

A basis for the unitary subgroup of the group of units in a finite commutative group algebra

By A. A. BOVDI (Debrecen) and A. SZAKÁCS (Eger)

1. Introduction

Let G be a finite abelian group, K the field $GF(p^m)$ of p^m elements and $V(KG)$ the group of normalized units (that is units of augmentation 1) in the group algebra KG .

For $x = \sum_{g \in G} \alpha_g g \in KG$, we say that the element $x^* = \sum_{g \in G} \alpha_g g^{-1}$ is conjugate to x , and if $x^* = x$, we say that x is selfconjugate. The map $x \rightarrow x^*$ is easily seen to be an involutory anti-automorphism (involution) of the algebra KG . An element $u \in V(KG)$ is called unitary if $u^{-1} = u^*$. The set of all unitary elements of the group $V(KG)$ is obviously a subgroup; we call it the unitary subgroup of $V(KG)$, and we denote it by $V_*(KG)$.

S. P. NOVIKOV had raised the problem of determining the invariants of $V_*(KG)$ when G has p -power order. This was solved by the authors in [1]; and in case $p > 2, m = 1$, we gave an explicit basis for $V_*(KG)$. Here we continue this work by giving a basis for the Sylow p -subgroup of $V_*(KG)$ whenever G is an arbitrary finite abelian group, without any restriction on p or m .

We shall write F for the field $GF(p)$ of p elements, C for the Sylow p -subgroup of G , and H for the direct complement of C in G : thus $G = C \times H$. Further, $C[p] = \{g \in C \mid g^p = 1\}$; $C^{p^i} = \{g^{p^i} \mid g \in C\}$; $f_i(C)$ denotes the number of components of order p^i in the decomposition of the group C into a direct product of cyclic groups; $r(C) = f_1(C) + f_2(C) + \dots$ denotes the p -rank of C ; $J = J(C)$ denotes the ideal of the algebra KG generated

by the elements $g-1$ ($g \in C$); and $V_p(KG)$ (respectively $W_p(KG)$) denotes the Sylow p -subgroup of the group $V(KG)$ (respectively $V_*(KG)$). Of course J is nilpotent, and $V_p(KG) = 1 + J$.

Note that the words 'basis' and 'independent' are used in two different senses to describe subsets of KG : on the one hand, additively, as subsets of the vector space KG ; on the other, multiplicatively, as subsets of the abelian group $V_p(KG)$. The context should make it clear which meaning is intended.

It is easy to prove the following statements using methods of proofs from [1].

Proposition 1.1. *Let be $p > 2$. Then*

$$r(W_p(KG)) = \frac{m}{2}|H|(|C| - |C^p|)$$

and

$$f_i(W_p(KG)) = \frac{m}{2}|H| \left(\left| C^{p^{i-1}} \right| - 2 \left| C^{p^i} \right| + \left| C^{p^{i+1}} \right| \right) \quad (i = 1, 2, 3, \dots).$$

Proposition 1.2. $W_2(KG) = C \times D(C) \times T(C)$,

$$r(W_2(KG)) = \frac{m}{2} (|H| (|C| - |C^2|) + |C[2]| + |C^2[2]| - 2),$$

$$f_1(T(C)) = r(T(C)) = m(|C[2]| - 1) - f_1(C),$$

$$\text{and } f_i(D(C)) = t_{i-1} - 2t_i + t_{i+1} - f_{i+1}(C) \quad (i = 1, 2, 3, \dots)$$

$$\text{where } t_j = \frac{m}{2} \left(|H| \left(\left| C^{2^j} \right| - 1 \right) - \left| C^{2^j}[2] \right| + 1 \right) \quad (j = 0, 1, 2, \dots).$$

2. A basis for $V_p(KG)$

We shall use the following notation: $C = \langle a_1 \rangle \times \dots \times \langle a_n \rangle$ is a decomposition of the p -group C as direct product of cyclic subgroups; q_i is the order of the element a_i ($i = 1, \dots, n$); and $L(C)$ is the set of all n -tuples of integers $(\alpha_1, \dots, \alpha_n) = \alpha$ for which $0 \leq \alpha_i < q_i$ and $p \nmid \alpha_i$ for some i .

R. SANDLING [2] proved that the set

$$\{x_\alpha = 1 + (a_1 - 1)^{\alpha_1} \dots (a_n - 1)^{\alpha_n} \mid \alpha \in L(C)\}$$

is a basis for $V(FC)$. We extend this result to the group $V_p(KG)$.

It is known (see [3], Theorem 2.35) that K has an F -basis of the form

$$(2.1) \quad \varepsilon, \varepsilon^p, \dots, \varepsilon^{p^{m-1}}.$$

The following statement was proved by S. A. JENNINGS (see [4], p. 89).

Lemma 2.1. *Let $A = A(KC)$ denote the augmentation ideal of the modular group algebra KC . Then the elements $y(\alpha_1, \dots, \alpha_n) =$*

$$y(\alpha) = (a_1 - 1)^{\alpha_1} \cdots (a_n - 1)^{\alpha_n} \quad (0 \leq \alpha_i < q_i, \alpha_1 + \cdots + \alpha_n \geq k)$$

form a K -basis for A^k .

Lemma 2.2. *Let $J = J(C)$ be the ideal of the algebra KG defined above and*

$$y(i, h, \alpha) = y(i, h, \alpha_1, \dots, \alpha_n) = \varepsilon^{p^i} h(a_1 - 1)^{\alpha_1} \cdots (a_n - 1)^{\alpha_n}.$$

Then

$$M_k = \{y(i, h, \alpha) \mid 0 \leq i < m, h \in H, 0 \leq \alpha_j < q_j (j = 1, \dots, n),$$

$$\alpha_1 + \cdots + \alpha_n \geq k\}$$

is an F -basis for J^k .

PROOF. It is known that the elements $h(c_1 - 1) \cdots (c_r - 1)$ ($h \in H$, $c_i \in C$, $r \geq k$) form a K -basis for J^k . By writing the elements $(c_1 - 1) \cdots (c_r - 1) \in J^k$ in terms of the basis given in Lemma 2.1, and the elements of K in terms of the basis (2.1), we can obtain a proof of the lemma.

Theorem 2.3. *The set*

$$B(G) = \{x(i, h, \alpha) = 1 + y(i, h, \alpha) \mid 0 \leq i < m, h \in H, \alpha \in L(C)\}$$

is a basis for $V_p(KG)$.

PROOF. It is easy to see that

$$\widetilde{M}_k = \{y(i, h, \alpha) + J^{k+1} \mid y(i, h, \alpha) \in M_k, \alpha_1 + \cdots + \alpha_n = k\}$$

is an F -basis for the vector space J^k/J^{k+1} . The additive group J^k/J^{k+1} is isomorphic to the multiplicative group $1 + J^k/1 + J^{k+1}$, so this factor-group is generated by the elements

$$(1 + y(i, h, \alpha)) (1 + J^{k+1}) \quad (\alpha_1 + \cdots + \alpha_n = k).$$

The subgroups $1 + J^k$ ($k = 1, 2, 3, \dots$) of $V_p(KG) = 1 + J$ form a finite series descending to 1, because J is nilpotent. Therefore $V_p(KG)$ is generated by the elements $x(i, h, \alpha) = 1 + y(i, h, \alpha)$ ($y(i, h, \alpha) \in M_1$). If $\alpha_1 = \beta_1 p^s, \dots, \alpha_n = \beta_n p^s$ and $p \nmid \beta_t$ for some t , then

$$x(i, h, \alpha) = \left(1 + \varepsilon^{p^j} g(a_1 - 1)^{\beta_1} \cdots (a_n - 1)^{\beta_n}\right)^{p^s} = x(j, g, \beta)^{p^s},$$

where $h = g^{p^s}$, $\beta = (\beta_1, \dots, \beta_n) \in L(C)$ and $j \equiv i - s \pmod{m}$. Consequently, $x(j, g, \beta) \in B(G)$ and so it follows that $V_p(KG)$ is generated by $B(G)$.

It is obvious that the cardinality $|B(G)|$ of the set $B(G)$ coincides with the rank of $V_p(KG)$. Let $x(i, h, \alpha)$ be an element from $B(G)$ for which

$$x(i, h, \alpha)^{p^k} = 1 + \varepsilon^{p^{i+k}} h^{p^k} (a_1^{p^k} - 1)^{\alpha_1} \cdots (a_n^{p^k} - 1)^{\alpha_n} \neq 1.$$

Then $\alpha_j < \frac{q_j}{p^k}$ for every $j = 1, \dots, n$ and $x(i, h, \alpha)^{p^k} \in B(C^{p^k} \times H)$.

Therefore, the cardinality of the set $B(G)^{p^k} = \{x^{p^k} \mid x \in B(G)\}$ coincides with $|B(C^{p^k} \times H)| = m|H|(|C^{p^k}| - |C^{p^{k+1}}|)$, and it follows that the number of elements of $B(G)$ of order p^k equals $|B(G)^{p^{k-1}}| - |B(G)^{p^k}| = f_k(V_p(KG))$. This completes the proof of our theorem.

Using this theorem, we describe a basis of the Sylow p -subgroup $W_p(KG)$ of the unitary subgroup $V_*(KG)$. First we consider the case $p > 2$.

3. A basis for $W_p(KG)$ in the case $p > 2$

It is easy to prove the following lemma by induction on n .

Lemma 3.1. *For $p > 2$ the cardinality of the set*

$$L_1(C) = \{(\alpha_1, \dots, \alpha_n) \in L(C) \mid \alpha_1 + \dots + \alpha_n \text{ is an odd number}\}$$

is equal to $\frac{1}{2}(|C| - |C^p|)$.

Theorem 3.2. *Let $p > 2$, $H[2] = \{h \in H \mid h^2 = 1\}$, E be a subset of $H \setminus H[2]$ having a unique representative in every set of the form $\{h, h^{-1}\}$,*

$$B_1(G) = \{x(i, h, \alpha)^* x(i, h, \alpha)^{-1} \mid x(i, h, \alpha) \in B(G), h \in E\}$$

and

$$B_2(G) = \{x(i, h, \alpha)^* x(i, h, \alpha)^{-1} \mid x(i, h, \alpha) \in B(G), h \in H[2], \\ \alpha_1 + \dots + \alpha_n \text{ is an odd number}\}.$$

Then $B_(G) = B_1(G) \cup B_2(G)$ is a basis for $W_p(KG)$.*

PROOF. Let $b_i = a_i - 1$, $k = \alpha_1 + \dots + \alpha_n$ and

$$y(\alpha) = y(\alpha_1, \dots, \alpha_n) = (a_1 - 1)^{\alpha_1} \cdots (a_n - 1)^{\alpha_n}.$$

By virtue of the equality

$$1 + b_i^{q_i} = (1 + b_i) (1 - b_i + b_i^2 - b_i^3 + \dots + b_i^{q_i-1}) = 1$$

it is easy to obtain that

$$(3.1) \quad b_i^* = -b_i + b_i^2 - b_i^3 + \dots + b_i^{q_i-1}.$$

Then $y(\alpha)^* = (-1)^k y(\alpha) + v$ for some v in $J^{k+1}(C)$ and

$$x(i, h, \alpha)^* = \left(1 + \varepsilon^{p^i} h y(\alpha)\right)^* = 1 + (-1)^k \varepsilon^{p^i} h^{-1} y(\alpha) + \tilde{v} \quad (\tilde{v} \in J^{k+1}(C)).$$

Clearly, for the $x(i, h, \alpha) = 1 + \varepsilon^{p^i} h y(\alpha) \in B(G)$ the element $y(\alpha)$ is nilpotent and

$$x(i, h, \alpha)^{-1} = 1 - \varepsilon^{p^i} h y(\alpha) + \left(\varepsilon^{p^i} h y(\alpha)\right)^2 - \left(\varepsilon^{p^i} h y(\alpha)\right)^3 + \dots.$$

Since

$$x(i, h, \alpha)^* x(i, h, \alpha)^{-1} = 1 + ((-1)^k h^{-1} - h) \varepsilon^{p^i} y(\alpha) + v$$

for some v in $J^{k+1}(C)$, it follows that $x(i, h, \alpha)^* x(i, h, \alpha)^{-1} \neq 1$ whenever $h \in E$ or k is odd. As an immediate consequence we have that $x(i, h, \alpha)^* x(i, h, \alpha)^{-1} \neq x(j, g, \beta)^* x(j, g, \beta)^{-1}$ if $i \neq j$ or $\alpha \neq \beta$ or $\{h, h^{-1}\} \neq \{g, g^{-1}\}$. This shows that the set $B_*(G)$ consists of pairwise distinct unitary elements. According to Lemma 3.1,

$|B_2(G)| = \frac{m}{2} |H[2]| (|C| - |C^p|)$. Since $|E| = \frac{1}{2} (|H| - |H[2]|)$, we also know that

$$|B_1(G)| = \frac{m}{2} (|H| - |H[2]|) (|C| - |C^p|).$$

Therefore, by Proposition 1.2, $|B_*(G)| = r(W_p(KG))$.

We shall prove that $(B_*(H \times C))^{p^s} = B_*(H \times C^{p^s})$. Suppose that $w(i, g, \alpha) = x(i, g, \alpha)^* x(i, g, \alpha)^{-1}$ and $w(j, h, \beta) = x(j, h, \beta)^* x(j, h, \beta)^{-1}$ are the different elements from $B_*(G)$ and their orders greater than p^s , yet $w(i, g, \alpha)^{p^s} = w(j, h, \beta)^{p^s}$. Then the element $v = (x(i, g, \alpha))^{p^s} (x(j, h, \beta)^*)^{p^s}$ is selfconjugate in the group algebra of the group $H \times C^{p^s}$. Let

$$c_j = a_j^{p^s}, \quad z(\alpha) = z(\alpha_1, \dots, \alpha_n) = (c_1 - 1)^{\alpha_1} \dots (c_n - 1)^{\alpha_n},$$

$$(x(i, g, \alpha))^{p^s} = 1 + \varepsilon^{p^{i+s}} g^{p^s} z(\alpha), \quad (x(j, h, \beta))^{p^s} = 1 + \varepsilon^{p^{j+s}} h^{p^s} z(\beta)$$

and $k = \alpha_1 + \dots + \alpha_n \leq \beta_1 + \dots + \beta_n$. Then, according to (3.1), we have

$$v \equiv 1 + \varepsilon^{p^{i+s}} g^{p^s} z(\alpha) + (-1)^k \varepsilon^{p^{j+s}} h^{-p^s} z(\beta) \pmod{J^{k+1}(C^{p^s})},$$

$$v^* \equiv 1 + (-1)^k \varepsilon^{p^{i+s}} g^{-p^s} z(\alpha) + \varepsilon^{p^{j+s}} h^{p^s} z(\beta) \pmod{J^{k+1}(C^{p^s})}.$$

Therefore from the condition $v = v^*$ we deduce that

$$(3.2) \quad \begin{aligned} & \varepsilon^{p^{i+s}} \left(g^{p^s} - (-1)^k g^{-p^s} \right) z(\alpha) \\ & - \varepsilon^{p^{j+s}} \left(h^{p^s} - (-1)^k h^{-p^s} \right) z(\beta) \equiv 0 \pmod{J^{k+1}(C^{p^s})}, \end{aligned}$$

where $(g^{p^s} - (-1)^k g^{-p^s}) z(\alpha) \neq 0$ since $w(i, g, \alpha) \in B_*(G)$. For any two different elements $w(i, g, \alpha)$ and $w(j, h, \beta)$ of $B_*(G)$ at least one of the following conditions holds: a) $i \neq j$; b) $\alpha \neq \beta$; c) $\{g, g^{-1}\} \neq \{h, h^{-1}\}$. Since $w(i, g, \alpha) \in B_*(G)$, it follows that $g \neq (-1)^k g^{-1}$ and neither the order of g nor the order of h is divisible by p , so c) is equivalent to the condition $\{g^{p^s}, g^{-p^s}\} \neq \{h^{p^s}, h^{-p^s}\}$. Hence (3.2) contradicts Lemma 2.2. Consequently, $(B_*(H \times C))^{p^s} = B_*(H \times C^{p^s})$ and $B_*(G)$ has exactly $|B_*(G)^{p^{s-1}}| - |B_*(G)^{p^s}| = f_s(W_p(KG))$ elements of order p^s .

We shall prove the independence of $B_*(G)$. Let

$$w(i_1, h_1, \alpha^{(1)}), \dots, w(i_s, h_s, \alpha^{(s)})$$

be different elements from $B_*(G)$, and let

$$w(i_1, h_1, \alpha^{(1)})^{k_1} \cdots w(i_s, h_s, \alpha^{(s)})^{k_s} = 1.$$

Then it is easy to see that the element

$$v = x(i_1, h_1, \alpha^{(1)})^{k_1} \cdots x(i_s, h_s, \alpha^{(s)})^{k_s}$$

is selfconjugate. Let $k_r = t_r p^{\nu(r)}$ and $p \nmid t_r$. Then

$$x(i_r, h_r, \alpha^{(r)})^{k_r} = x(j_r, g_r, \beta^{(r)})^{t_r},$$

where $j_r \equiv i_r + \nu(r) \pmod{m}$, $g_r = h_r p^{\nu(r)}$ and

$$\beta^{(r)} = (p^{\nu(r)} \alpha_1^{(r)}, \dots, p^{\nu(r)} \alpha_n^{(r)}).$$

Hence v can be written in the form

$$v = x(j_1, g_1, \beta^{(1)})^{t_1} \cdots x(j_s, g_s, \beta^{(s)})^{t_s},$$

where $p \nmid t_1 t_2 \cdots t_s$. Let $y(i, g, \alpha) = \varepsilon^{p^i} g(a_1 - 1)^{\alpha_1} \cdots (a_n - 1)^{\alpha_n}$ and

$k = \min_{1 \leq r \leq s} \left\{ \beta_1^{(r)} + \cdots + \beta_n^{(r)} \right\}$. Therefore $x(j_r, g_r, \beta^{(r)}) = 1 + y(j_r, g_r, \beta^{(r)})$ ($r = 1, \dots, s$) and

$$v \equiv 1 + t_1 y(j_1, g_1, \beta^{(1)}) + \cdots + t_s y(j_s, g_s, \beta^{(s)}) \pmod{J^{k+1}(C)}.$$

Without loss of generality we can assume that

$$k = \beta_1^{(1)} + \cdots + \beta_n^{(1)} = \cdots = \beta_1^{(s)} + \cdots + \beta_n^{(s)}.$$

It is clear that

$$v^* \equiv 1 + (-1)^k t_1 y(j_1, g_1^{-1}, \beta^{(1)}) + \cdots + (-1)^k t_s y(j_s, g_s^{-1}, \beta^{(s)}) \pmod{J^{k+1}(C)}.$$

Hence, by virtue of the equality $v = v^*$, we have

$$(3.3) \quad t_1 \left(y(j_1, g_1, \beta^{(1)}) - (-1)^k y(j_1, g_1^{-1}, \beta^{(1)}) \right) + \cdots + t_s \left(y(j_s, g_s, \beta^{(s)}) - (-1)^k y(j_s, g_s^{-1}, \beta^{(s)}) \right) \equiv 0 \pmod{J^{k+1}(C)}.$$

Since $w(i_r, h_r, \alpha^{(r)}) \in B_*(G)$ and $p > 2$, it follows that $g_r \neq (-1)^k g_r^{-1}$ and the summand $u_r = y(j_r, g_r, \beta^{(r)}) - (-1)^k y(j_r, g_r^{-1}, \beta^{(r)})$ is nonzero. If $\beta^{(r)} \neq \beta^{(q)}$, then obviously $u_r \neq u_q$. Hence from (3.3) follows that $\beta^{(1)} = \cdots = \beta^{(s)} = \beta$ and $g_r = h_r^{p^\nu}$ ($r = 1, \dots, s$) for a fixed ν . If $\{h_r, h_r^{-1}\} \neq \{h_q, h_q^{-1}\}$, then $\{g_r, g_r^{-1}\} \neq \{g_q, g_q^{-1}\}$ (p does not divide the order of h_r, h_q) and $u_r \neq u_q$. Therefore, from (3.3) we deduce that $\{g_1, g_1^{-1}\} = \cdots = \{g_s, g_s^{-1}\}$. Since $y(j_1, g_1, \beta), \dots, y(j_s, g_1, \beta)$ are the pairwise distinct elements, it follows from (3.3) that $t_1 \varepsilon^{p^{j_1}} + \cdots + t_s \varepsilon^{p^{j_s}} \equiv 0 \pmod{p}$ which is impossible because $p \nmid t_1 t_2 \cdots t_s$. This completes the proof of the theorem.

4. A basis for $W_2(KG)$

We now turn to the case $p = 2$. First we describe a basis $B_*(C)$ for the unitary subgroup $V_*(KC)$. It is obvious that $V_*(KC) = V(KC)$ when C is elementary abelian or C is the cyclic group of order 4. Therefore we shall assume that the exponent of C is greater than 2 and C is not the cyclic group of order 4.

Let $N(C)$ denote the set of all n -tuples of integers $(\alpha_1, \dots, \alpha_n) \neq$

$(0, \dots, 0)$ for which $\alpha_i \in \{0, q_i - 1\}$ and

$$T(C) = \left\{ 1 + \sum_{\alpha \in N(C)} \lambda_\alpha (1 + a_1)^{\alpha_1} \cdots (1 + a_n)^{\alpha_n} \mid \lambda_\alpha \in K \right\}.$$

It is easy to see that $T(C)$ is an elementary subgroup of $V_*(KC)$, $T(C) \cap C = \{a_i \mid a_i^2 = 1, i = 1, \dots, n\}$ and the group $T(C)$ has a basis of the form

$$B_T(C) = \left\{ 1 + \varepsilon^{2^r} (1 + a_1)^{\alpha_1} \cdots (1 + a_n)^{\alpha_n} \mid 0 \leq r < m, \alpha \in N(C) \right\}$$

where $\varepsilon, \varepsilon^2, \dots, \varepsilon^{2^{m-1}}$ is a $GF(2)$ -basis of the field $K = GF(2^m)$ (see (2.1)). According to Proposition 1.2,

$$V_*(KC) = \langle a_i \mid a_i^2 \neq 1 \rangle \times T(C) \times D(C)$$

where by [1] $D(C) \subset \{x^*x^{-1} \mid x \in V(KC)\}$. In the following we shall construct a basis of the group $D(C)$.

From now on, let F be the field of 2 elements, C a finite abelian 2-group of exponent greater than 2 and different from the cyclic group of order 4, $A = A(FC)$ the augmentation ideal of the algebra FC , $L_2(C) = \{(\alpha_1, \dots, \alpha_n) \mid \alpha_i \in \{0, 2, 4, \dots, q_i - 2\}, i = 1, 2, \dots, n\}$ and

$$\mu(C) = \frac{1}{2} (|C| - |C^2| - |C[2]| + |C^2[2]|) - r(C^2).$$

We shall construct a subset $L_*(C)$ of $L(C)$ for which the set

$$B_0(C) = \{x_\alpha^* x_\alpha^{-1} \mid x_\alpha = 1 + (a_1 + 1)^{\alpha_1} \cdots (a_n + 1)^{\alpha_n} \in B(C), \alpha \in L_*(C)\}$$

is a basis of the group $D(C)$. For the proof of this fact we shall construct subsets $L_0(C) \subset L(C) \cup L_2(C)$ and $L_1(C) \subset L(C)$ and we shall prove that they have the following properties:

- $a_1)$ there exists a one-to-one map ψ from $L_*(C)$ onto $L_0(C)$;
- $a_2)$ $L_0(C) \cap L_*(C) = \emptyset$ (empty set);
- $a_3)$ $L_0(C) \cap L_1(C) = \emptyset$;
- $a_4)$ $|L_*(C)| = \mu(C)$;
- $a_5)$ if $\alpha = (\alpha_1, \dots, \alpha_n) \in L_*(C)$ and $\psi(\alpha) = \bar{\alpha} = (\bar{\alpha}_1, \dots, \bar{\alpha}_n) \in L_0(C)$, then $\alpha_1 + \dots + \alpha_n = \bar{\alpha}_1 + \dots + \bar{\alpha}_n - 1 = k$ and

$$x_\alpha^* x_\alpha^{-1} = x_{\bar{\alpha}} \left(\prod_{\tau \in Q} x_\tau \right) \left(\prod_{\nu \in R} x_\nu \right) (1 + y) \quad (y \in A^{k+2})$$

where $Q \subset \{\tau \in L_*(C) \mid \tau_1 + \dots + \tau_n = k + 1\}$ and $R \subset \{\nu \in L_1(C) \mid \nu_1 + \dots + \nu_n = k + 1\}$.

Note that the subsets Q and R may be empty.

For the proof of property a_5) and the following below theorems we need two lemmas.

Lemma 4.1. *Let a be an element of order q in the 2-group C and let $\gamma = a + 1$. Then $(\gamma^*)^s = (a^{-1} + 1)^s = \ell_0 \gamma^s + \ell_1 \gamma^{s+1} + \ell_2 \gamma^{s+2} + v$ for some v in A^{s+3} , with ℓ_0, ℓ_1, ℓ_2 defined in terms of s as follows:*

*if $s \equiv 0 \pmod{4}$ or $s \in \{q-1, q-2\}$, then $\ell_0 = 1, \ell_1 = \ell_2 = 0$;
 if $s \equiv 1 \pmod{4}$, then $\ell_0 = \ell_1 = \ell_2 = 1$;
 if $s \equiv 2 \pmod{4}$ and $s < q-2$, then $\ell_0 = \ell_2 = 1, \ell_1 = 0$;
 if $s \equiv 3 \pmod{4}$ and $s < q-1$, then $\ell_0 = \ell_1 = 1, \ell_2 = 0$.*

PROOF. According to (3.1), $\gamma^* = \gamma + \gamma^2 + \dots + \gamma^{q-1}$. Since KC is a ring of characteristic 2, it follows that $(\gamma^*)^2 = \gamma^2 + \gamma^4 + \dots + \gamma^{q-2}$ and $(\gamma^*)^4 = \gamma^4 + \gamma^8 + \dots + \gamma^{q-4}$. Hence we easily obtain a proof of the lemma.

Lemma 4.2. *Let $\alpha = (\alpha_1, \dots, \alpha_n) \in L(C)$, $\alpha_1 + \dots + \alpha_n = k$ and $x_\alpha = 1 + (a_1 + 1)^{\alpha_1} \dots (a_n + 1)^{\alpha_n}$. Then*

$$x_\alpha^* x_\alpha^{-1} = \left(\prod_{\tau} x_\tau \right) (1 + y) \quad (y \in A^{k+3})$$

where the product is taken over all $\tau = (\tau_1, \dots, \tau_n)$ such that $k + 1 \leq \tau_1 + \dots + \tau_n \leq k + 2$ and the components τ_i satisfy the following conditions:

- 1) $\tau_i = \alpha_i$, if $\alpha_i \equiv 0 \pmod{4}$ or $\alpha_i \in \{q_i - 1, q_i - 2\}$;
- 2) $\tau_i \in \{\alpha_i, \alpha_i + 1, \alpha_i + 2\}$, if $\alpha_i \equiv 1 \pmod{4}$;
- 3) $\tau_i \in \{\alpha_i, \alpha_i + 2\}$, if $\alpha_i \equiv 2 \pmod{4}$ and $\alpha_i < q_i - 2$;
- 4) $\tau_i \in \{\alpha_i, \alpha_i + 1\}$, if $\alpha_i \equiv 3 \pmod{4}$ and $\alpha_i < q_i - 1$.

PROOF. In the following we shall make frequent use of the fact: if $u \in A^k$ and $v \in A^r$ there exists a $z \in A^{k+r}$ for which

$$(4.1) \quad 1 + u + v = (1 + u)(1 + v)(1 + z).$$

According to Lemma 4.1,

$$(4.2) \quad (a_i^{-1} + 1)^{\alpha_i} = \ell_0^{(i)} (a_i + 1)^{\alpha_i} + \ell_1^{(i)} (a_i + 1)^{\alpha_i+1} + \ell_2^{(i)} (a_i + 1)^{\alpha_i+2} + v_i,$$

where $v_i \in A^{\alpha_i+3}$ and $\ell_0^{(i)}, \ell_1^{(i)}, \ell_2^{(i)}$ we defined as in Lemma 4.1 (with reference to $s = \alpha_i$). By definition, $x_\alpha^* = 1 + (a_1^{-1} + 1)^{\alpha_1} \dots (a_n^{-1} + 1)^{\alpha_n}$,

and so by (4.2),

$$\begin{aligned} x_\alpha^* &= 1 + \left(v_1 + \sum_{j_1=0}^2 \ell_{j_1}^{(1)} (a_1 + 1)^{\alpha_1 + j_1} \right) \cdots \left(v_n + \sum_{j_n=0}^2 \ell_{j_n}^{(n)} (a_n + 1)^{\alpha_n + j_n} \right) \\ &= 1 + \sum_{j_1, \dots, j_n} \ell_{j_1}^{(1)} (a_1 + 1)^{\alpha_1 + j_1} \cdots \ell_{j_n}^{(n)} (a_n + 1)^{\alpha_n + j_n} + v \quad (v \in A^{k+3}). \end{aligned}$$

Obviously, we can assume that $j_1 + \cdots + j_n \leq 2$. Therefore, according to (4.1), we have $x_\alpha^* = x_\alpha \left(\prod_{\tau} x_\tau \right) (1 + y)$ ($y \in A^{k+3}$), where the product is taken over all those $\tau = (\tau_1, \dots, \tau_n)$ for which $k + 1 \leq \tau_1 + \cdots + \tau_n \leq k + 2$ and whose components τ_i satisfy the conditions of the lemma. This completes the proof.

We now turn to the construction of the sets $L_*(C)$, $L_0(C)$ and $L_1(C)$. Let $C = \langle a_1 \rangle \times \cdots \times \langle a_n \rangle$, $n \geq 1$, $q_1 = 2^t$, $q_1 \geq q_2 \geq \cdots \geq q_n$ and $a_1, \dots, a_s$ ($s \leq n$) be all those basic elements of the group C , which have orders greater than 2. We shall construct the sets $L_*(C)$, $L_0(C)$, $L_1(C)$ by induction on s . The first step of the induction (the cases $s = n = 1$; $s = 1$ and $n > 1$; $s = n = 2$) is the following three lemmas.

Lemma 4.3. *Let C be a cyclic group of order $q_1 > 4$. Put $L_1(C) = \emptyset$,*

$$L_*(C) = \left\{ \alpha = (4i + 1) \mid i = 1, \dots, \frac{1}{4}q_1 - 1 \right\}$$

and

$$L_0(C) = \left\{ \bar{\alpha} = (4i + 2) \mid i = 1, \dots, \frac{1}{4}q_1 - 1 \right\}.$$

Then $L_*(C)$, $L_0(C)$ and $L_1(C)$ have properties $a_1) - a_5)$.

PROOF. Properties $a_2)$ and $a_3)$ are obvious. We define the one-to-one map ψ of $L_*(C)$ onto $L_0(C)$ the following way: $\psi((4i + 1)) = (4i + 2)$. It is easy to see that $\mu(C) = \frac{1}{2} \left(q_1 - \frac{1}{2}q_1 \right) - 1 = \frac{1}{4}q_1 - 1$ and so $|L_*(C)| = \mu(C)$. According to Lemma 4.2,

$$(x_{(4i+1)})^* (x_{(4i+1)})^{-1} = x_{(4i+2)} (1 + y) \quad (y \in A^{4i+3}).$$

The proof is complete.

Lemma 4.4. *Let be $n > 1$, $q_1 \geq 4$ and $q_2 = \dots = q_n = 2$. Put*

$$L_1(C) = \emptyset, \quad L_*(C) = \left\{ \alpha = (4i+1, 0, \dots, 0) \mid i = 1, \dots, \frac{1}{4}q_1 - 1 \right\} \cup \\ \cup \left\{ \alpha = (2i-1, \alpha_2, \dots, \alpha_n) \mid i = 1, \dots, \frac{1}{2}q_1 - 1, \alpha_2 + \dots + \alpha_n > 0 \right\}$$

and

$$L_0(C) = \left\{ \bar{\alpha} = (4i+2, 0, \dots, 0) \mid i = 1, \dots, \frac{1}{4}q_1 - 1 \right\} \cup \\ \cup \left\{ \bar{\alpha} = (2i, \alpha_2, \dots, \alpha_n) \mid i = 1, \dots, \frac{1}{2}q_1 - 1, \alpha_2 + \dots + \alpha_n > 0 \right\}.$$

Then $L_*(C)$, $L_0(C)$ and $L_1(C)$ have properties $a_1) - a_5)$.

PROOF. Properties $a_2)$ and $a_3)$ are obvious. We define ψ the following way: $\psi((\alpha_1, \alpha_2, \dots, \alpha_n)) = (\alpha_1 + 1, \alpha_2, \dots, \alpha_n)$. It is clear that

$$|L_*(C)| = \left(\frac{1}{4}q_1 - 1 \right) + \left(\frac{1}{2}q_1 - 1 \right) (2^{n-1} - 1) \text{ and}$$

$$\mu(C) = \frac{1}{2} \left(q_1 2^{n-1} - \frac{1}{2}q_1 - 2^n + 2 \right) - 1, \text{ so } a_4) \text{ holds. If } \alpha \in L_*(C) \text{ and } \psi(\alpha) = \bar{\alpha} \in L_0(C), \text{ then by Lemma 4.2,}$$

$$x_\alpha^* x_\alpha^{-1} = x_{\bar{\alpha}}(1 + y) \quad (y \in A^{\alpha_1 + \dots + \alpha_n + 2}).$$

So the lemma is true.

Lemma 4.5. *Let $n = 2$, $q_1 = 2^t \geq q_2 \geq 4$. Put*

$$L_1(C) = \{(\alpha_1, \alpha_2) \mid \alpha_1 \equiv 0 \pmod{4}, \alpha_2 \equiv 1 \pmod{4}\} \cup \\ \cup \{(\alpha_1, \alpha_2) \mid \alpha_1 \equiv 3 \pmod{4}, \alpha_1 \neq 2^i - 1 \ (1 < i \leq t), \alpha_2 \equiv 0 \pmod{4}\}, \\ L_*(C) = \{(0, \alpha_2) \mid \alpha_2 \equiv 1 \pmod{4}, \alpha_2 > 1\} \cup \\ \cup \{(2^i, \alpha_2) \mid 1 < i < t, \alpha_2 \equiv 1 \pmod{4}\} \cup \\ \cup \{(1, \alpha_2) \mid \alpha_2 > 0\} \cup \{(\alpha_1, \alpha_2) \mid \alpha_1 \equiv 1 \pmod{4}, \alpha_1 > 1\} \cup \\ \cup \{(\alpha_1, \alpha_2) \mid \alpha_1 \equiv 3 \pmod{4}, \alpha_2 \equiv 1 \pmod{4}\} \cup \\ \cup \{(\alpha_1, \alpha_2) \mid \alpha_1 \equiv 3 \pmod{4}, \alpha_1 \neq 2^i - 1 \ (1 < i \leq t), \alpha_2 \equiv 3 \pmod{4}\}$$

and

$$L_0(C) = \{(0, \bar{\alpha}_2) \mid \bar{\alpha}_2 \equiv 2 \pmod{4}, \bar{\alpha}_2 > 2\} \cup \\ \cup \{(2^i, \bar{\alpha}_2) \mid 1 < i < t, \bar{\alpha}_2 \equiv 2 \pmod{4}\} \cup$$

$$\begin{aligned}
& \cup \{(2, \bar{\alpha}_2) \mid \bar{\alpha}_2 > 0\} \cup \{(\bar{\alpha}_1, \bar{\alpha}_2) \mid \bar{\alpha}_1 \equiv 2 \pmod{4}, \bar{\alpha}_1 > 2\} \cup \\
& \cup \{(\bar{\alpha}_1, \bar{\alpha}_2) \mid \bar{\alpha}_1 \equiv 3 \pmod{4}, \bar{\alpha}_2 \equiv 2 \pmod{4}\} \cup \\
& \cup \{(\bar{\alpha}_1, \bar{\alpha}_2) \mid \bar{\alpha}_1 \equiv 0 \pmod{4}, \bar{\alpha}_1 \neq 2^i (1 < i < t), \bar{\alpha}_2 \equiv 3 \pmod{4}\}.
\end{aligned}$$

Then $L_*(C)$, $L_0(C)$ and $L_1(C)$ have properties $a_1) - a_5)$.

PROOF. First we define the one-to-one map ψ :

$$\psi((\alpha_1, \alpha_2)) = \begin{cases} (\alpha_1, \alpha_2 + 1), & \text{if } \alpha_2 \equiv 1 \pmod{4} \text{ and } \alpha_1 \not\equiv 1 \pmod{4}, \\ (\alpha_1 + 1, \alpha_2), & \text{otherwise.} \end{cases}$$

Let $\beta = (\beta_1, \beta_2) \in L_0(C) \cap L_*(C)$. If β_1 is odd, then from $\beta \in L_0(C)$ it follows that $\beta_1 \equiv 3 \pmod{4}$ and $\beta_2 \equiv 2 \pmod{4}$. But from $(\beta_1, \beta_2) \in L_*(C)$, $\beta_1 \equiv 3 \pmod{4}$ we have that $\beta_2 \equiv 1 \pmod{2}$, which is impossible. Similarly, if β_1 is even, then from $\beta \in L_*(C)$ it follows $\beta_1 \in \{0; 2^i (1 < i < t)\}$ and $\beta_2 \equiv 1 \pmod{4}$. However for $(\beta_1, \beta_2) \in L_0(C)$ we have $\beta_2 \equiv 2 \pmod{4}$ and, therefore, $L_0(C) \cap L_*(C) = \emptyset$.

Let now $\beta = (\beta_1, \beta_2) \in L_0(C) \cap L_1(C)$. If $\beta_1 \equiv 0 \pmod{4}$, then $\beta_2 \equiv 1 \pmod{4}$ for the elements β of $L_1(C)$, and $\beta_2 \equiv 2 \pmod{4}$ or $\beta_2 \equiv 3 \pmod{4}$ for $\beta \in L_0(C)$, so we get a contradiction. Similarly, if $\beta_1 \equiv 3 \pmod{4}$, then on the one hand, $\beta_2 \equiv 0 \pmod{4}$ and on the other, $\beta_2 \equiv 2 \pmod{4}$. Therefore, $L_0(C) \cap L_1(C) = \emptyset$.

$$\begin{aligned}
& \text{It is easy to see that } |L_*(C)| = \left(\frac{1}{4}q_2 - 1\right) + (t-2)\frac{1}{4}q_2 + (q_2 - 1) + \\
& \left(\frac{1}{4}q_1 - 1\right)q_2 + \frac{1}{4}q_1\frac{1}{4}q_2 + \left(\frac{1}{4}q_1 - (t-1)\right)\frac{1}{4}q_2 = \frac{3}{8}q_1q_2 - 2, \text{ which equals} \\
& \mu(C) = \frac{1}{2} \left(q_1q_2 - \frac{1}{4}q_1q_2 - 4 + 4\right) - 2.
\end{aligned}$$

Let now $\alpha = (\alpha_1, \alpha_2) \in L_*(C)$. Then according to Lemma 4.2,

$$x_\alpha * x_\alpha^{-1} = (x_{(\alpha_1+1, \alpha_2)})^{k_1} (x_{(\alpha_1, \alpha_2+1)})^{k_2} (1+y) \quad (y \in A^{\alpha_1+\alpha_2+2})$$

where

$$k_i = \begin{cases} 0, & \text{if } \alpha_i \equiv 0 \pmod{2} \text{ or } \alpha_i = q_i - 1, \\ 1, & \text{if } \alpha_i \equiv 1 \pmod{2} \text{ and } \alpha_i < q_i - 1. \end{cases}$$

So if $\alpha_1 \equiv 0 \pmod{4}$ and $\alpha_2 \equiv 1 \pmod{4}$, then $k_1 = 0$ and the element $(\alpha_1, \alpha_2 + 1)$ coincides with $\psi(\alpha) \in L_0(C)$. Suppose that $\alpha_1 \equiv 1 \pmod{4}$. Then $(\alpha_1 + 1, \alpha_2)$ coincides with $\psi(\alpha)$ and $(\alpha_1, \alpha_2 + 1) \in L_*(C)$ whenever $k_2 \neq 0$. Let now $\alpha_1 \equiv 3 \pmod{4}$ and $\alpha_2 \equiv 1 \pmod{4}$. Then $(\alpha_1, \alpha_2 + 1) = \psi(\alpha)$ and $(\alpha_1 + 1, \alpha_2) \in L_1(C)$ in case $\alpha_1 < q_1 - 1$. At last, if $\alpha_1 \equiv 3 \pmod{4}$, $\alpha_1 \neq 2^i - 1$ and $\alpha_2 \equiv 3 \pmod{4}$, then $(\alpha_1 + 1, \alpha_2) = \psi(\alpha) \in$

$L_0(C)$ and $(\alpha_1, \alpha_2 + 1) \in L_1(C)$ whenever $\alpha_2 < q_2 - 1$. The proof is complete.

We remind that we shall construct by induction on the p -rank of the group C such sets $L_*(C)$, $L_0(C)$ and $L_1(C)$ which have properties $a_1) - a_5)$. In the Lemmas 4.3–4.5 the first step of the induction is proved. Now we present the group C as the direct product of groups $\langle a_1 \mid a_1^{2^t} = 1 \rangle$ and $\tilde{C} = \langle a_2, \dots, a_n \rangle$. According to Lemmas 4.3–4.5, we can assume that the sets $L_*(\tilde{C})$, $L_0(\tilde{C})$ and $L_1(\tilde{C})$ exist and have properties $a_1) - a_5)$. We remind that

$$N(C) = \{(\alpha_1, \dots, \alpha_n) \mid \alpha_i = 0 \text{ or } q_i - 1, \alpha_1 + \dots + \alpha_n > 0\},$$

$$L_2(C) = \{(\alpha_1, \dots, \alpha_n) \mid \alpha_i \in \{0, 2, 4, \dots, q_i - 2\}, i = 1, 2, \dots, n\}.$$

Let L_i^* denotes the set of all elements from $L(C)$ for which the condition $i)$ holds:

- 1) $\alpha_1 = 0$ and $(\alpha_2, \dots, \alpha_n) \in L_*(\tilde{C})$;
- 2) $\alpha_1 = 1$ and $\alpha_2 + \dots + \alpha_n > 0$;
- 3) $\alpha_1 \equiv 1 \pmod{4}$, $\alpha_1 > 1$;
- 4) $\alpha_1 = 2^i - 1$ ($1 < i \leq t$) and $(\alpha_2, \dots, \alpha_n) \in L_*(\tilde{C})$;
- 5) $\alpha_1 = 2^i - 1$ ($1 < i < t$), $(\alpha_2, \dots, \alpha_n) \in N(\tilde{C})$, $s < n$ and $\alpha_{s+1} + \dots + \alpha_n > 0$;
- 6) $\alpha_1 = 2^i - 1$ ($1 < i \leq t$) and α has the form

$$\eta^{(j)} = (\alpha_1, 0, \dots, 0, 1, 0, \dots, 0) \quad (1 \text{ in the } j\text{-th position})$$

where $j = 2, \dots, s$;

- 7) $\alpha_1 \equiv 3 \pmod{4}$, $\alpha_1 \neq 2^i - 1$ ($1 < i \leq t$) and $(\alpha_2, \dots, \alpha_n) \in L(\tilde{C})$;
- 8) $\alpha_1 = 2^i$ ($1 < i < t$) and $(\alpha_2, \dots, \alpha_n) \in L_*(\tilde{C})$;
- 9) $\alpha_1 = 2^i$ ($1 < i < t$) and $\alpha \in \{\eta^{(2)}, \eta^{(3)}, \dots, \eta^{(s)}\}$.

Let L_i^0 denotes the set of all elements from $L(C) \cup L_2(C)$ for which the condition $i')$ holds:

- 1') $\bar{\alpha}_1 = 0$ and $(\bar{\alpha}_2, \dots, \bar{\alpha}_n) \in L_0(\tilde{C})$;
- 2') $\bar{\alpha}_1 = 2$ and $\bar{\alpha}_2 + \dots + \bar{\alpha}_n > 0$;
- 3') $\bar{\alpha}_1 \equiv 2 \pmod{4}$, $\bar{\alpha}_1 > 2$;

- 4') $\bar{\alpha}_1 = 2^i - 1$ ($1 < i \leq t$) and $(\bar{\alpha}_2, \dots, \bar{\alpha}_n) \in L_0(\tilde{C})$;
 5') $\bar{\alpha}_1 = 2^i$ ($1 < i < t$), $(\bar{\alpha}_2, \dots, \bar{\alpha}_n) \in N(\tilde{C})$, $s < n$ and $\bar{\alpha}_{s+1} + \dots + \bar{\alpha}_n > 0$;
 6') $\bar{\alpha}_1 = 2^i - 1$ ($1 < i \leq t$) and $\bar{\alpha}$ has the form

$$\bar{\eta}^{(j)} = (\bar{\alpha}_1, 0, \dots, 0, 2, 0, \dots, 0) \quad (2 \text{ in the } j\text{-th position})$$

where $j = 2, \dots, s$;

- 7') $\bar{\alpha}_1 \equiv 0 \pmod{4}$, $\bar{\alpha}_1 > 0$, $\bar{\alpha}_1 \neq 2^i$ ($1 < i \leq t$) and $(\bar{\alpha}_2, \dots, \bar{\alpha}_n) \in L(\tilde{C})$;
 8') $\bar{\alpha}_1 = 2^i$ ($1 < i < t$) and $(\bar{\alpha}_2, \dots, \bar{\alpha}_n) \in L_0(\tilde{C})$;
 9') $\bar{\alpha}_1 = 2^i$ ($1 < i < t$) and $\bar{\alpha} \in \{\bar{\eta}^{(2)}, \bar{\eta}^{(3)}, \dots, \bar{\eta}^{(s)}\}$.

Lemma 4.6. Put $L_*(C) = L_1^* \cup L_2^* \cup \dots \cup L_9^*$,

$$L_0(C) = L_1^0 \cup L_2^0 \cup \dots \cup L_9^0 \quad \text{and}$$

$$\begin{aligned} L_1(C) = & \{(\alpha_1, \alpha_2, \dots, \alpha_n) \mid \alpha_1 \equiv 3 \pmod{4}, \alpha_1 \neq 2^i - 1, 1 < i \leq t\} \cup \\ & \cup \{(\alpha_1, \alpha_2, \dots, \alpha_n) \mid \alpha_1 \in \{0; 2^i \ (1 < i < t); 2^i - 1 \ (1 < i \leq t)\}, \\ & (\alpha_2, \dots, \alpha_n) \in L_1(\tilde{C})\}. \end{aligned}$$

Then $L_*(C)$, $L_0(C)$ and $L_1(C)$ have properties $a_1) - a_5)$.

Remark. Note that in case $n > 2$, $q_1 \geq q_2 \geq 4$, $q_3 = \dots = q_n = 2$ the set $L_1(\tilde{C})$ is empty (see Lemma 4.4) and so $L_1(C)$ has the form

$$L_1(C) = \{(\alpha_1, \alpha_2, \dots, \alpha_n) \mid \alpha_1 \equiv 3 \pmod{4}, \alpha_1 \neq 2^i - 1, 1 < i \leq t\}.$$

PROOF of the Lemma. First we prove that if $q_n = 2$ and $q_s > q_{s+1} = \dots = q_n = 2$, then

$$(4.3) \quad L_0(C) \cap \{(\gamma_1, \dots, \gamma_n) \in N(C) \mid \gamma_{s+1} + \dots + \gamma_n > 0\} = \emptyset.$$

We shall use induction on s . In case $s = 1$ (4.3) follows from Lemma 4.4. Suppose that $s > 1$ and

$$\delta = (\delta_1, \delta_2, \dots, \delta_n) \in L_0(C) \cap \{(\gamma_1, \dots, \gamma_n) \in N(C) \mid \gamma_{s+1} + \dots + \gamma_n > 0\}.$$

If $\delta_1 = 0$, then the element $(\delta_2, \dots, \delta_n)$ belongs to the set

$$L_0(\tilde{C}) \cap \{(\gamma_2, \dots, \gamma_n) \in N(\tilde{C}) \mid \gamma_{s+1} + \dots + \gamma_n > 0\}$$

which, by the induction hypothesis, is empty. Hence, using the form of the elements from $N(C)$, it follows that $\delta_1 = q_1 - 1$. Then for $\delta \in L_0(C)$ condition 4') holds and, therefore, $(\delta_2, \dots, \delta_n) \in L_0(\tilde{C})$. Since $(\delta_2, \dots, \delta_n) \in N(\tilde{C})$ and $\delta_{s+1} + \dots + \delta_n > 0$, it follows that

$$(\delta_2, \dots, \delta_n) \in L_0(\tilde{C}) \cap \{(\gamma_2, \dots, \gamma_n) \in N(\tilde{C}) \mid \gamma_{s+1} + \dots + \gamma_n > 0\}$$

and, by the induction hypothesis, we get a contradiction. The statement is proved.

Let us prove now by induction on s that

$$(4.4) \quad N(C) \cap (L_*(C) \cup L_1(C)) = \emptyset.$$

In cases $s = 1$ or $s = n = 2$ (4.4) immediately follows from Lemmas 4.3–4.5. Suppose that $N(\tilde{C}) \cap (L_*(\tilde{C}) \cup L_1(\tilde{C})) = \emptyset$ and $\delta = (\delta_1, \delta_2, \dots, \delta_n)$ belongs to the set $N(C) \cap (L_*(C) \cup L_1(C))$. If $\delta_1 = 0$, then $(\delta_2, \dots, \delta_n) \in N(\tilde{C}) \cap (L_*(\tilde{C}) \cup L_1(\tilde{C}))$, which contradicts the induction hypothesis. So $\delta_1 = q_1 - 1$. It is easy to see that $(q_1 - 1, 0, \dots, 0) \notin L_*(C) \cup L_1(C)$. Clearly, $(\delta_2, \dots, \delta_n) \in N(\tilde{C})$ and from $(q_1 - 1, \delta_2, \dots, \delta_n) \in L_*(C) \cup L_1(C)$ it follows that $(\delta_2, \dots, \delta_n) \in L_1(\tilde{C}) \cup L_*(\tilde{C})$ or δ has the form $\eta^{(j)} = (q_1 - 1, 0, \dots, 0, 1, 0, \dots, 0)$ (1 in the j -th position and $2 \leq j \leq s$). By the induction hypothesis, $(\delta_2, \dots, \delta_n)$ can not belong to the set $L_*(\tilde{C}) \cup L_1(\tilde{C})$. Obviously, $\eta^{(j)} \notin N(C)$ and so (4.4) is proved.

Now we turn to the proof of the lemma. According to Lemmas 4.3–4.5, we shall assume that the sets $L_*(\tilde{C})$, $L_0(\tilde{C})$ and $L_1(\tilde{C})$ have properties $a_1) - a_5)$.

By the induction hypothesis, we can assume that if $(\alpha_2, \dots, \alpha_n) \in L_*(\tilde{C})$, there exists an element $(\bar{\alpha}_2, \dots, \bar{\alpha}_n)$ in $L_0(\tilde{C})$. So we can define ψ the following way:

$$\psi(\alpha) = \begin{cases} (\alpha_1, 0, \dots, 0, 2, 0, \dots, 0), & \text{if } \alpha \in L_6^* \cup L_9^*, \\ (\alpha_1, \bar{\alpha}_2, \dots, \bar{\alpha}_n), & \text{if } \alpha \in L_1^* \cup L_4^* \cup L_8^*, \\ (\alpha_1 + 1, \alpha_2, \dots, \alpha_n), & \text{if } \alpha \in L_2^* \cup L_3^* \cup L_5^* \cup L_7^*. \end{cases}$$

Obviously if $\alpha = (\alpha_1, \dots, \alpha_n) \in L_i^*$, then $\psi(\alpha) \in L_i^0$.

Let us prove $a_2)$. Suppose that $\gamma = (\gamma_1, \gamma_2, \dots, \gamma_n) \in L_0(C) \cap L_*(C)$. If $\gamma_1 = 0$, then $(\gamma_2, \dots, \gamma_n)$ belongs to the set $L_0(\tilde{C}) \cap L_*(\tilde{C})$, which, by the induction hypothesis, is empty. Therefore, comparing the first components of elements from $L_0(C)$ and $L_*(C)$, we have that $\gamma_1 = 2^i$ ($1 < i < t$) or $\gamma_1 = 2^i - 1$ ($1 < i \leq t$).

Suppose $\gamma_1 = 2^i$ ($1 < i < t$). Then for $\gamma \in L_0(C)$ one of the conditions 5'), 8'), 9') holds and from the condition $\gamma \in L_*(C)$ we have

that $(\gamma_2, \dots, \gamma_n) \in L_*(\tilde{C})$ or $\gamma \in \{\eta^{(2)}, \dots, \eta^{(s)}\}$. It is easy to see that the elements $\eta^{(2)}, \dots, \eta^{(s)}$ are not in the set $L_5^0 \cup L_8^0 \cup L_9^0$. Hence $(\gamma_2, \dots, \gamma_n) \in L_*(\tilde{C})$. The induction hypothesis $L_*(\tilde{C}) \cap L_0(\tilde{C}) = \emptyset$ gives that $\gamma \notin L_8^0$, and from (4.4) it follows $\gamma \notin L_5^0$. So $\gamma \in L_9^0$, that is γ coincides with some $\bar{\eta}^{(r)} = (2^i, 0, \dots, 0, 2, 0, \dots, 0)$, which contradicts the condition $(\gamma_2, \dots, \gamma_n) \in L_*(\tilde{C})$.

Suppose now $\gamma_1 = 2^i - 1$ ($1 < i \leq t$). Then for the element $\gamma \in L_*(C)$ one of the conditions 4), 5), 6) holds and from $\gamma \in L_0(C)$ it follows that $(\gamma_2, \dots, \gamma_n) \in L_0(\tilde{C})$ or $\gamma \in \{\bar{\eta}^{(2)}, \dots, \bar{\eta}^{(s)}\}$. Since for $\bar{\eta}^{(2)}, \dots, \bar{\eta}^{(s)}$ the conditions 4), 5), 6) do not hold, we have that $(\gamma_2, \dots, \gamma_n) \in L_0(\tilde{C})$ and $\gamma \in L_4^* \cup L_5^* \cup L_6^*$. From the induction hypothesis $L_*(\tilde{C}) \cap L_0(\tilde{C}) = \emptyset$ we have that $(\gamma_2, \dots, \gamma_n) \notin L_4^* \cup L_6^*$ and hence

$$(\gamma_2, \dots, \gamma_n) \in L_0(\tilde{C}) \cap N(\tilde{C}), \gamma_{s+1} + \dots + \gamma_n > 0,$$

which contradicts (4.3). So property a_2) is proved.

Let now $\gamma = (\gamma_1, \gamma_2, \dots, \gamma_n) \in L_0(C) \cap L_1(C)$. If γ such element from $L_1(C)$ for which $\gamma_1 \equiv 3 \pmod{4}$, $\gamma_1 \neq 2^i - 1$, $1 < i \leq t$, then obviously γ can not belong to the set $L_0(C)$. So for the element γ from $L_1(C)$ the conditions

$$\gamma_1 \in \{0; 2^i \ (1 < i < t); 2^i - 1 \ (1 < i \leq t)\}, (\gamma_2, \dots, \gamma_n) \in L_1(\tilde{C})$$

hold. Hence γ (as an element of the set $L_0(C)$) belongs to the set $L_1^0 \cup L_4^0 \cup L_5^0 \cup L_6^0 \cup L_8^0 \cup L_9^0$. Using the induction hypothesis $L_0(\tilde{C}) \cap L_1(\tilde{C}) = \emptyset$, it follows that $\gamma \notin L_1^0 \cup L_4^0 \cup L_8^0$. If $\gamma \in L_6^0 \cup L_9^0$, then the element $(\gamma_2, \dots, \gamma_n) \in L_1(\tilde{C})$ has the form $(0, \dots, 0, 2, 0, \dots, 0)$, which contradicts to the construction of the set $L_1(\tilde{C})$. So $\gamma \in L_5^0$, that is, $(\gamma_2, \dots, \gamma_n) \in N(\tilde{C})$. Hence from the condition $(\gamma_2, \dots, \gamma_n) \in L_1(\tilde{C})$ using (4.4) we get a contradiction. Property a_3) is proved.

Let us prove a_4). Using the induction hypothesis we have

$$|L_1^*| = |L_*(\tilde{C})| = \mu(\tilde{C}) = \frac{1}{2} \left(|\tilde{C}| - |\tilde{C}^2| - |\tilde{C}[2]| + |\tilde{C}^2[2]| \right) - r(\tilde{C}^2).$$

It is easy to see that $|L_4^*| = (t-1) |L_1^*|$, $|L_8^*| = (t-2) |L_1^*|$,

$$|L_2^*| = |\tilde{C}| - 1, |L_6^*| = (t-1) r(\tilde{C}^2), |L_9^*| = (t-2) r(\tilde{C}^2), |L_3^*| = (2^{t-2} - 1) |\tilde{C}| \text{ and } |L_7^*| = (2^{t-2} - t + 1) \left(|\tilde{C}| - |\tilde{C}^2| \right). \text{ Therefore}$$

$$\begin{aligned} & |L_1^* \cup L_4^* \cup L_6^* \cup L_8^* \cup L_9^*| = \\ & (1 + (t-1) + (t-2)) \frac{1}{2} \left(|\tilde{C}| - |\tilde{C}^2| - |\tilde{C}[2]| + |\tilde{C}^2[2]| \right) - r(\tilde{C}^2) \end{aligned}$$

and

$$\begin{aligned} |L_2^* \cup L_3^* \cup L_7^*| = \\ \left(|\tilde{C}| - 1 \right) + \left(2^{t-2} |\tilde{C}| - |\tilde{C}| \right) + (2^{t-2} - t + 1) \left(|\tilde{C}| - |\tilde{C}^2| \right) = \\ 2^{t-1} |\tilde{C}| - 1 - (t-1) \left(|\tilde{C}| - |\tilde{C}^2| \right) - 2^{t-2} |\tilde{C}^2|. \end{aligned}$$

It is clear that $|N(\tilde{C})| = |\tilde{C}[2]| - 1$ and the cardinality of the set

$$\left\{ (\gamma_1, \dots, \gamma_s, 0, \dots, 0) \in N(\tilde{C}) \right\}$$

is equal to $|\tilde{C}^2[2]| - 1$. Hence $|L_5^*| = (t-2) \left(|\tilde{C}[2]| - |\tilde{C}^2[2]| \right)$. So

$$\begin{aligned} |L_*(C)| = (t-1) \left(|\tilde{C}| - |\tilde{C}^2| - |\tilde{C}[2]| + |\tilde{C}^2[2]| \right) - r(\tilde{C}^2) + \\ (t-2) \left(|\tilde{C}[2]| - |\tilde{C}^2[2]| \right) + 2^{t-1} |\tilde{C}| - 1 - (t-1) \left(|\tilde{C}| - |\tilde{C}^2| \right) - \\ 2^{t-2} |\tilde{C}^2| = 2^{t-1} |\tilde{C}| - 2^{t-2} |\tilde{C}^2| - |\tilde{C}[2]| + |\tilde{C}^2[2]| - r(\tilde{C}^2) \end{aligned}$$

and since

$$\mu(C) = \frac{1}{2} \left(2^t |\tilde{C}| - 2^{t-1} |\tilde{C}^2| - 2 |\tilde{C}[2]| + 2 |\tilde{C}^2[2]| \right) - r(C^2),$$

it follows that property a_4) is proved.

Let $\alpha = (\alpha_1, \alpha_2, \dots, \alpha_n) \in L_*(C)$ and $\alpha_1 + \alpha_2 + \dots + \alpha_n = k$. Suppose that $\tilde{\alpha} = (\alpha_2, \dots, \alpha_n) \in L_*(\tilde{C})$. Then, by the induction hypothesis,

$$(4.5) \quad x_{\tilde{\alpha}}^* x_{\tilde{\alpha}}^{-1} = x_{(\bar{\alpha}_2, \dots, \bar{\alpha}_n)} \left(\prod_{\tilde{\tau} \in Q} x_{\tilde{\tau}} \right) \left(\prod_{\tilde{\nu} \in R} x_{\tilde{\nu}} \right) (1 + \tilde{y})$$

where $Q \subset L_*(\tilde{C})$, $R \subset L_1(\tilde{C})$, $\tilde{y} \in A^{k-\alpha_1+2}$ and $\tau_2 + \dots + \tau_n = \nu_2 + \dots + \nu_n = \alpha_2 + \dots + \alpha_n + 1$. If $\alpha_1 = 0$, then $x_{(\alpha_1, \alpha_2, \dots, \alpha_n)} = x_{(\alpha_2, \dots, \alpha_n)}$ and a_5) follows from (4.5). If $\alpha_1 = 2^i$ ($1 < i < t$), then, by Lemma 4.2,

$$x_{\alpha}^* x_{\alpha}^{-1} = x_{(\alpha_1, \bar{\alpha}_2, \dots, \bar{\alpha}_n)} \left(\prod_{\tau} x_{(\alpha_1, \tau_2, \dots, \tau_n)} \right) \left(\prod_{\nu} x_{(\alpha_1, \nu_2, \dots, \nu_n)} \right) (1 + y)$$

where $y \in A^{k+2}$. Since $(\alpha_1, \bar{\alpha}_2, \dots, \bar{\alpha}_n) = \psi(\alpha) \in L_8^0$, $\tau \in L_8^*$ and $\nu \in L_1(C)$, it follows that a_5) is proved for the elements from L_8^* . If $\alpha_1 = 2^i - 1$

($1 < i \leq t$), then, according to Lemma 4.2,

$$x_\alpha^* x_\alpha^{-1} = x_{(\alpha_1, \bar{\alpha}_2, \dots, \bar{\alpha}_n)} x_{(\alpha_1+1, \alpha_2, \dots, \alpha_n)} \cdot \left(\prod_{\tau} x_{(\alpha_1, \tau_2, \dots, \tau_n)} \right) \left(\prod_{\nu} x_{(\alpha_1, \nu_2, \dots, \nu_n)} \right) (1+y), \quad (y \in A^{k+2})$$

where $(\alpha_1, \bar{\alpha}_2, \dots, \bar{\alpha}_n) \in L_4^0$, $(\alpha_1+1, \alpha_2, \dots, \alpha_n) \in L_8^*$, $\tau \in L_4^*$ and $\nu \in L_1(C)$. Therefore a_5 is proved for the elements from L_4^* . Suppose now that $\alpha \in L_2^* \cup L_3^* \cup L_5^* \cup L_7^*$. Then, by Lemma 4.2,

$$x_\alpha^* x_\alpha^{-1} = x_{(\alpha_1+1, \alpha_2, \dots, \alpha_n)} \left(\prod_{\tau \in Q} x_{(\alpha_1, \tau_2, \dots, \tau_n)} \right) (1+y) \quad (y \in A^{k+2})$$

where the product is taken over those $\tau = (\alpha_1, \tau_2, \dots, \tau_n)$ for which $\alpha_1 + \tau_2 + \dots + \tau_n = k+1$ and

$$\tau_i = \begin{cases} \alpha_i, & \text{when } \alpha_i \text{ is divisible by 2 or } \alpha_i = q_i - 1, \\ \alpha_i + 1, & \text{when } \alpha_i \text{ is an odd number and } \alpha_i < q_i - 1. \end{cases}$$

Obviously, the element $(\alpha_1+1, \alpha_2, \dots, \alpha_n)$ coincides with $\psi(\alpha)$ and $Q = \emptyset$ whenever every α_i ($i = 2, \dots, n$) is even or equals $q_i - 1$. It is easy to see also that

$$Q \subset \begin{cases} L_*(C), & \text{when } \alpha \in L_2^* \cup L_3^*, \\ L_1(C), & \text{when } \alpha \in L_7^*. \end{cases}$$

So a_5 is proved for the elements from $L_2^* \cup L_3^* \cup L_5^* \cup L_7^*$. If α has the form $(2^i, 0, \dots, 0, 1, 0, \dots, 0)$ or $(2^i - 1, 0, \dots, 0, 1, 0, \dots, 0)$, then, by Lemma 4.2, there exists $y \in A^{k+2}$ such that the equations

$$x_\alpha^* x_\alpha^{-1} = x_{(2^i, 0, \dots, 0, 2, 0, \dots, 0)} (1+y)$$

and

$$x_\alpha^* x_\alpha^{-1} = x_{(2^i-1, 0, \dots, 0, 2, 0, \dots, 0)} x_{(2^i, 0, \dots, 0, 1, 0, \dots, 0)} (1+y)$$

hold respectively. Obviously $(2^i, 0, \dots, 0, 2, 0, \dots, 0) \in L_9^0$, $(2^i-1, 0, \dots, 0, 2, 0, \dots, 0) \in L_6^0$ and $(2^i, 0, \dots, 0, 1, 0, \dots, 0) \in L_9^*$. Therefore condition a_5 is fully proved and the lemma is true.

Theorem 4.7. *Let K be the field of 2 elements, $C = \langle a_1, \dots, a_n \rangle$ a finite abelian 2-group, $a_1, \dots, a_s$ ($s \leq n$) all basic elements of the group C with orders greater than 2, $L_*(C)$ is the set constructed above,*

$$B_0(C) = \{z_\alpha = x_\alpha^* x_\alpha^{-1} \mid x_\alpha = 1 + (a_1 + 1)^{\alpha_1} \dots (a_n + 1)^{\alpha_n}, \alpha \in L_*(C)\}$$

and $B_T(C) = \{x_\alpha \mid \alpha \in N(C)\}$. Then the elements of the set

$$B_*(C) = \{a_i \mid a_i^2 \neq 1, i = 1, \dots, n\} \cup B_T(C) \cup B_0(C)$$

form a basis of the group $V_*(KC)$.

PROOF. Let $T(C)$ denote the subgroup

$$T(C) = \left\{ 1 + \sum_{\alpha \in N(C)} \lambda_\alpha (1 + a_1)^{\alpha_1} \cdots (1 + a_n)^{\alpha_n} \mid \lambda_\alpha \in K \right\}.$$

It is easy to see that $T(C) \subset V_*(KC)$, $B_T(C)$ is a basis of the group $T(C)$ and $T(C) \cap C = \{a_i \mid a_i^2 = 1, i = 1, \dots, n\}$. According to Proposition 1.2,

$$V_*(KC) = \langle a_1, \dots, a_s \rangle \times T(C) \times D(C)$$

where, by [1], $D(C) \subset \{x^*x^{-1} \mid x \in V(KC)\}$. Therefore it suffices to prove that $B_0(C)$ is a basis of $D(C)$.

Let $L_*(C)$, $L_0(C)$ and $L_1(C)$ be the sets defined by Lemmas 4.3–4.6. Then, according to Lemmas 4.3–4.6, the sets $L_*(C)$, $L_0(C)$ and $L_1(C)$ have properties $a_1) - a_5)$. It is easy to see that the set $B_0(C)$ consists of pairwise distinct unitary elements, not equal to one.

We shall prove by induction on the exponent of C that the number of elements of order 2^i of the set $B_0(C)$ coincides with $f_i(D(C))$. If C is a group of exponent 4, then $|C^2| = |C^2[2]|$ and, according to property $a_4)$, we have that $|B_0(C)| = |L_*(C)| = \mu(C) = \frac{1}{2}(|C| - |C[2]|) - r(C^2)$ which, by Proposition 1.2, equals $f_1(D(C))$. Suppose now that C is a group of exponent greater than 4 and the number of elements of order 2^i of the set $B_0(C^2)$ equals $f_i(D(C^2))$ ($i = 1, 2, 3, \dots$). It is easy to prove that $(D(C))^2 = D(C^2)$ (see [1]) and hence the number of elements of order 2^i of the set $B_0(C)$ coincides with $f_{i-1}(D(C^2)) = f_i(D(C))$ ($i = 2, 3, \dots$). Therefore $f_1(D(C)) = |B_0(C)| - |B_0(C^2)|$ and, by property $a_4)$, $f_1(D(C)) = \mu(C) - \mu(C^2)$ which coincides with the number defined by Proposition 1.2. The statement is proved.

Let us prove the independence of $B_0(C)$. We shall use again induction on the exponent of C . Let C be a group of exponent 4. Then every element from $B_0(C)$ has order 2. Suppose that

$$(4.6) \quad z_{\alpha^{(1)}} \cdots z_{\alpha^{(r)}} = 1$$

for the distinct elements $\alpha^{(i)} = (\alpha_1^{(i)}, \dots, \alpha_n^{(i)})$ ($i = 1, \dots, r$) from $L_*(C)$. Let $k = \min_{1 \leq i \leq r} \{\alpha_1^{(i)} + \dots + \alpha_n^{(i)}\}$. Without loss of generality we can assume that $k = \alpha_1^{(1)} + \dots + \alpha_n^{(1)} = \dots = \alpha_1^{(s)} + \dots + \alpha_n^{(s)}$ for some $s \leq r$. Then,

according to property a_5), we have that for every $i = 1, \dots, s$

$$z_{\alpha^{(i)}} = x_{\bar{\alpha}^{(i)}} v_i w_i (1 + y_i) \quad (y_i \in A^{k+2})$$

where $\bar{\alpha}^{(i)} \in L_0(C)$, $v_i = \prod_{\tau \in Q_i \subset L_*(C)} x_\tau$ and $w_i = \prod_{\nu \in R_i \subset L_1(C)} x_\nu$. Hence

$$u = z_{\alpha^{(1)}} \cdots z_{\alpha^{(r)}} = (x_{\bar{\alpha}^{(1)}} \cdots x_{\bar{\alpha}^{(s)}})(v_1 \cdots v_s)(w_1 \cdots w_s)(1 + y),$$

where $y \in A^{k+2}$, $\bar{\alpha}^{(1)}, \dots, \bar{\alpha}^{(s)} \in L_0(C)$, $v_1 \cdots v_s = \prod_{\tau \in Q \subset L_*(C)} x_\tau$ and

$$w_1 \cdots w_s = \prod_{\nu \in R \subset L_1(C)} x_\nu. \text{ According to (4.1), } u + A^{k+2} =$$

$$= 1 + \sum_{i=1}^s (x_{\bar{\alpha}^{(i)}} + 1) + \sum_{\tau \in Q \subset L_*(C)} (x_\tau + 1) + \sum_{\nu \in R \subset L_1(C)} (x_\nu + 1) + A^{k+2}.$$

Since, by properties a_2) and a_3), the sets $L_*(C) \cup L_1(C)$ and $L_0(C)$ are disjoint, it follows that $\{\bar{\alpha}^{(1)}, \dots, \bar{\alpha}^{(s)}\} \cap (Q \cup R) = \emptyset$. Obviously the set $\{\bar{\alpha}^{(1)}, \dots, \bar{\alpha}^{(s)}\}$ is not empty and, by Lemma 2.1, the elements $(x_{\bar{\alpha}^{(i)}} + 1)$, $(x_\tau + 1)$, $(x_\nu + 1)$ are the distinct basic elements of the additive group of the factor-ring A^{k+1}/A^{k+2} . Then $u + A^{k+2} \neq 1 + A^{k+2}$, which contradicts (4.6). The independence of the set $B_0(C)$ is proved for the group C of exponent 4.

Let C be a group of exponent greater than 4. Suppose that for some distinct elements $\alpha^{(1)}, \dots, \alpha^{(r)}$ from $L_*(C)$ the equation

$$(4.7) \quad u = (z_{\alpha^{(1)}})^{j_1} \cdots (z_{\alpha^{(r)}})^{j_r} = 1$$

holds. If every $j_i = 2t_i$ ($i = 1, \dots, r$), then the elements $z_{\tau^{(i)}} = (z_{\alpha^{(i)}})^2$ belong to the set $B_0(C^2)$ and, according to (4.7), the equation

$$(z_{\tau^{(1)}})^{t_1} \cdots (z_{\tau^{(r)}})^{t_r} = 1$$

holds, which contradicts the induction hypothesis. If $j_i = 2t_i + 1$ ($i = 1, \dots, s$) are all the odd ones among the numbers $j_1, \dots, j_r$, then equation (4.7) has the form

$$(4.8) \quad u = z_{\alpha^{(1)}} \cdots z_{\alpha^{(s)}} v^2 = 1$$

and $v^2 \in D(C^2)$. It is easy to see that $y = z_{\alpha^{(1)}} \cdots z_{\alpha^{(s)}} \notin D(C^2)$. Indeed, as in above we can assume that

$$k = \min_{1 \leq i \leq s} \{\alpha_1^{(i)} + \cdots + \alpha_n^{(i)}\} = \alpha_1^{(1)} + \cdots + \alpha_n^{(1)} = \cdots = \alpha_1^{(s)} + \cdots + \alpha_n^{(s)}.$$

So, according to Lemmas 4.3–4.6,

$$z_{\alpha^{(i)}} = x_{\bar{\alpha}^{(i)}} v_i w_i (1 + y_i) \quad (y_i \in A^{k+2})$$

where $\bar{\alpha}^{(i)} \in L_0(C)$, $v_i = \prod_{\tau \in Q_i \subset L_*(C)} x_\tau$ and $w_i = \prod_{\nu \in R_i \subset L_1(C)} x_\nu$. Using (4.1) we have

$$y + A^{k+2} = 1 + \sum_{i=1}^s (x_{\bar{\alpha}^{(i)}} + 1) + \sum_{\tau \in Q} (x_\tau + 1) + \sum_{\nu \in R} (x_\nu + 1) + A^{k+2}$$

where $Q = Q_1 \cup \dots \cup Q_s \subset L_*(C)$ and $R = R_1 \cup \dots \cup R_s \subset L_1(C)$. By Lemma 2.1, the elements $x_{\bar{\alpha}^{(i)}} + 1$ ($i = 1, \dots, s$), $x_\tau + 1$ ($\tau \in Q$), $x_\nu + 1$ ($\nu \in R$) are the distinct basic elements of the additive group of the factor-ring A^{k+1}/A^{k+2} . According to properties $a_1) - a_3)$, $\{\bar{\alpha}^{(1)}, \dots, \bar{\alpha}^{(s)}\} \cap (Q \cup R) = \emptyset$. Therefore, if among the elements $\bar{\alpha}^{(1)}, \dots, \bar{\alpha}^{(s)}$ exists at least one $\bar{\alpha}^{(j)}$ which belongs to the set $L(C)$, then obviously $y \notin D(C^2)$. Suppose now that every $\bar{\alpha}^{(1)}, \dots, \bar{\alpha}^{(s)}$ belongs to the set $L_2(C)$. According to Lemma 4.2, it can may be only in case when every $\bar{\alpha}^{(i)}$ consists only one odd component which, by the construction of the set $L_*(C)$, is congruent with one modulo 4. Without loss of generality we can assume that $\bar{\alpha}_1^{(i)}$ is the only one odd number among the the components of the element $\bar{\alpha}^{(i)} = \tau$. Then Lemma 4.2 gives that

$$z_\tau = x_{(\tau_1+1, \tau_2, \dots, \tau_n)} x_{(\tau_1+2, \tau_2, \dots, \tau_n)} \prod_{\nu \in S_i} x_{(\tau_1, \nu_2, \dots, \nu_n)} (1 + y)$$

where $y \in A^{k+3}$, $S_i \subset L_*(C)$ (see the construction of the set $L_*(C)$) and the product is taken over all $\nu = (\tau_1, \nu_2, \dots, \nu_n)$ such that $\tau_1 + \nu_2 + \dots + \nu_n = k + 2$ and

$$\nu_j = \begin{cases} \tau_j, & \text{when } \tau_j \equiv 0 \pmod{4} \text{ or } \tau_j = q_j - 2, \\ \tau_j + 2, & \text{when } \tau_j \equiv 2 \pmod{4} \text{ and } \tau_j < q_j - 2. \end{cases}$$

Since $\tau_1 \equiv 1 \pmod{4}$, it follows that the element $\tilde{\alpha}^{(i)} = (\tau_1 + 2, \tau_2, \dots, \tau_n)$ belongs to the set $L(C) \setminus L_*(C)$. Therefore $\{\tilde{\alpha}^{(1)}, \dots, \tilde{\alpha}^{(s)}\}$ and $S_1 \cup \dots \cup S_s$ are the disjoint subsets of the set $L(C)$. Hence, in the expression $y + A^{k+3}$ we can write the element y using (4.1), and, as in above, we can prove that $z_{\alpha^{(1)}} \dots z_{\alpha^{(s)}} \notin D(C^2)$.

So it follows from (4.8) that $z_{\alpha^{(1)}} \dots z_{\alpha^{(s)}} = 1$. This equation can not hold in the group $V(KC)$ for the distinct elements $\alpha^{(i)} = (\alpha_1^{(i)}, \dots, \alpha_n^{(i)})$

($i = 1, \dots, s$) from $L_*(C)$. Really, let $k = \min_{1 \leq i \leq s} \{ \alpha_1^{(i)} + \dots + \alpha_n^{(i)} \}$. Without loss of generality we can assume that $k = \alpha_1^{(1)} + \dots + \alpha_n^{(1)} = \dots = \alpha_1^{(s)} + \dots + \alpha_n^{(s)}$. Then, according to property a_5), we have that for every $i = 1, \dots, s$

$$z_{\alpha^{(i)}} = x_{\bar{\alpha}^{(i)}} v_i w_i (1 + y_i) \quad (y_i \in A^{k+2})$$

where $\bar{\alpha}^{(i)} \in L_0(C)$, $v_i = \prod_{\tau \in Q_i \subset L_*(C)} x_\tau$ and $w_i = \prod_{\nu \in R_i \subset L_1(C)} x_\nu$. Hence

$$u = z_{\alpha^{(1)}} \cdots z_{\alpha^{(s)}} = (x_{\bar{\alpha}^{(1)}} \cdots x_{\bar{\alpha}^{(s)}}) (v_1 \cdots v_s) (w_1 \cdots w_s) (1 + y),$$

where $y \in A^{k+2}$, $\bar{\alpha}^{(1)}, \dots, \bar{\alpha}^{(s)} \in L_0(C)$, $v_1 \cdots v_s = \prod_{\tau \in Q \subset L_*(C)} x_\tau$ and

$$w_1 \cdots w_s = \prod_{\nu \in R \subset L_1(C)} x_\nu. \text{ According to (4.1), } u + A^{k+2} =$$

$$= 1 + \sum_{i=1}^s (x_{\bar{\alpha}^{(i)}} + 1) + \sum_{\tau \in Q \subset L_*(C)} (x_\tau + 1) + \sum_{\nu \in R \subset L_1(C)} (x_\nu + 1) + A^{k+2}.$$

Since, by properties a_2) and a_3), the sets $L_*(C) \cup L_1(C)$ and $L_0(C)$ are disjoint, it follows that $\{ \bar{\alpha}^{(1)}, \dots, \bar{\alpha}^{(s)} \} \cap (Q \cup R) = \emptyset$. Obviously the set $\{ \bar{\alpha}^{(1)}, \dots, \bar{\alpha}^{(s)} \}$ is not empty and, by Lemma 2.1, the elements $(x_{\bar{\alpha}^{(i)}} + 1)$, $(x_\tau + 1)$, $(x_\nu + 1)$ are the distinct basic elements of the additive group of the factor-ring A^{k+1}/A^{k+2} . Then $u + A^{k+2} \neq 1 + A^{k+2}$, so we get a contradiction. The independence of the set $B_0(C)$ is proved. The proof of the theorem is complete.

Theorem 4.8. *Let K be the field of 2^m ($m > 1$) elements, $\varepsilon, \varepsilon^2, \dots, \varepsilon^{2^{m-1}}$ a basis of K over $GF(2)$, C a finite abelian 2-group, $x(i, \alpha) = 1 + \varepsilon^{2^i} (a_1 - 1)^{\alpha_1} \cdots (a_n - 1)^{\alpha_n}$,*

$$B_1(C) = \left\{ x(i, \alpha)^* x(i, \alpha)^{-1} \mid 0 \leq i < m, \alpha \in L_*(C) \right\},$$

$$B_2(C) = \left\{ \left(1 + \varepsilon^{2^i} (1 + a_j) \right)^* \left(1 + \varepsilon^{2^i} (1 + a_j) \right)^{-1} \mid 0 \leq i < m - 1, \right.$$

$$\left. a_j^2 \neq 1 \right\}$$

and $B_T(C) = \{ x(i, \alpha) \mid 0 \leq i < m, \alpha \in N(C) \}$. Then

$$B_*(C) = \{ a_i \mid a_i^2 \neq 1, i = 1, \dots, n \} \cup B_T(C) \cup B_1(C) \cup B_2(C)$$

is a basis for $V_*(KC)$.

PROOF. Let us write the identity element of K in the form

$$1 = \gamma_0\varepsilon + \gamma_1\varepsilon^2 + \cdots + \gamma_{m-1}\varepsilon^{2^{m-1}}.$$

Raising this equation to the powers $2, 4, 8, \dots$ we get that $\gamma_0 = \gamma_1 = \cdots = \gamma_{m-1} = 1$. Therefore the elements $1, \varepsilon, \varepsilon^2, \dots, \varepsilon^{2^{m-2}}$ of the field K are independent over $GF(2)$. From this the independence of the set $C \cup B_2(C)$ follows by Lemma 2.2 and as in the proof of Theorem 4.7 we can prove this theorem too.

Theorem 4.9. *Let K be the field of 2^m elements, C a Sylow 2-subgroup of a finite abelian group $G = C \times F$, E a subset of the set $F \setminus \{1\}$, that has a unique representative in every subset of the form $\{g, g^{-1}\}$,*

$$\tilde{B}(G) = \left\{ x(i, g, \alpha)^* x(i, g, \alpha)^{-1} \mid x(i, g, \alpha) \in B(G), g \in E \right\}$$

and $B_*(C)$ is a basis of $V_*(KC)$. Then the elements of the set

$$B_*(G) = \tilde{B}(G) \cup B_*(C)$$

form a basis of the Sylow 2-subgroup $W_2(KG)$ of the group $V_*(KG)$.

PROOF. Let $k = \alpha_1 + \cdots + \alpha_n$ and

$$z(\alpha_1, \dots, \alpha_n) = (a_1 - 1)^{\alpha_1} \cdots (a_n - 1)^{\alpha_n}.$$

Using equation (3.1) it is easy to prove that

$$x(i, g, \alpha)^* = 1 + \varepsilon^{2^i} g^{-1} z(\alpha_1, \dots, \alpha_n) + v_1$$

and

$$x(i, g, \alpha)^{-1} = 1 + \varepsilon^{2^i} g z(\alpha_1, \dots, \alpha_n) + v_2$$

where the elements v_1 and v_2 belong to the $(k+1)$ -th power of the ideal $J = J(C)$ of the group algebra KG . Hence

$$x(i, g, \alpha)^* x(i, g, \alpha)^{-1} = 1 + \varepsilon^{2^i} (g + g^{-1}) z(\alpha_1, \dots, \alpha_n) + v \quad (v \in J^{k+1})$$

and as in the proof of theorem 4.7 we can prove that the elements of the set $\tilde{B}(G)$ are independent and belong to the basis of the group $W_2(KG)$. According to Lemma 2.2, the elements of the set $\tilde{B}(G) \cup B_*(C)$ are independent and form a basis of $W_2(KG)$. Indeed, since

$$|\tilde{B}(G)| = m \frac{|F| - 1}{2} (|C| - |C^2|) \text{ and}$$

$|B_*(C)| = \frac{m}{2} (|C| - |C^2| + |C[2]| + |C^2[2]| - 2)$, it follows that the cardinality of the set $\tilde{B}(G) \cup B_*(C)$ coincides with the 2-rank of the group $W_2(KG)$. This completes the proof of the theorem.

References

- [1] A. A. BOVDI and A. A. SZAKÁCS, The unitary subgroup of the group of units in a modular group algebra of a finite abelian p -group,, *Math. Zametki. (6)* **45** (1989), 23–29, (in Russian) (see English translation in *Math. Notes, (5–6)* **45** (1989), 445–450.).
- [2] R. SANDLING, Units in the modular group algebra of a finite abelian p -group, *J. Pure Appl. Algebra.* **33** (1984), 337–346.
- [3] R. LIDL and H. NIEDERREITER, Finite fields, *Addison-Wesley Publishing Company, London–Amsterdam–Don Mills, Ontario–Sydney–Tokyo*, 1983.
- [4] D. S. PASSMAN, The algebraic structure of group rings, *New York: Interscience*, 1977.

ADALBERT BOVDI
INSTITUTE OF MATHEMATICS,
KOSSUTH LAJOS UNIVERSITY,
H-4010 DEBRECEN, PF. 12,
HUNGARY

ATTILA SZAKÁCS
DEPARTMENT OF MATHEMATICS,
ESZTERHÁZY KÁROLY UNIVERSITY,
LEÁNYKA U. 4,
3301 EGER,
HUNGARY

(Received February 23, 1994)