Investigations in a crossed group algebra over a finite field

By E. SZABÓ (Debrecen)

Dedicated to Professor Zoltán Daróczy on his 50th birthday

S. D. BERMAN and K. BUZÁSI have started to investigate the representations of a group G which contains an infinite cyclic subgroup with finite index. In [4] they showed that if K is an algebraically closed field such that the group algebra KG is semisimple then we can reduce the investigation of the finitely generated KG-modules to the investigation of finitely generated modules over the algebras of type E. For the real field they have described all the algebras of type E, and for every algebra of type E the finite-dimensional finitely generated modules and the finitely generated torsion-free modules which contain a zero-divisor. For two algebras of type E over the real field they showed that these algebras have no zero-divisor and so it is not possible to investigate the finitely generated torsion-free modules over these algebras in the way mentioned above. It is a very important question whether these algebras are left principal-ideal-rings or not. If they are left principal-ideal-rings the description of the modules follows from classical results. Otherwise the description of the above-mentioned modules requires new arguments.

K. BUZÁSI, T. KRAUSZ, and Z. M. MONEIM began to investigate the algebras of type E over finite fields. They described [5] all the algebras of type E over the field L where K is a finite field $K\subseteqq L$ and $(L:K)=2$. In this case there is only one algebra of type E which does not contain zero-divisors. This crossed group algebra A is defined by the relations

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

where ξ is a fixed element of L, a quadratic non-remainder.

To describe the representations of the group G over finite fields it is necessary to study the algebra A.

In this paper we shall investigate the algebra A.

It is easy to show that the subring $L(a)$ in the algebra A $(L(a)$ is a groupalgebra of an infinite cyclic group over $L)$ is an Euclidean ring where we define the Euclidean norm $|f(a)|$ of an element $f(a)$ as follows:

$$|f(a)|=|\lambda_n a^n+\lambda_{n-1}a^{n-1}+\ldots+\lambda_m a^m|=n-m\quad (\lambda_i\in L,\ n\geqq m,\ n,m\in Z).$$

1.1. Lemma. *Let $f(a)$, $g(a)$ be elements of $L(a), f(a)\neq 0$, $g(a)\neq 0$. Then there* *exist* $h(a), r(a) \in L(a)$ *such that*

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

where $r(a)=0$ *or* $|g(a)| > |r(a)|$ *and if* $|f(a)| \geqq |g(a)|$, *then*

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

PROOF. *I.* To prove this lemma we first investigate the case: $f(a)=\alpha_n a^n + \ldots + \alpha_0$, $g(a)=\beta_m a^m + \ldots + \beta_0$ where $\alpha_i, \beta_j \in L$, $\alpha_0 \neq 0$, $\beta_0 \neq 0$. Then it is well-known that there exist $h_1(a)=\gamma_k a^k + \ldots + \gamma_0$ and $r_1(a)=\lambda_s a^s + \ldots + \lambda_0$ elements of $L(a)$ such that

$$f(a) = g(a) h_1(a) + r_1(a) \tag{1.1}$$

where $r_1(a)=0$ or $|r_1(a)| \leqq r_1^0(a) < g^0(a) = |g(a)|$ and if $f^0(a) \geqq g^0(a)$ then $f^0(a) = (g(a) \cdot h_1(a))^0$. Here $\psi^0(a)$ denotes the degree of the element $\psi(a)$ in the polynomial ring $L[x]$. Then

$$\alpha_0 = \beta_0 \gamma_0 + \lambda_0. \tag{1.2}$$

If $\gamma_0 \neq 0$ then $\beta_0 \cdot \gamma_0 \neq 0$ hence

$$|f(a)| = f^0(a) = (g(a) h_1(a))^0 = |g(a) h_1(a)|.$$

If $\gamma_0 = 0$ then it follows from (1.2) that $\lambda_0 = 0$. Put

$$h(a) = h_1(a) + \frac{\lambda_0}{\beta_0}.$$

Then

$$f(a) = g(a) \cdot h(a) + \left[r_1(a) - \frac{\lambda_0}{\beta_0} g(a) \right].$$

It is obvious that the constant term in the element

$$r(a) = r_1(a) - \frac{\lambda_0}{\beta_0} g(a)$$

is equal to zero, hence $|r(a)| < r^0(a)$. Considering $r_1^0(a) < g^0(a)$ we have $r^0(a) = g^0(a)$ and

$$|r(a)| < r^0(a) = g^0(a) = |g(a)|.$$

Consequently,

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

where $|r(a)| < |g(a)|$ and $|f(a)| = f^0(a) = (g(a) h(a))^0 = |g(a) h(a)|$.

II. Now we consider the general case:

$$f_1(a) = \alpha_n a^n + \alpha_{n-1} a^{n-1} + \ldots + \alpha_k a^k \qquad \alpha_k \neq 0$$

$$g_1(a) = \beta_m a^m + \beta_{m-1} a^{m-1} + \ldots + \beta_s a^s \quad \beta_s \neq 0.$$

Let $f(a) = f_1(a) \cdot a^{-k}$, $g(a) = g_1(a) a^{-s}$. According to the first part of the proof the statement is true for the elements $f(a)$ and $g(a)$. Using this fact we get that

$$f_1(a) = a^k f(a) = a^k[g(a)h(a)+r(a)] = a^s g(a)\, a^{k-s} h(a)+a^k r(a) =$$
$$= g_1(a)\, a^{k-s} h(a)+a^k r(a) = g_1(a)h_1(a)+r_1(a)$$

where $|r_1(a)|=|r(a)|<|g(a)|=|g_1(a)|$; moreover,

$$|f_1(a)| = |f(a)| = |g(a)h(a)| = |g_1(a)\cdot h_1(a)|.$$

1.1. Definition. Let $f(a)$ be an element of $L(a)$ and let $\overline{f(a)}$ denote the element $f(a^{-1})$. We say that the element $f(a)$ is symmetrical if $\overline{f(a)}=\delta a^n f(a)$ holds where $\delta\in L$.

1.2. Lemma. *Let $I\subseteq A$ be a left ideal generated by the elements p and $1+qb$, where $p, q\in L(a)$ moreover $(p)=I\cap L(a)$. Then p is a symmetrical element.*

PROOF. Since $p(1+qb)=p+pqb\in I$, it follows that $pqb=b\bar{p}\bar{q}\in I$, consequently, $\bar{p}\bar{q}\in I$. Since $\bar{p}\bar{q}\in I\cap L(a)$ and $I\cap L(a)$ is generated by p, we have

$$p|\bar{p}\bar{q}. \tag{1.3}$$

It is true that

$$(1-qb)(1+qb) = 1-qbqb = 1-\xi q\bar{q}\in I\cap L(a)$$

hence $p|1-\xi q\bar{q}$ and so $(p, \bar{q})=1$. On account of (1.3) and $(p, \bar{q})=1$ it follows that $p|\bar{p}$, consequently, there exists $s\in L(a)$ such that $\bar{p}=sp$ hence $p=\bar{s}\bar{p}=\bar{s}sp$. Since $L(a)$ has no zero-divisor, the element s must be a unit in the ring $L(a)$, consequently it can be written in the form $s=\delta a^n$.

Hence $\bar{p}=\delta a^n\cdot p$ i.e. p is a symmetrical element.

1.3. Lemma. *Every left ideal I in the algebra A can be generated by two elements p and $s_0+s_1 b$ where $s_0, s_1\in L(a)$ and p is the generator of the ideal $I\cap L(a)$.*

PROOF. Every element z in the algebra can be written in the form $z=\alpha+\beta b$ where $\alpha, \beta\in L(a)$. Let us denote by L_1 the following set

$$L_1 = \{l_1|l_0+l_1 b\in I,\ l_0, l_1\in L(a)\}.$$

It is easy to see that L_1 is an ideal in $L(a)$. Since $L(a)$ is an Euclidean ring it is well-known that every ideal L_1 in $L(a)$ is a principal ideal. Let us suppose that L_1 is generated by the element s_1, i. e. $L_1=(s_1)$.

Let $x_0=s_0+s_1 b$ be a fixed element in the ideal I. Let $x=l_0+l_1 b$ be an arbitrary element of I. On account of $l_1\in L_1$, there exists $t\in L(a)$ such that $l_1=ts_1$. Let us denote by p_0 the element $x-tx_0$. Then

$$x-tx_0 = (l_0+l_1 b)-t(s_0+s_1 b) = l_0-ts_0 = p_0\in I\cap L(a).$$

Let us denote by L_0 the set of elements p_0 if x is running through I:

$$L_0 = \{p_0 = x-tx_0|x\in I\}.$$

It is easy to see that L_0 is an ideal in $L(a)$ hence L_0 is a principal ideal and it can be written in the form $L_0=(p_1)$. There exists $t_0\in L(a)$ such that $p_0=t_0 p_1$ and by means of this every element x of I can be written in the form

$$x = p_0 + tx_0 = t_0 p_1 + tx_0.$$

Consequently, the ideal I is generated by the elements p_1 and $x_0 = s_0 + s_1 b$. We have $p_1 = t_1 p$ because of $p_1 \in I \cap L(a)$ where $t_1 \in L(a)$, hence I is generated by p and $s_0 + s_1 b$. This completes the proof of the lemma.

1.4. Lemma. *Let* $I \subseteq A$ *be a left ideal and*

$$I = (p, s_0 + s_1 b), \quad s_0, s_1 \in L(a) \quad \textit{where} \quad (p) = I \cap L(a).$$

If $(p, s_0) = 1$ *or* $(p, \bar{s}_1) = 1$ *then there exists* $q \in L(a)$ *such that* $I = (p, 1 + qb)$ *and* p *is a symmetrical element.*

Proof. We first observe the case $(s_0, p) = 1$. Without loss of generality we can assume that $|p| > |s_0|$. If this were not true we could write s_0 in the form

$$s_0 = ph + r \quad \text{where} \quad h, r \in L(a) \quad |p| < |r|$$

and I is generated by p and $r + s_1 b$.

Let us apply the Euclidean algorithm for p and s_0.

$$\begin{aligned} p &= s_0 h_0 + r_0 \qquad |r_0| < |s_0| \\ s_0 &= r_0 h_1 + r_1 \qquad |r_1| < |r_0| \\ r_0 &= r_1 h_2 + r_2 \\ &\vdots \\ r_{k-2} &= r_{k-1} h_k + r_k \quad |r_k| < |r_{k-1}| \\ r_{k-1} &= r_k h_{k+1} \end{aligned}$$

where $r_k = (p, s_0) = 1$.

Using this algorithm we can change the generators of I. In the first step from the first equality of the algorithm we obtain

$$p - h_0(s_0 + s_1 b) = r_0 - h_0 s_1 b = r_0 + m_0 b \quad m_0 \in L(a)$$

i.e. we can write

$$p = h_0(s_0 + s_1 b) + (r_0 + m_0 b).$$

Hence

$$I = (r_0 + m_0 b, \ s_0 + s_1 b).$$

In the second step from the second equality we obtain

$$(s_0 + s_1 b) - h_1(r_0 + m_0 b) = r_1 + (s_1 - h_1 m_0) b = r_1 + m_1 b \quad m_1 \in L(a).$$

Hence

$$I = (r_0 + m_0 b, r_1 + m_1 b).$$

Continueing the procedure, in the last step we get

$$I = (m_{k+1} b, r_k + m_k b), \quad m_k, m_{k+1} \in L(a).$$

From $m_{k+1}b=b\overline{m}_{k+1}$ we obtain $I=(\overline{m}_{k+1}, r_k+m_k b)$ and since $\overline{m}_{k+1}\in I\cap L(a)=(p)$ we have $I=(p, 1+m_k b)$. If $(p, \bar{s}_1)=1$ then we look at the element $z=\bar{s}_1+\bar{s}_0\xi^{-1}b$. Because of $s_0+s_1 b=b(\bar{s}_1+\bar{s}_0\xi^{-1}b)$, $I=(p, \bar{s}_1+s_0\xi^{-1}b)$ and we can return to the first case. Applying the Lemma 1.2 we see that p is a symmetrical element.

1.5. Lemma. *Let $I\subseteq A$ be a left ideal and $I=(p, s_0+s_1 b)$ where $s_0, s_1\in L(a)$, $(p)=I\cap L(a)$. Let us suppose that $(s_0, p)\neq 1$ and $(\bar{s}_1, p)\neq 1$. Then there exist elements d, q in $L(a)$ such that the ideal I can be written in the form $I=I_1 d$ where $I_1=(p_1, 1+qb)$ and $dp_1=p$.*

PROOF. Every element of I can be written in the form

$$x = \mu_0+\mu_1 b \quad \text{where} \quad \mu_0, \mu_1\in L(a).$$

Let the sets L_0 and L_1 are defined by

$$L_0 = \{\mu_0|\mu_0+\mu_1 b\in I,\ \mu_0, \mu_1\in L(a)\}$$

and

$$L_1 = \{\mu_1|\mu_0+\mu_1 b\in I,\ \mu_0, \mu_1\in L(a)\}.$$

It is easy to see that $L_0\subseteq L(a)$ and $L_1\subseteq L(a)$ are ideals in $L(a)$. Let us suppose that $L_0=(d)$.

From

$$bx = b(\mu_0+\mu_1 b) = \bar{\mu}_0 b+\xi\bar{\mu}_1\in I$$

and

$$\xi^{-1}bx = \xi^{-1}b(\mu_0+\mu_1 b) = \xi^{-1}\bar{\mu}_0 b+\bar{\mu}_1\in I$$

we get $\mu_0\in L_0$ if and only if $\bar{\mu}_0\in L_1$. Consequently, L_1 is generated by the element $\bar{d}$. Since $p\in L_0$ we can write $p=p_1 d$. By similar arguments as in Lemma 1.4. instead of the generator $s_0+s_1 b$ we can choose a new one in the form $d+s_1' b$ where $s_1'\in L_1$, hence $s_1'=q\bar{d}$. Using this element we can express every element y of I in the form

$$y = (\lambda_0+\lambda_1 b)p_1 d+(\lambda_0'+\lambda_1' b)(d+q\bar{d}b) = [(\lambda_0+\lambda_1 b)p_1+(\lambda_0'+\lambda_1' b)(1+qb)]\,d$$

i.e. $I=I_1 d$ where $I_1=(p_1, 1+qb)$.

1.1. Theorem. *Every left ideal I in the algebra A can be written in the form $I=I_1 d$ where $I_1=(p, 1+qb)$, $p, q, d\in L(a)$, $(p)=I_1\cap L(a)$ and p is a symmetrical element.*

PROOF. The theorem follows from the lemmas.

1.6. Lemma. *Let $I\subseteq A$ be a left ideal. Suppose that*

$$I = (p, 1+qb) \quad \text{and} \quad I = (p, 1+q_1 b), \quad q_1, p_1, q\in L(a); \quad (p) = I\cap L(a).$$

Then $q\equiv q_1 \pmod p$.

PROOF.

$$(1+qb)-(1+q_1 b) = (q-q_1)b\in I$$

hence

$$b(\bar{q}-\bar{q}_1)\in I, \quad \bar{q}-\bar{q}_1\in I\cap L(a).$$

Consequently, $p|\bar{q}-\bar{q}_1$ and $\bar{p}|q-q_1$. Considering that p is a symmetrical element, $q\equiv q_1 \pmod p$ follows. Thus the lemma is proved.

Every element in the algebra A can be written in the form

$$x = \alpha+\beta b \quad \alpha, \beta\in L(a).$$

For the elements of A we define a norm $N(x)$ in the following way:

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

It is easy to verify that $N(x)\in L(a)$ and

$$N(x\cdot y) = N(x)\cdot N(y) \quad \text{for every} \quad x, y\in A.$$

By $N(x)=(\bar{\alpha}-\beta b)(\alpha+\beta b)$, if $I\subseteq A$ is a left ideal and x is an element of I then $N(x)\in I$.

1.7. Lemma. *Let $I\subseteq A$ be a left principal ideal and s_0+s_1b, $s_0, s_1\in L(a)$ a generator of I. Moreover, $(p)=I\cap L(a)$ and $d=(\bar{s}_0, s_1)$. Then dp and $N(s_0+s_1b)$ are associated elements.*

Proof. First we investigate the case $d=(\bar{s}_0, s_1)=1$. Since $p\in I$, there exists an element $\lambda_0+\lambda_1 b\in A$ such that $p=(\lambda_0+\lambda_1 b)(s_0+s_1 b)$. Now $p\in I\cap L(a)$ implies that

$$p = \lambda_0 s_0+\xi\lambda_1\bar{s}_1$$

$$0 = \lambda_0 s_1+\lambda_1\bar{s}_0.$$

Since $(\bar{s}_0, s_1)=1$, from the second equality we get

$$\lambda_0 = t\bar{s}_0, \quad \lambda_1 = -ts_1 \quad \text{where} \quad t\in L(a).$$

Using this, from the first equality we get that

$$p = t(\bar{s}_0 s_0-\xi s_1\cdot\bar{s}_1) = tN(s_0+s_1 b)$$

and thus $N(s_0+s_1b)|p$. We know that $N(s_0+s_1b)\in I\cap L(a)$ consequently, $p|N(s_0+s_1b)$. So, p and $N(s_0+s_1b)$ are associated elements.

Now we consider the general case $(\bar{s}_0, s_1)=d$. Let us suppose that $\bar{s}_0=\bar{h}_0 d$, $s_1=h_1 d$, $\bar{h}_0, h_1\in L(a)$, then $(\bar{h}_0, h_1)=1$. By means of these elements s_0+s_1b can be written in the form $s_0+s_1b=(h_0+h_1b)\bar{d}$ and so the ideal I can be written in the form $I=I_1\bar{d}$ where I_1 is a left principal ideal generated by h_0+h_1b and $(\bar{h}_0, h_1)=1$ holds. According to the first part of the proof, if $(p_1)=I_1\cap L(a)$ then p_1 and $N(h_0+h_1b)$ are associated elements. It is true that $pd=p_1\bar{d}$. Consequently, the element $pd=p_1\bar{d}d$ and the element $N(h_0+h_1b)d\bar{d}=(h_0\bar{h}_0-\xi h_1\bar{h}_1)d\bar{d}=\bar{s}_0 s_0-\xi s_1\bar{s}_1=$ $=N(s_0+s_1b)$ are associated.

1.8. Lemma. *Let $I\subseteq A$ be a left ideal, p and $1+qb$ be the generators of I where $p, q\in L(a)$, $(p)=I\cap L(a)$. Then every element z of I can be written in the form*

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

PROOF. Let z be an arbitrary element of I, $z=(s_0+s_1b)$; $s_0, s_1\in L(a)$. Then

$$(s_0+s_1 b)-s_0(1+qb) = (s_1-s_0 q) b\in I. \tag{1.5}$$

Consequently,

$$b(\bar{s}_1-\bar{s}_0\bar{q})\in I, \quad \bar{s}_1-\bar{s}_0\bar{q}\in I-L(a).$$

Since $(p)=I\cap L(a)$ there exists an element $\bar{m}$ in $L(a)$ such that

$$\bar{s}_1-\bar{s}_0\bar{p} = p\bar{m}.$$

Then

$$s_1-s_0 p = \bar{p}m.$$

From (1.5) it follows that

$$s_0+s_1 b = mbp+s_0(1+qb)$$

which was to be proved.

References

[1] С. Д. Берман и К. Бузаши, О представлениях бесконечной группы диэрда. *Publ. Math. (Debrecen)* **28** (1981), 173—187.

[2] С. Д. Берман и К. Бузаши, О представлениях группы содержащей бесконечную циклическую подгруппу конечного индекса. *Publ. Math. (Debrecen)* **29** (1982), 163—170.

[3] С. Д. Берман и К. Бузаши, О модулях над групповами алгебрами групп содержащих бесконечную циклическую подгруппу конечного индекса. *Studia Sci. Math. Hungarica* **16** (1981), 455—470.

[4] С. Д. Берман и К. Бузаши, Описание всех конечных вещественных представлений групп, содержащих бесконечную циклическую подгруппу конечного индекса. *Publ. Math. (Debrecen)* **31** (1984), 133—144.

[5] К. Бузаши, Т. Краус и З. М. Монеим, О скрещенных групповых алгебрах над конечными полями. *Publ. Math. (Debrecen)* **33** (1986), 147—152.

(Received October 12, 1986)