D. BERMAN and K. BUZÁSI [1] and by classical results on the modules over principal ideal rings the modules over all the algebras of type E can be considered to be finished. K. BUZÁSI has shown that in the case of the real field R the question mentioned above has a negative answer (see [4]). In this paper we shall shown that the algebra A defined above is not a ring of principal left ideals.

§ 1. Preliminary results

Throughout this paper let A denote the algebra defined by (1). Let $D(a)<A$ be the group algebra of the infinite cyclic group (a) over D. There was defined in [3] for every $f(a)\in D(a), f(a)\neq 0$ a norm

$$f(a)=|(\lambda_n a^n+\ldots+\lambda_m a^m)|=n-m(\lambda_i\in D;\ n\geqq m,\ n,m\in Z)$$

and it was shown that $D(a)$ is a Euclidean ring with respect to this norm.

The element $f(a)\in D(a)$ is called symmetric if $\overline{f(a)}=\mu a^{-m}f(a)$ for some $m\in Z$ and $\mu\in D$, where $\overline{f(a)}=f(a^{-1})$.

It is proved in [3] that

Lemma 1.1. *Let* $f(a), g(a) \in D(a), f(a) \neq 0$ *and* $|f(a)| \geqq |g(a)|$, *then there exist elements* $h(a), r(a) \in D(a)$ *such that*

$$f(a) = g(a) \cdot h(a) + r(a),$$

where $r(a)=0$, *or* $|r(a)| < |g(a)|$ *and*

$$|f(a)| = |g(a) \cdot h(a)|.$$

Lemma 1.2. *Let* $I \leqq A$ *be a left ideal generated by elements* P *and* $1+qb$, *where* $P, q \in D(a)$ *and* P *is the generator element of the ideal* $I \cap D(a)$. *Then* P *is a symmetric element.*

Lemma 1.3. *Every left ideal* I *of the algebra* A *can be generated by the elements* P, $S_0+S_1 b$, *where* p, $S_0, S_1 \in D(a)$, P *is a symmetric element and generates the ideal* $I \cap D(a)$.

Lemma 1.4. *Let the left ideal* $I \leqq A$ *be generated by elements* P, $S_0+S_1 b$, *where* P, $S_0, S_1 \in D(a)$, $(P) = I \cap D(a)$. *If either* $(P, S_0)=1$ *or* $(P, \overline{S_1})=1$, *then there exists an element* $q \in D(a)$ *such that the left ideal* I *can be generated by the elements* P, $1+qb$.

Theorem 1.1. *Every left ideal* $I \leqq A$ *can be expressed in the form*

$$I = I_1 \cdot d,$$

where I_1 *is a left ideal generated by elements* P, $1+qb$, $p, q \in D(a)$; $(P) = I_1 \cap D(a)$ *and* $d \in D(a)$.

§ 2. Construction of a left ideal being not a principal left ideal

We define for the element $x = \alpha + \beta b$; $\alpha, \beta \in D(a)$ of A a norm $N(x)$ by the formula

$$N(x) = (\alpha+\beta b)(\bar{\alpha} - \beta b) = \alpha \cdot \bar{\alpha} - \xi \beta \cdot \bar{\beta}.$$

It is easy to see that $N(x) \in I \cap D(a)$ and $N(x \cdot y) = N(x) \cdot N(y)$, for all the $x, y \in A$.

Lemma 2.1. *Let* $I \leqq A$ *be a principal left ideal generated by the element* $S_0 + S_1 b$, $S_0, S_1 \in D(a)$. *If* $(P) = I \cap D(a)$, *then the elements* dP *and* $N(S_0+S_1 b)$ *are associates, where* $(\overline{S_0}, S_1) = d$.

PROOF. First, let $(\bar{S}_0, S_1) = 1$. We have

$$P = (\lambda_0 + \lambda_1 b)(S_0 + S_1 b), \tag{2}$$

for some $\lambda_0 + \lambda_1 b \in A$.

This implies

$$P = \lambda_0 \cdot S_0 + \xi \lambda_1 \overline{S_1}$$

$$0 = (\lambda_0 S_1 + \lambda_1 \cdot \overline{S_0}). \tag{3}$$

Because of $(\overline{S_0}, S_1)=1$, it follows from the second equality of (3) that $\lambda_0=t\cdot\overline{S_0}$, $\lambda_1=-t\cdot S_1$ $(t\in D(a))$. Then (3) implies $P=t(S_0\cdot\overline{S_0}-\xi S_1\cdot\overline{S_1})$, that is

$$P\equiv 0 \pmod{N(S_0+S_1 b)}.$$

On the other hand, $N(S_0+S_1b)\in I\cap D(a)$, so $N(S_0+S_1b)\equiv 0 (\operatorname{mod} P)$, that is P and $N(S_0+S_1b)$ are associates.

Now let

$$(4)\qquad (\bar{S}_0, S_1)=d\neq 1;\quad \bar{S}_0=\bar{h}_0 d;\quad S_1=h_1 d\quad (h_0, h_1\in D(a);\ (h_0, h_1)=1).$$

In the case $S_0+S_1b=(h_0\bar{d}+h_1 b\bar{d})=(h_0+h_1b)\bar{d}$, we have $I=I_1\cdot\bar{d}$, where I_1 is a principal left ideal generated by h_0+h_1b. Here $(h_0, h_1)=1$, and if $(P_1)=I_1\cap D(a)$, then P_1 and $N(h_0+h_1b)$ are associates. It holds, at the same time, that

$$P=P_1\bar{d},\quad \text{and so}\quad P\cdot d=P_1\bar{d}\cdot d$$

and

$$N(S_0+S_1 b)=S_0\cdot\overline{S_0}-\xi S_1\cdot\overline{S_1}=(h_0\cdot\bar{h}_0-\xi h_1\cdot\bar{h}_1)d\cdot\bar{d}=N(h_0+h_1 b)d\cdot\bar{d}$$

are associates, too.

Lemma 2.2. *Let $I\leqq A$ be a left ideal generated by the elements P, $1+qb$, where $(P)=I\cap D(a)$, $q\in D(a)$. Then every element of I can be expressed in the form*

$$xbp+y(1+qb),\quad \textit{where}\quad x, y\in D(a).$$

Proof. Let $S_0+S_1b\in I$ be an arbitrary element of I.

$$(5)\qquad s_0+s_1 b-s_0(1+qb)=(s_1-s_0 q)b\in I,$$

that is

$$b(s_1-s_0q)b=\xi(\bar{s}_1-\bar{s}_0\cdot\bar{q})\in I-D(a).$$

Since $(p)=I\cap D(a)$, one has

$$\bar{s}_1-\bar{s}_0\cdot\bar{q}=p\cdot\bar{x}\quad \text{for some}\quad \bar{x}\in D(a).$$

This implies $s_1-s_0\cdot q=p\cdot x$ $(x\in D(a))$, because by Lemma 1.2 the element p is symmetric. By (5) we have

$$xbp+s_0(1+qb)=s_0+s_1 b,$$

which proves the lemma.

Theorem 2.1. *The algebra A is not a ring of principal left ideals.*

Proof. Let A, B be algebras given by the relations

$$A=\{D, a, b\};\quad \lambda a=a\lambda;\quad \lambda b=b\lambda;\quad b^{-1}ab=a^{-1},\quad b^2=\xi,\quad (\lambda\in D)$$

$$B=\{D, a, b\};\quad \lambda a=a\lambda;\quad \lambda b=b\lambda;\quad b^{-1}ab=a^{-1},\quad b^2=\eta$$

where $\xi, \eta\in D^*$ are non-square elements, then A and B are isomorphic. Indeed, let $|K|=p^m$, where p is a prime, $(D:K)=n$, and let θ be a primitive element of D^*. Then $\xi=\theta^{2s+1}$ and $\eta=\theta^{2t+1}$ for some $s, t\in Z$. The element $\xi^{-1}\cdot\eta=\theta^{2(t-s)}$ is a square, so $a \to a$, $b \to \sqrt{\xi^{-1}}\,\eta \cdot b$ gives an isomorphism $A \to B$, because $\sqrt{\xi^{-1}}\,\eta \in D$ and $(\sqrt{\xi^{-1}}\,\eta \cdot b)^2 = \xi^{-1} \cdot \eta b^2 = \xi^{-1}\eta\xi = \eta$. That is the element ξ in A can be replaced by any non-square element of D^*.

We shall construct a left ideal I generated by some element p^1, $1+qb$ which is not a principal ideal. Let $q = a^p + 1$, where p is the characteristic of the finite field, $(p, p^{nm}-1) = 1$.

In this case $\sqrt[p]{\lambda}$ has values in D^* for all the $\lambda \in D^*$, because $M = \{\mu^p | \mu \in D^*\}$ is a subgroup of D^* of index p, or 1. Since $(p, p^{nm}-1) = 1$, so the index equals 1 and $M = D^*$. Since $(p^1(a)) = I \cap D(a)$, the element $p^1(a)$ divides the element

$$N(1+qb) = 1 - \xi q \cdot \bar{q} = \big(1 - \xi(a^p+1)(a^{-p}+1)\big) =$$
$$= 1 - \xi(a^p + 2 + a^{-p}) = -\xi\big(a^p + (2-\xi^{-1}) + a^{-p}\big).$$

Consider the element

$$a^{2p} + (2-\xi^{-1})\,a^p + 1 = x^2 + (2-\xi^{-1})x + 1$$
$$x = \xi^{-1} - 2 \pm \sqrt{\xi^2 - 4\xi^{-1}}.$$

The element ξ can be chosen such that

$$\xi^{-2} - 4\xi^{-1} = \xi^{-1}(\xi^{-1} - 4)$$

is a square element, so that $x \in D$. Since $\sqrt[p]{x} = \alpha \in D$, the element

$$-\xi a^{-p}\big(a^{2p} + (2-\xi^{-1})\,a^p + 1\big)$$

can be expressed as a product

$$-\xi a^{-p}(a-\alpha)^p(a-\alpha^{-1})^p = -\xi a^{-p}(a-\alpha)(a-\alpha^{-1})(a-\alpha)^{p-1}(a-\alpha^{-1})^{p-1};$$

consider the element

$$p^1(a) = (a-\alpha)^{p-1}(a-\alpha^{-1})^{p-1} = a^{2(p-1)} + \delta_1 a^{2(p-1)-1} + \ldots + \delta_{p-2} a^{2(p-1)-(p-2)} +$$
$$+ \delta_{p-1} a^{p-1} + \delta_{p-2} a^{p-2} + \ldots + \delta_2 a^2 + \delta_1 a + 1,$$

where

$$\delta_1 = \alpha + \alpha^{-1}$$
$$\delta_2 = \alpha^2 + 1 + \alpha^{-2}$$
$$\delta_3 = \alpha^3 + \alpha + \alpha^{-1} + \alpha^{-3}$$
$$\vdots$$
$$\delta_{p-k} = \alpha^{p-k} + \alpha^{p-(k+2)} + \ldots + \alpha + \alpha^{-1} + \ldots + \alpha^{-(p-(k+2))} + \alpha^{-(p-k)},$$

if k is an even number and

$$\delta_{p-k} = \alpha^{p-k} + \alpha^{p-(k+2)} + \ldots + \alpha^2 + 1 + \alpha^{-2} + \ldots + \alpha^{-(p-(k+2))} + \alpha^{-(p-k)},$$

if k is an odd number,

$$\delta_{p-2} = \alpha^{p-2} + \alpha^{p-4} + \ldots + \alpha + \alpha^{-1} + \ldots + \alpha^{-(p-4)} + \alpha^{-(p-2)}$$
$$\delta_{p-1} = \alpha^{p-1} + \alpha^{p-3} + \ldots + \alpha^2 + 1 + \alpha^{-2} + \ldots + \alpha^{-(p-3)} + \alpha^{-(p-1)}$$

let us divide $p^1(a)$ by q

(6) $$p^1(a) = q\cdot h + r.$$

It is easy to see that

(7) $$h = a^{p-2}+\delta_1 a^{p-3}+\delta_2 a^{p-4}+\ldots+\delta_{p-2}$$

$$r = \delta_{p-1}a^{p-1}+(\delta_{p-2}-1)a^{p-2}+(\delta_{p-2}-\delta_1)a^{p-3}+(\delta_{p-4}-\delta_2)a^{p-4}+\ldots$$
$$\ldots+(\delta_2-\delta_{p-4})a^2+(\delta_1-\delta_{p-3})a+(1-\delta_{p-2}).$$

It is true in (6) that $|r|=p-1<|q|$; $|h|=p-2$. We construct an element

(8) $$u = bp^1-h(1+qb) = (qh+r)b-h(1+qb) = -h+rb\in I.$$

It holds that

$$N(U) = |(-h+rb)(-\bar{h}-rb)| = |(h\cdot\bar{h}-\xi r\cdot\bar{r})| = 2(q-1) = |p^1(a)|.$$

We show that the element u does not generate the left ideal I.

Indeed, assume that $I=(u)$, then (8) implies

(9) $$u-bp^1 = -h(1+qb).$$

Because $N(u)\in I\cap D(a)$, it holds that $N(u)\equiv 0(\text{mod } p^1(a))$. However, $|N(u)|=|p^1(a)|$, so the elements $N(u)$ and $p^1(a)$ are associates.

It can be assumed that $p^1(a)=N(u)$. This means that

$$p^1(a) = (-\bar{h}-rb)(-h+rb).$$

Then (9) implies

(10) $$u-b(-\bar{h}-rb)u = -h(1+qb).$$

Since $I=(u)$, there exists an element $\mu_0+\mu_1 b\in A$ such that

$$1+qb = (\mu_0+\mu_1 b)u.$$

Then (10) can be expressed in the form

$$[1-b(-\bar{h}-rb)]u = -h(\mu_0+\mu_1 b)u.$$

But the algebra A contains no zero divisors, so we have

$$1+b\bar{h}+brb = -h\mu_0-\mu_1 hb$$

$$1+hb+\xi\bar{r} = -h\mu_0-\mu_1 hb,$$

or

$$1+\xi\bar{r} = -h\mu_0,$$

that is

(11) $$1+\xi\bar{r}\equiv 0 \ (\text{mod } h).$$

We show that the congruence (11) gives rise to a contradiction. Indeed, applying (7) we have

$$1+\xi\bar{r} = \xi(\xi^{-1}+\bar{r}) = \xi[\delta_{p-1}a^{-(p-1)}+(\delta_{p-2}-1)a^{-(p-2)}+\ldots+(\delta_1-\delta_{p-3})a^{-1}+$$
$$+(1+\xi^{-1}-\delta_{p-2})] = \xi a^{-(p-1)}[(1+\xi^{-1}-\delta_{p-2})a^{p-1}+\ldots+(\delta_1-\delta_{p-3})a^{p-2}+\ldots$$
$$\ldots+(\delta_{p-3}-\delta_1)a^2+(\delta_{p-2}-1)a+\delta_{p-1}] = \xi a^{-(p-1)}\cdot g(a).$$

It is clear that h divides the element $1+\xi\bar{r}$ if and only if $h(a)$ divides $g(a)$. But $|h|=p-2$; $|r|=p-1$, and so

$$h(a)[(1+\xi^{-1}-\delta_{p-2})a+\beta] = g(a), \tag{12}$$

for some $\beta\in D$.

It follows from this equation for the coefficients of the two sides of (12) that

$$\beta+\delta_1(1+\xi^{-1}-\delta_{p-2}) = \delta_1-\delta_{p-3}, \tag{13}$$

$$\beta\cdot\delta_1+\delta_2(1+\xi^{-1}-\delta_{p-2}) = \delta_2-\delta_{p-4}; \tag{14}$$

equation (13) implies

$$\beta = \delta_1\delta_{p-2}-\delta_1\xi^{-1}-\delta_{p-3}.$$

Now we obtain from (14) that

$$[\delta_1\cdot\delta_{p-2}-\delta_1\xi^{-1}-\delta_{p-3}]\cdot\delta_1+\delta_2(\xi^{-1}-\delta_{p-2}) = -\delta_{p-4}$$
$$\delta_1^2\cdot\delta_{p-2}-\delta_1^2\xi^{-1}-\delta_1\delta_{p-3}+\delta_2\xi^{-1}-\delta_2\delta_{p-2} = -\delta_{p-4}$$
$$(\delta_1^2-\delta_2)\delta_{p-2}-(\delta_1^2-\delta_2)\xi^{-1} = \delta_1\delta_{p-3}-\delta_{p-4}$$
$$(\delta_1^2-\delta_2)(\delta_{p-2}-\xi^{-1}) = \delta_1\delta_{p-3}-\delta_{p-4}$$

that is

$$[(\alpha+\alpha^{-1})^2-(\alpha^2+1+\alpha^{-2})][\delta_{p-2}-\xi^{-1}] = \delta_1\cdot\delta_{p-3}-\delta_{p-4}.$$
$$\alpha^{p-2}+\alpha^{p-4}+\ldots+\alpha+\alpha^{-1}+\ldots+\alpha^{-(p-4)}+\alpha^{-(p-2)}-\xi^{-1} =$$
$$= (\alpha+\alpha^{-1})[\alpha^{p-3}+\alpha^{p-5}+\ldots+\alpha^2+1+\alpha^{-2}+\ldots+\alpha^{-(p-5)}+\alpha^{-(p-3)}]-$$
$$-[\alpha^{p-4}+\alpha^{p-6}+\ldots+\alpha+\alpha^{-1}+\ldots+\alpha^{-(p-6)}+\alpha^{-(p-4)}];$$
$$\alpha^{p-2}+2\delta_{p-4}+\alpha^{-(p-2)}-\xi^{-1} = \alpha^{p-2}+\alpha^{p-4}+\ldots+\alpha^3+\alpha+\alpha^{-1}+\ldots+\alpha^{-(p-6)}+$$
$$+\alpha^{-(p-4)}+\alpha^{p-4}+\alpha^{p-6}+\ldots+\alpha+\alpha^{-1}+\alpha^{-3}+\ldots+\alpha^{-(p-4)}+\alpha^{-(p-2)}$$

so

$$\alpha^{p-2}+2\delta_{p-4}+\alpha^{-(p-2)}-\xi^{-1} = \alpha^{p-2}+2\delta_{p-4}+\alpha^{-(p-2)},$$

and

$$-\xi^{-1} = 0, \quad \text{a contradiction.}$$

This proves that the element $u=-h+rb$ does not generate the left ideal I.

Now let us assume that I is a principal left ideal generated by an element $z=s_0+$ $+s_1b$. Then it holds that

$$u = -h+rb = (\lambda_0+\lambda_1 b)(s_0+s_1 b) \tag{15}$$

for some element $\lambda_0+\lambda_1 b\in A$. (15) implies the equation

$$N(u) = N(\lambda_0+\lambda_1 b)\cdot N(Z), \tag{16}$$

that is the element $N(z)$ divides $N(u)$. On the other hand, $N(z)\in I\cap D(a)=(P^1(a))$ that is $N(z)=m\cdot p^1(a)$ for some $m\in D(a)$. Then it follows from (16) that

$$N(u) = N(\lambda_0+\lambda_1 b)\cdot m\cdot p^1(a).$$

Assuming that $N(u)=n\cdot p^1(a)$ for some $n\in D(a)$, we obtain that $\lambda_0+\lambda_1 b$ is an invertible element.

By (15) this implies that the elements u and z are associates. This is in contradiction with the fact that the element u does not generate the left ideal.

References

[1] S. D. Berman and K. Buzási, On the modules over group algebras of groups containing infinite cyclic subgroup of finite index. *Studia Sci. Math. Hungarica*, **16** (1981), 455—470.

[2] K. Buzási, T. Krausz and Z. M. Abd-El-Moneim, Description of crossed group algebras over finite fields. *Acta Sci. Math. Szeged. (To appear.)*

[3] E. Szabó, Investigation in a crossed group algebra. *Publ. Math. Debrecen. (To appear.)*

[4] K. Buzási, On the structure of a real crossed group algebra. *Bull. of the Australian Math. Soc. (To appear.)*

(Received February 15, 1988)