ON THE STRUCTURE OF A REAL CROSSED GROUP ALGEBRA
K. BUZÁSI

The main result of this paper is that there exist non-principal left ideals in a certain twisted group algebra $A$ of the infinite dihedral group $< a, b | b^{-1}ab = a^{-1}, b^2 = 1 >$ over the field $\mathbb{R}$ of real numbers: namely in the $A$ defined by $b^{-1}ab = a^{-1}, b^2 = -1$, and $\lambda a = a\lambda, \lambda b = b\lambda$ for all real $\lambda$.

The motivation comes from the study (in a series of papers by Berman and the author) of finitely generated torsion-free $RG$-modules for groups $G$ which have an infinite cyclic subgroup of finite index. In a sense, this amounts to studying modules over (full matrix algebras over) a finite set of $\mathbb{R}$-algebras [namely, for the groups in question, these algebras take on the role played by $\mathbb{R}, C$ and $H$ (the real quaternions) in the theory of real representations of finite groups]. For all but two algebras in that finite set, satisfying results have been obtained by exploiting the fact that each of them is either a ring with zero divisors or a principal left ideal ring. The other two are known to have no zero divisors. One of them is the present $A$. The point of the main result is that new ideas will be needed for understanding $A$-modules.

A number of subsidiary results are concerned with convenient generating sets for left ideals in $A$.

0. INTRODUCTION

Let $G$ be an arbitrary group containing an infinite cyclic subgroup of finite index. Berman and the author showed (see [1]) that $G$ contains a normal subgroup $H$ such that $(G : H) = 2^\alpha (\alpha = 0, 1)$ and $H = F.(a)$, where $F$ is a finite normal subgroup in $H$ and $(a)$ the infinite cyclic group. Let $K$ be an arbitrary field with $\text{Char } K \nmid |F|$. It was proved in [1] that the investigation of finitely generated $KG$-modules can be reduced to the study of finitely generated modules over algebras of so-called type $E$ over $K$.

Berman and Buzési described in [2] all the algebras of type $E$ over the real field $\mathbb{R}$ and discussed the structure of finitely generated modules over them. It was shown that the algebras

$A = (\mathbb{R}, a, b), \lambda a = a\lambda, \lambda b = b\lambda, b^{-1}ab = a^{-1}, b^2 = -1(\lambda \in \mathbb{R}),$

$B = (\mathbb{C}, a, b), \lambda a = a\lambda, \lambda b = b\lambda, b^{-1}ab = a^{-1}, b^2 = -1(\lambda \in \mathbb{C}),$

Received 11 September 1987
Research (partially) supported by Hungarian National Foundation for Scientific Research, grant no. 1813.

Copyright Clearance Centre, Inc. Serial-fee code: 0004-9729/88 $A2.00+0.00.$
contain no zero divisors. All the other algebras of type $E$ over $R$ are either principal left ideal rings or contain zero divisors, so the investigation of the structure of finitely generated torsion-free modules over such algebras can be considered completed by applying classical results and the results of [2]. If the algebra $A$ or $B$ is not a principal left ideal ring, then the structure of finitely generated torsion-free $A$-modules needs additional investigation.

It will be shown in this paper that the algebra $A$ defined above is not a principal left ideal ring.

1. THE STRUCTURE OF LEFT IDEALS

Throughout this paper $A$ denotes the algebra defined above. It was shown in [2] that the group algebra $R(a) \subset A$ of the infinite cyclic group $(a)$ is a Euclidean ring with respect to the norm:

$$|f(a)| = |\lambda_n a^n + \cdots + \lambda_m a^m| = n - m \quad (\lambda_i \in \mathbb{R}; n \geq m; n, m \in \mathbb{Z}).$$

It is easy to see that when $f(a), g(a) \in R(a)$ and $g(a) \neq 0$, there exist $h(a)$ and $r(a) \in R(a)$ such that

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

where $r(a) = 0$ or $|g(a)| > |r(a)|$; however the elements $h(a)$ and $r(a)$ are not uniquely determined.

We write $f(a^{-1}) = \overline{f(a)}$. The element $f(a) \in R(a)$ is called symmetric if $f(a) = \mu a^{-m}f(a)$, for some $m \in \mathbb{Z}$ and $\mu \in \mathbb{R}$. The units of $R(a)$ are exactly the elements $\mu a^m$.

**Lemma 1.1.** Let $f(a)$ and $g(a) \in R(a)$ with $f(a) \neq 0$ and $|f(a)| \geq |g(a)|$. Then there exist elements $h(a)$ and $r(a) \in R(a)$ such that

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

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

**Proof:** First let $f(a) = \alpha_n a^n + \cdots + \alpha_0$ and $g(a) = \beta_m a^m + \cdots + \beta_0$, where $\alpha_i, \beta_j \in \mathbb{R}, \alpha_0 \neq 0$ and $\beta_0 \neq 0$. Then there exist elements $h_1(a) = \gamma_k a^k + \cdots + \gamma_0$ and $r_1(a) = \lambda_s a^s + \cdots + \lambda_0$ in $R(a)$ such that

$$f(a) = g(a)h_1(a) + r_1(a),$$

where $r_1(a) = 0$ or $r_1^0(a) < g^0(a)$. Here $g^0(a)$ denotes the degree of the polynomial $g(a) \in R(a)$. (1.1) implies

$$\alpha_0 = \beta \cdot \gamma_0 + \lambda_0.$$
If $\gamma_0 \neq 0$, then $|h_1(a)| = h_1^0(a)$, and since $n \geq m$,

$$|f(a)| = f^0(a) = (g(a).h_2(a))^0 = |g(a).h_2(a)|.$$ 

If $\gamma_0 = 0$, then (1.2) implies $\lambda_0 \neq 0$. Consider the element

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

Then the equation

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

holds. It is clear that the element

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

has no constant term and so $|r(a)| < r^0(a)$. Consequently, as $r_1^0(a) < g^0(a)$ it follows that $r^0(a) = g^0(a)$ and

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

So we obtain the equation

$$f(a) = g(a).h(a) + r(a),$$

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

Now let $f_1(a) = \alpha'_n a^{n_1} + \cdots + \alpha'_n a^{n_2}$ and $g_1(a) = \beta'_m a^{m_1} + \cdots + \beta'_m a^{m_2}$ with $\alpha'_1, \alpha'_2 \in \mathbb{R}; n_i, m_j \in \mathbb{Z}; n_1 \geq n_2$ and $m_1 \geq m_2$. Then $f_1(a) = a^{n_2} . f(a)$ and $g_1(a) = a^{m_2} . g(a)$, where

$$f(a) = \alpha_n a^n + \cdots + \alpha_0, \quad g(a) = \beta_m a^m + \cdots + \beta_0,$$

$$\alpha'_n = \alpha_n, \ldots, \alpha'_n = \alpha_0, \quad n = n_1 - n_2,$$

$$\beta'_m = \beta_m, \ldots, \beta'_m = \beta_0, \quad m = m_1 - m_2.$$ 

As was shown above, the equation (1.3) holds for the elements $f(a)$ and $g(a)$. Then, applying (1.3), we obtain

$$f_1(a) = a^{n_2} . f(a)$$

$$= a^{n_2} [g(a).h(a) + r(a)]$$

$$= a^{m_2} . g(a).a^{n_2 - m_2} . h(a) + a^{n_2} . r(a)$$

$$= g_1(a).a^{n_2 - m_2} . h(a) + a^{n_2} . r(a).$$

Since $|f_1(a)| = |f(a)|, |g_1(a)| = |g(a)| = g(a)$ and $|r(a)| = |a^{n_2} . r(a)|$, the inequality $|g_1(a)| > |a^{n_2} . r(a)|$ follows from $|g(a)| > |r(a)|$; consequently we obtain

$$|f_1(a)| = |f(a)| = |g(a).h(a)| = |g_1(a).a^{n_2 - m_2} . h(a)|.$$
Lemma 1.2. Let $I \subseteq A$ be a left ideal generated by elements $p$ and $1 + qb$, where $p, q \in R(a)$ and $p$ is the generator of the ideal $I \cap R(a)$. Then $p$ is a symmetric element.

Proof: Since $p(1 + qb) = p + pqb \in I$, we have $pqb \in I$. This implies that $bpq \in I$ and so $\overline{p} \overline{q} \in I \cap R(a)$. The element $p$ generates the ideal $I \cap R(a)$, so it follows that

$$\overline{p} \overline{q} \equiv 0 \pmod{p}.$$  

But

$$(1 - qb)(1 + qb) = 1 + q \overline{q} \in I \cap R(a),$$

and hence

$$1 + q \overline{q} \equiv 0 \pmod{p}.$$ 

Thus the congruence (1.4) implies that $\overline{p} \equiv 0 \pmod{p}$. Then $\overline{p} = s \overline{p}$, for an element $s \in R(a)$. Under the action of the automorphism $f \rightarrow \overline{f}$, this equation implies

$$p = \overline{s} \overline{p} = \overline{s} s \overline{p}.$$ 

As the ring $R(a)$ has no zero divisors, it follows from this equation that $s$ is a unit in $Ra$, and $p$ is a symmetric element. $lacksquare$

Lemma 1.3. Every left ideal $I$ of the algebra $A$ can be generated by elements $p$ and $s_0 + s_1 b$, where $p, s_0, s_1 \in R(a)$; here $p$ is a symmetric element and generates the ideal $I \cap R(a)$.

Proof: Every element of $A$ can be expressed by the form $\alpha + \beta b$ with $\alpha, \beta \in R(a)$. Consider the elements $x = t_0 + t_1 b$ of the left ideal $I$. As $x$ runs over $I$, the corresponding elements $t_1$ run over an ideal $L_1$ in $R(a)$. Since $R(a)$ is a principal ideal ring, $L_1 = (s_1)$ for some element $s_1 \in R(a)$. Consider a fixed element

$$x_0 = s_0 + s_1 b \in I$$

and let $x = \lambda_0 + \lambda_1 b$ be an arbitrary element of $I$. Here $\lambda_1 \in L_1$ and so $\lambda_1 = t s_1$ for some $t \in R(a)$. Consider the element

$$p_0 = x - t x_0 = (\lambda_0 + t s_1 b) - t(s_0 + s_1 b) = \lambda_0 - t s_0 \in I.$$ 

As the element $x$ runs over the $I$, the element $p_0$ runs over an ideal $L_0$ of $R(a)$. Let $L_0 = (p_1)$. Then $p_0 = t_0 p_1$ for some $t_0 \in R(a)$ and the element of $x$ can be expressed in the form

$$x = t_0 p_1 + t x_0,$$

that is the elements $p_1, x_0 + s_1 b$ generate the left ideal $I$. If $I \cap R(a) = (p)$, then $p_1 = t_1 p$ for some $t_1 \in R(a)$, and consequently $I$ can be generated by elements $p, s_0 + s_1 b$. By Lemma 1.2 the element $p$ is symmetric. $lacksquare$
LEMMA 1.4. Let the left ideal $I \subseteq A$ be generated by elements $p$ and $s_0 + s_1 b$, where $p, s_0, s_1 \in R(a)$ and $(p) = I \cap R(a)$. If either $(p, s_0) = 1$, or $(p, s_1) = 1$, then there exists an element $q \in R(a)$ such that the left ideal $I$ can be generated by elements $p$ and $1 + qb$.

PROOF: Let $(s_0, p) = 1$. It can be assumed that $|p| > |s_0|$. Indeed, if $|p| \leq |s_0|$ then $s_0 = ph + r$ for some $h, r \in R(a)$, where $r = 0$ or $|r| < |p|$. We set

$$ (s_0 + s_1 b) - hp = ph + r + s_1 b - hp = r + s_1 b, $$

and the elements $p, r + s_1 b$ generate the left ideal $I$, where $|p| > |r|$.

Applying the Euclidean algorithm to the elements $p$ and $s_0$, we obtain

\[
\begin{align*}
p &= s_0 h_0 + r_0, & |r_0| < |s_0|, \\
s_0 &= r_0 h_1 + r_1, & |r_1| < |r_0|, \\
r_0 &= r_1 h_2 + r_2, & |r_2| < |r_1|, \\
&\vdots \\
r_{k-2} &= r_{k-1} h_k + r_k, & |r_k| < |r_{k-1}|, \\
r_{k-1} &= r_k h_{k+1}.
\end{align*}
\]

We have $r_k = (p, s_0) = 1$. We use this algorithm in the following way: As the first step we form an element

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

and change the generator elements of $I$ to the generators

$$ r_0 + m_0 b, s_0 + s_1 b. $$

At the second step we form the element

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

and change the generators to

$$ r_0 + m_0 b, r_1 + m_1 b, $$

and so on. At the last step we get the generators $m_k b, 1 + m_{k+1} b \quad (m_k, m_{k+1} \in R(a))$. Since $b$ is an invertible element and $m_k \in I \cap R(a) = (p)$, we obtain the generators $p$ and $1 + qb$, where $m_{k+1} = q$.

If $(p, s_1) = 1$, then the element

$$ b(s_0 + s_1 b) = -s_1 + s_0 b $$

is also a generator, and we have the case considered above. 
\[\square\]
THEOREM 1.1. Every left ideal $I \subseteq A$ can be expressed in the form

$$I = I_1d,$$

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

PROOF: By Lemma 1.3 the left ideal $I$ can be expressed as $I = (p_1, s_0 + s_1b)$, where $p_1, s_0, s_1 \in R(a)$ and $(p_1) = I \cap R(a)$. If $(s_0, p_1) = 1$ or $(p_1, s_1) = 1$, then by Lemma 1.4 we obtain the theorem with $d = 1$.

Let us consider the set of all elements

$$x = \mu_0 + \mu_1b \quad (\mu_0, \mu_1 \in R(a))$$

of $I$. As the element $x$ runs over $I$, the corresponding elements $\mu_i$ form ideals $L_i$ in $R(a)$ $(i = 0, 1)$. Let $L_0 = (d)$. Then $L_1 = (d)$. Indeed, $bx = -\mu_1 + \bar{\mu}_0b \in I$, consequently if $\mu_0 \in L_0$ then $\mu_0 \in L_1$. Since $p_1 \in L_0$, so $p_1 = pd$ for some $p \in R(a)$. Since $L_0 = (d)$, applying the Euclidean algorithm, as in the proof of Lemma 1.4, we can replace the generator $s_0 + s_1b$ by an element $d + s'_1b$. As $s'_1 \in L_1$, it follows that $s'_1 = qd$ for some $q \in Ra$. Consequently, every element $y \in I$ can be expressed in the form

$$y = (\lambda_0 + \lambda_1b)p_1 + (\lambda'_0 + \lambda'_1b)(d + s'_1b)$$

$$= (\lambda_0 + \lambda_1b)p_1 + (\lambda'_0 + \lambda'_1b)(d + qdb)$$

$$= [(\lambda_0 + \lambda_1b)p_1 + (\lambda'_0 + \lambda'_1b)(1 + qb)]d,$$

where $\lambda_0 + \lambda_1b$ and $\lambda'_0 + \lambda'_1b \in A$. The elements

$$(\lambda_0 + \lambda_1b)p_1 + (\lambda'_0 + \lambda'_1b)(1 + qb)$$

form a left ideal $I_1$ generated by elements $p$ and $1 + qb$.

LEMMA 1.5. Let the left ideal $I \subseteq A$ be generated by two pairs of elements $p, 1 + qb$ and $p, 1 + q_1b$, where $(p) = I \cap R(a)$ and $q, q_1 \in R(a)$. Then $q \equiv q_1 (\text{mod } p)$.

PROOF: Clearly

$$(1 + qb) - (1 + q_1b) = (q - q_1)b \in I,$$

which implies $q - q_1 \in I$. But $q - q_1 \in R(a)$ and hence $q \equiv q_1 (\text{mod } q)$. Since $p$ is symmetric, the lemma follows from this congruence.
2. CONSTRUCTION OF A LEFT IDEAL WHICH IS NOT A PRINCIPAL LEFT IDEAL

For the element \( x = \alpha + \beta b(\alpha, \beta \in \mathbb{R}(a)) \) of \( A \) we define a norm \( N(x) \) by the formula
\[
N(x) = (\alpha - \beta b)(\alpha + \beta b) = \alpha, \alpha + \beta, \beta.
\]
It is easy to see that \( N(x.y) = N(x).N(y) \) for all \( x, y \in A \) and \( N(x) \in I \cap \mathbb{R}(a) \) for all \( x \in I \) where \( I \) is a left ideal of \( A \).

**Lemma 2.1.** Let \( I \subseteq A \) be a principal left ideal generated by the element \( s_0 + s_1 b \) with \( s_0, s_1 \in \mathbb{R}(a) \). If \( (p) = I \cap \mathbb{R}(a) \), then the elements \( d.p \) and \( N(s_0 + s_1 b) \) are associates, where \((s_0, s_1) = d\).

**Proof:** First let \((s_0, s_1) = 1\). We have that
\[
(2.1) \quad p = (\lambda_0 + \lambda_1 b)(s_0 + s_1 b)
\]
for some \( \lambda_0 + \lambda_1 b \in A \). This implies
\[
(2.2) \quad p = \lambda_0 s_0 - \lambda_1 s_1 \quad \text{and} \quad 0 = \lambda_0 s_1 + \lambda_1 s_0.
\]
Because \((s_0, s_1) = 1\), it follows from the second equality of (2.2) that \( \lambda_0 = t s_0 \) and \( \lambda_1 = -t s_1 (t \in \mathbb{R}(a)) \). Then (2.2) implies that \( p = t(s_0 s_0 + s_1 s_1) \), that is, \( p \equiv 0(\text{mod } N(s_0 + s_1 b)) \). On the other hand, \( N(s_0 + s_1 b) \in I \cap \mathbb{R}(a) \) and so \( N(s_0 + s_1 b) \equiv 0(\text{mod } p) \), that is, \( p \) and \( N(s_0 + s_1 b) \) are associates. Now let
\[
(2.3) \quad (s_0, s_1) = d \neq 1 \quad \text{with} \quad s_0 = \overline{h}_0 d \quad \text{and} \quad s_1 = \overline{h}_1 d \quad (h_0, h_1 \in \mathbb{R}(a)),
\]
where \((h_0, h_1) = 1\). In this case \( s_0 + s_1 b = (h_0 + h_1 b)d \), that is, \( I = I_1 d \), where \( I_1 \) is a principal left ideal generated by \( h_0 + h_1 b \). Here \((h_0, h_1) = 1\), and if \((p_1) = I_1 \cap \mathbb{R}(a)\), then \( p_1 \) and \( N(h_0 + h_1 b) \) are associates. It follows, at the same time, that \( p = p_1 d \), and so \( p.d = p_1 d.d \) and
\[
N(s_0 + s_1 b) = s_0 \overline{s}_0 + s_1 \overline{s}_1 = (h_0 \overline{h}_0 + h_1 \overline{h}_1)d.d = N(h_0 + h_1 b)d.d
\]
are associates too.

**Lemma 2.2.** Let \( I \subseteq A \) be a left ideal generated by elements \( p \) and \( 1 + qb \), where \( (p) = I \cap \mathbb{R}(a) \), \( q \in \mathbb{R}(a) \). Then every element of \( I \) can be expressed in the form \((xb)p + y(1 + qb)\), where \( x, y \in \mathbb{R}(a) \).

**Proof:** Let \( s_0 + s_1 b \in I \) be an arbitrary element of \( I \). Then
\[
(2.4) \quad s_0 + s_1 b - s_0(1 + qb) = (s_1 - s_0 q)b \in I,
\]
that is
\[
b(s_1 - s_0 q)b = -s_1 + s_0 \overline{q} \in I \cap \mathbb{R}(a).
\]
Since \((p) = I \cap \mathbb{R}(a)\), so \( \overline{s}_1 - s_0 \overline{q} = p.\overline{x} \) for some \( \overline{x} \in \mathbb{R}(a) \). This implies that \( s_1 - s_0 q = p.x(x \in \mathbb{R}(a)) \), because by Lemma 1.2, the element \( p \) is symmetric. By 2.4 we have \((xb)p + s_0(1 + qb) = s_0 + s_1 b\), which proves the lemma.
THEOREM 2.1. Algebra $A$ is not a principal left ideal ring.

PROOF: We shall construct a left ideal $I$ generated by certain elements $p, 1 + qb$ which is not a principal left ideal.

Let $q = a^3 + 1$. Since $(p) = I \cap R(a)$, the element $p$ divides the element $N(1 + qb) = 1 + q\overline{q}$. The element $1 + q\overline{q}$ is expressed as a product of prime elements as follows:

$$1 + q\overline{q} = (a - \alpha)(a^{-1} - \alpha)(a^2 - \alpha a + \alpha^2)(a^{-2} - \alpha a^{-1} + \alpha^2),$$

where $\alpha$ is a real value of

$$\alpha = \sqrt[3]{\frac{-3 + 5}{2}}.$$

Let $p = (a^2 - \alpha a + \alpha^2)(a^{-2} - \alpha a^{-1} + \alpha^2)$. For $p$ and $q$ there exist elements $h$ and $r$ such that

$$(2.5) \quad p = qh + r.$$

Here

$$h = \alpha^2 a^{-1} - (\alpha + \alpha^3) a^{-2},$$

$$r = (1 + \alpha^2 + \alpha^4) - (\alpha + \alpha^2 + \alpha^3) a^{-1} + (\alpha + \alpha^2 + \alpha^3) a^{-2}.$$

It is true in (2.5) that $|r| = 2 < |q|$ and $|h| = 1$. We construct an element

$$(2.7) \quad u = bp - h(1 + qb) = (qh + r)b - h(1 + qb) = -h + rb \in I.$$

It follows that $|N(u)| = |h\overline{h} + r\overline{r}| = 4 = |p|.$

We show that the element $u$ does not generate the left ideal $I$. Indeed, assume that $I = (u)$. (2.7) implies

$$(2.8) \quad u - bp = -h(1 + qb).$$

Because $N(u) \in I \cap R(a)$, it follows that $n(u) \equiv 0 \pmod{p}$. However, $|N(u)| = |p|$, so the elements $N(u)$ and $p$ are associates. This means that $p = \delta \cdot N(u)$, and it is easy to calculate that $\delta = \alpha \cdot (1 + \alpha + 2\alpha^2 + \alpha^3 + 2\alpha^4 + \alpha^5 + \alpha^6)^{-1}$. Consequently

$$p = \delta(-\overline{h} - rb)(-h + rb),$$

so (2.8) implies

$$(2.9) \quad u - \delta b(-\overline{h} - rb)u = -h(1 + qb).$$

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 (2.9) can be expressed in the form

\[ [1 - \delta b(-h - rb)]u = -h(\mu_0 + \mu_1 b)u. \]

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

\[ 1 - \delta \bar{r} + \delta h b = -h(\mu_0 + \mu_1 b), \]

or \( 1 - \delta \bar{r} = -h\mu_0 \), that is

\[ 1 - \delta \bar{r} \equiv 0 \pmod{h}. \]

We show that congruence (2.10) gives rise to a contradiction. Indeed, applying (2.6) we have

\[ f(a) = 1 - \delta \bar{r} = -\delta(\alpha + \alpha^2 + \alpha^3)a^2 + \delta(\alpha + \alpha^2 + \alpha^3)a - \delta(1 + \alpha^2 + \alpha^4) + 1. \]

We set

\[ g(a) = a^2.h = a^2a - (\alpha + \alpha^3). \]

It is clear that \( h \) divides the element \( 1 - \delta \bar{r} \) if and only if \( g(a) \) divides \( f(a) \). Since \( g(a) = \alpha^2[a - \alpha^{-1}(1 + \alpha^2)] \), the congruence \( f(a) \equiv 0 \pmod{g(a)} \) is true if and only if \( f[a^{-1}(1 + \alpha^2)] = 0 \). It is easy to calculate that this is not true for the real value of \( \alpha \) mentioned above. 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 \( z = s_0 + s_1 b \). Then it follows that

\[ u = -h + rb = (\lambda_0 + \lambda_1 b)(s_0 + s_1 b) \]

for some element \( \lambda_0 + \lambda_1 b \in A \). (2.11) implies the equation

\[ N(u) = N(\lambda_0 + \lambda_1 b).N(z), \]

that is, the element \( N(z) \) divides \( N(u) \). On the other hand, \( N(z) \in I \cap R(a) \), that is, \( N(z) = m.p \) for some \( m \in R(a) \). Then it follows from (2.12) that \( N(u) = N(\lambda_0 + \lambda_1 b).m.p \). Since \( \delta N(u) = p \), we obtain that \( \lambda_0 + \lambda_1 b \) is an invertible element.

By (2.11) this implies that the elements \( u \) and \( z \) are associates. This is in contradiction with the fact that element \( u \) does not generate the left ideal \( I \).
References


L. Kossuth University
H:4010 Debrecen Pb.12
Hungary