Filtered Multiplicative Basis and Group of Units of Group Algebra

Doktori (PhD) értekezés

Balogh Zsolt Ádám

Debreceni Egyetem
Természettudományi Kar
Debrecen, 2004

II

Ezen értekezést a Debreceni Egyetem TTK *Matematika- és számítástudományok* doktori iskola *Csoportalgebrák és alkalmazásai* programja keretében készítettem a Debreceni Egyetem TTK doktori (Ph.D.) fokozatának elnyerése céljából.

Debrecen, 2005.

_____

a jelölt aláírása

Tanúsítom, hogy Balogh Zsolt Ádám doktorjelölt 1998 – 2004 között a fent megnevezett Doktori alprogram keretében irányításommal végezte munkáját. Az értekezésben foglaltak a jelölt önálló munkáján alapulnak, az eredményekhez önálló alkotó tevékenységével meghatározóan hozzájárult. Az értekezés elfogadását javasolom.

Debrecen, 2005.

_____

a témavezető aláírása

Acknowledgements

I would like to express my gratitude to my supervisor, Professor A. Bovdi for his invaluable ideas and his continuous encouragement during the years of the preparation of this work. I also would like to thank V. Bovdi for his careful proof-reading this work and for his advice and remarks to improve this thesis.

II

Contents

Chapter 1

Introduction

1.1 Preliminaries

The concept of a group algebra was introduced during the study of representation of groups. They are, however applied in numerous fields of mathematics as well, such as homology, cohomology and algebraic topology. It was Frobenius who first used this interesting algebraic construction consisting of fields and groups, by the help of it he studied representations of finite groups. The coinage group algebra comes from Noether.

The study of group algebras started at the begining of the 30s of the past century, mainly with the results of Frobenius, Schur, Magnus, Noether, Higman and Jennings. The most fundamental characterization theorems were proved during the 1960s and since then diverse fields of research have developed. Today the major directions of research include, besides the study of ring theoretical properties of the group algebras, the examination of groups of units of group algebras and their associated Lie algebras.

Our notation is standard. Let G be a group and $\mathbb{F}$ a field with unity 1. Denote by $\mathbb{F}G$ the all formal sums $\sum_{g\in G}\alpha_g g$, where only finite coefficient $\alpha_g \in \mathbb{F}$ is not zero. Evidently, $\mathbb{F}G$ is a vector space over $\mathbb{F}$ with basis G. The multiplication of the group G induces a multiplication on $\mathbb{F}G$. Then $\mathbb{F}G$ is an algebra over the field $\mathbb{F}$ which is called

group algebra. In the special case when $\mathbb{F}$ is a field of characteristic p and G contains an element of order p, $\mathbb{F}G$ is called *modular group algebra*.

Let the mapping $\chi : \mathbb{F}G \to \mathbb{F}$ be given by

$$\chi\Big(\sum_{g\in G} \alpha_g g\Big) = \sum_{g\in G} \alpha_g$$

for any elements $\sum_{g\in G} \alpha_g g \in \mathbb{F}G$. Then χ is a homomorphism and is called *augmentation mapping*. The kernel of χ is the *augmentation ideal*, which is denoted by $A(\mathbb{F}G)$.

If H is a normal subgroup of G then the set

$$I(H) = \big\{\ (h-1)x \ \big|\ h \in H,\ x \in \mathbb{F}G\ \big\}$$

is a two-sided ideal of $\mathbb{F}G$. Clearly, the ideals $A(\mathbb{F}G)$ and $I(G)$ coincide. The isomorphism $\mathbb{F}G/I(H) \cong \mathbb{F}(G/H)$ is called the isomorphism theorem of group algebra.

Now let us mention a problem originating from Higman and Thrall, and which exerted a great influence on the study of the structure of group algebras and their groups of units.

If the group algebras $\mathbb{F}G$ and $\mathbb{F}H$ are isomorphic as algebras over the field $\mathbb{F}$ then what is the relation between the groups G and H, and under what conditions are G and H isomorphic?

Deskins [26] gave a positive answer to this isomorphism problem for finite abelian p-groups. Numerous authors have investigated this question with nonabelian groups which has not been solved so far. Baginski [3] solved the problem above for group algebras of 2-groups of maximal class over the field of elements two. Additional results can be found in the survey article of Sandling [42].

A large part of the theory of group algebras consists of examinations of ring theoretical properties. In this field the results have been profound for which an excellent source is books by Passman [41] and Bovdi [22].

The set of units $U(\mathbb{F}G)$ of the group algebra $\mathbb{F}G$ forms a group and its subset

$$V(\mathbb{F}G) = \Big\{ \sum_{g\in G} \alpha_g g \in U(\mathbb{F}G) \;\Big|\; \sum_{g\in G} \alpha_g = 1 \Big\}$$

is a normal subgroup, which is called *normalized group of units*. It is well known fact that $U(\mathbb{F}G)$ is isomorphic to the direct product $V(\mathbb{F}G) \times U(\mathbb{F})$, where $U(\mathbb{F})$ is the group of units of the field $\mathbb{F}$. To get information on the group of units $U(\mathbb{F}G)$ it is enough to examine the normalized group of units $V(\mathbb{F}G)$ instead of the examination of the full group of units $U(\mathbb{F}G)$. A good survey of this theory can be found in Artamonov and Bovdi [1] and Bovdi [11], [22].

The subject of this thesis is the examination of filtered multiplicative bases and groups of units of group algebras. First of all let us mention some general remarks which will be used throughout this thesis. The Frattini subgroup and the center of G will be denoted by $\Phi(G)$ and $\zeta(G)$, respectively. It is well known that the Frattini subgroup $\Phi(G)$ coincides with $G'G^p$ for finite p-groups G, where

$$G^p = \langle\ g^p \mid g \in G\ \rangle$$

and G' is the commutator subgroup of G. Let $\gamma_1(G) = G$ and

$$\gamma_{i+1}(G) = \big(\gamma_i(G), G\big).$$

The series of subgroups of G with the property

$$\gamma_1(G) \supseteq \gamma_2(G) \supseteq \cdots \supseteq \gamma_i(G) \supseteq \cdots$$

is called *lower central series*. Evidently, $\gamma_2(G)$ coincides with the commutator subgroup G'.

1.2 Structure of group of units

Let G be a finite p-group and $\mathbb{F}_p$ the field of p elements. Then the fundamental ideal $A(\mathbb{F}_pG)$ is nilpotent, and the normalized group

of units $V(\mathbb{F}_pG)$ coincides with $1 + A(\mathbb{F}_pG)$. Therefore, the element $\sum_{g\in G}\alpha_g g$ of group algebra $\mathbb{F}_pG$ is in the normalized group of units if and only if $\sum_{g\in G}\alpha_g = 1$. That is why the order of the normalized group of units $V(\mathbb{F}_pG)$ is $p^{|G|-1}$.

After the simple groups had been described, the structure of finite p-groups became the focus of studies on group theory, the study of groups of units of group algebras of finite p-groups has become topical.

In the following, let G be a finite nonabelian p-group. Bovdi's article [11] gives a survey of the theory of the normalized group of units $V(\mathbb{F}G)$. According to the results of Coleman and Passman [25] the group $V(\mathbb{F}G)$ is non p-regular, and its exponent is at least p^2. Due to its complicated structure the study of the group $V(\mathbb{F}G)$ necessitates the use of methods borrowed from other areas of algebra, besides means of group theory.

Bovdi and Khripta [12] applied first the Lie algebraic methods to investigate the normalized group of units. Du [27] showed that in the associated Lie algebra of the fundamental ideal $A(\mathbb{F}_pG)$ the kth member of the upper Lie central series $\gamma_k\big(A(\mathbb{F}_pG)\big)$ determines the kth member of the upper central series of $V(\mathbb{F}_pG)$, which coincides with $1+\gamma_k\big(A(\mathbb{F}_pG)\big)$. Bovdi and Polcino Milies [14] proved that Du's result is valid for normal subgroups of $V(\mathbb{F}_pG)$ as well.

In the first part of this thesis we investigate the structure of $V(\mathbb{F}_2G)$, where G is a group of maximal class of order 2^n, that is, its nilpotency class is $n-1$. It is well known that the 2-groups of maximal class are the following extensions of $C = \langle\ a\ \mid\ a^{2^n} = 1\ \rangle$:

$$\begin{aligned}
Q_{2^{n+1}} &= \langle\ a, b_1\ \mid\ a^{2^n} = 1, b_1^2 = a^{2^{n-1}}, (a, b_1) = a^{-2}\rangle \text{ with } n \geq 2;\\
D_{2^{n+1}} &= \langle\ a, b_2\ \mid\ a^{2^n} = 1, b_2^2 = 1, (a, b_2) = a^{-2}\rangle \text{ with } n \geq 2;\\
SD_{2^{n+1}} &= \langle\ a, b_3\ \mid\ a^{2^n} = 1, b_3^2 = 1, (a, b_3) = a^{-2+2^{n-1}}\rangle \text{ with } n \geq 3.
\end{aligned}$$

One of the main results of the thesis is the description of the structure of the element of order two of $V(\mathbb{F}_2G)$, and giving their numbers. Let us denote by $\Theta_G(2)$ the number of the elements of order two in the

normalized group of units $V(\mathbb{F}_2G)$. Then

$$\Theta_{D_{2^{n+1}}}(2) = 2^{2^n+n-1} + 2^{2^n};$$
$$\Theta_{SD_{2^{n+1}}}(2) = 2^{2^n+n-1};$$
$$\Theta_{Q_{2^{n+1}}}(2) = 2^{2^n+n-1} - 2^{2^n}.$$

To prove of this theorem we use Jennings's results [34] on the basis S of the ideal $A(\mathbb{F}_pG)$. Then the set $1+S$ forms a generator system of $V(\mathbb{F}_pG)$. Apart from the well-known properties of the group of units, the individual subgroups of the group of units, just like the unitary subgroup, play a major role.

Let us mention that the mapping $x \mapsto x^\sigma$ of the group algebra $\mathbb{F}_pG$ is called *involution*, if

$$(x+y)^\sigma = x^\sigma + y^\sigma, \quad (xy)^\sigma = y^\sigma x^\sigma, \quad \text{and} \quad (x^\sigma)^\sigma = x.$$

The set

$$V_\sigma(\mathbb{F}_pG) = \{\ x \in V(\mathbb{F}_pG)\ \mid\ x^{-1} = x^\sigma\ \}$$

is a subgroup of the group $V(\mathbb{F}_pG)$, which is called *σ-unitary subgroup*. For example, the canonical mapping

$$x = \sum_{g\in G} \alpha_g g \mapsto x^* = \sum_{g\in G} \alpha_g g^{-1}$$

is the $*$-involution of $\mathbb{F}_pG$.

During our investigations, the order of the σ-unitary subgroup $V_\sigma(\mathbb{F}_2C)$ pertaining to the cyclic group $C = \langle\ a\ \mid\ a^{2^n} = 1\ \rangle$ has been given a major role. The order of the commutative $*$-unitary subgroup $V_*(\mathbb{F}_pG)$ has been described by Bovdi and Sakach [15] for finite abelian p-groups G. Le us note that the order of $V_*(\mathbb{F}_pG)$ has been given by Bovdi [20], Bovdi and Rozgonyi [21] for some nonabelian groups G.

With regard to a σ-involution the set

$$S_\sigma(G) = \{\ x \in V(\mathbb{F}_pG)\ \mid\ x = x^\sigma\ \}$$

has great importance as well, and the elements of the set $S_\sigma(G)$ are called *σ-symmetric elements*. In the case of canonical involution the

order of the commutative unitary subgroup $V_*(\mathbb{F}_pG)$ has been determined by Bovdi and Sakach [15] for abelian p-groups G. Let us note that the set $S_\sigma(G)$ is a subgroup of the group of units for finite abelian groups G, but generally it is not true for nonabelian groups. The paper of Bovdi and Kovács [19] determines the groups G for which $S_\sigma(G)$ is a subgroup.

Let us denote by $\circledast$ the linearly extension of the automorphism $a^i \mapsto a^{(2^{n-1}-1)i}$ of the group C to the group algebra $\mathbb{F}_2C$. This extension is also an involution of the algebra $\mathbb{F}_2C$. We proved that the equation

$$\left|V_{\circledast}(\mathbb{F}_2C)\right| = \frac{\left|V_*(\mathbb{F}_2C)\right|}{2}$$

holds for the order of the unitary subgroups, belonging to the involutions $*$ and $\circledast$. These results form the basis of the first part of the thesis.

The question raised by Berman, is called the isomorphism problem of the normalized group of units, is a more general and considerably more difficult question than the isomorphism problem of modular group algebras:

Assume that the normalized groups of units $V(\mathbb{F}_pG)$ and $V(\mathbb{F}_pH)$ are isomorphic. Under which conditions are groups G and H isomorphic?

In 1967 Berman [9] solved this problem for finite abelian p-groups. An interesting consequence of our results above is that the Berman's question is true for 2-groups of maximal class.

An other actual problem in the theory of finite p-groups is the description of the pth power structure. The results achieved during these inquiries made it possible to prove many theorems in the theory of finite p-groups. These inquiries have not been extended to normalized group of units $V(\mathbb{F}_pG)$ of group algebra $\mathbb{F}_pG$.

Baginski [2], Shalev and Mann [39, 43] proved that the nilpotency class of $V(\mathbb{F}_pG)$ is equal to p if and only if the commutator subgroup of G is of order p. Further results pertaining to nilpotency class of group of units of group algebras can be found in Khripta's article

[36]. He described all group algebras with group of units of nilpotency class two, as well as in the paper of Bovdi and Kurdics [13] those group algebras can be found whose group of units is of nilpotency class three.

Let G be a group with commutator subgroup G' of order p. In this case we examine the power structure of $V(\mathbb{F}_pG)$. We verify that if the nilpotency class of $V(\mathbb{F}_pG)$ is odd p prime then $V(\mathbb{F}_pG)^p$ is a central subgroup of the normalized group of units, consequently the further powers can be easy determined. Moreover, if the Frattini subgroup of G is of order p then we can describe the structure of the group $V(\mathbb{F}_pG)^p$. Let $C_{g_1}, C_{g_2}, \ldots, C_{g_t}$ be the all conjugacy classes of G, which consists of at least two elements, and $N = \prod_{i=1}^{t} \langle 1 + \widehat{C_{g_i}} \rangle$, where $\widehat{C_{g_i}}$ is the sum of all elements of C_{g_i}. Then we can prove that

$$V(F_pG)^p = V\left(\mathbb{F}_pG^p\right) \times N.$$

The question is that, is it true the equation

$$G^p = V(\mathbb{F}_pG)^p \cap G$$

is also attached to the power structure of normalized group of units. This question can be found in Johnson's paper [35]. Using the previous results of the power structure, we prove that if G is a p-group with Frattini subgroup of order p ($p > 2$) then the pth power of the group G coincides with the intersection of the pth power of the normalized group of units $V(\mathbb{F}_pG)$ and the group G.

An other main theorem of this thesis is that the isomorphism class of the group $V(\mathbb{F}_pG)$ determines the isomorphism class of the group G if G is a group of cyclic Frattini subgroup and $p > 2$.

The basis of proving these results is the power structure of $V(\mathbb{F}_pG)$ and the description of Berger, Kovács and Newman [8] on the finite p-groups with cyclic Frattini subgroups.

1.3 Filtered multiplicative basis

In the fourth chapter of this thesis we investigate the bases of the group algebra over the field $\mathbb{F}$ of characteristic p. In 1960s Kupisch

introduced the concept of the filtered multiplicative basis of algebras. Let A be a finite-dimensional algebra over a field $\mathbb{F}$ with the Jacobson radical $rad\,(A)$ and $\mathbb{F}$-basis B. Assume that B, an $\mathbb{F}$-basis, has the following properties:

1. if $u, v \in B$ then either $u \cdot v = 0$ or $u \cdot v \in B$;
2. $B \cap rad\,(A)$ is an $\mathbb{F}$-basis for $rad\,(A)$.

Then B is called a *filtered multiplicative* $\mathbb{F}$*-basis* of the algebra A.

The significance of the filtered multiplicative basis for algebras with finitely many indecomposable representations has been given by the research of Bautista, Gabriel, Roiter, and Salmeron [7]. They showed that if there are only finitely many isomorphism classes of indecomposable A-modules over an algebraically closed field $\mathbb{F}$, then A has a filtered multiplicative $\mathbb{F}$-basis. That problem when the group algebra $\mathbb{F}G$ has a filtered multiplicative basis was raised by the paper of Bautista, Gabriel, Roiter, and Salmeron [7].

Higman [30] proved that the group algebra $\mathbb{F}G$ has only finitely many isomorphism classes of indecomposable $\mathbb{F}G$-modules if and only if all the Sylow p-subgroups of G are cyclic.

In 1978, Landrock and Michler [38] proved that the group algebra of the smallest Janko group over a field of characteristic 2 does not have a filtered multiplicative $\mathbb{F}$-basis. In 1987, Paris [40] gave an example for nonabelian group algebra $\mathbb{F}G$ which has a filtered multiplicative $\mathbb{F}$-basis.

The systematic study of filtered multiplicative $\mathbb{F}$-basis has been begun by Bovdi [16]. In [16] the following theorem is proved: Let G be a finite metacyclic p-group and $\mathbb{F}$ a field of characteristic p. Then the group algebra $\mathbb{F}G$ possesses a filtered multiplicative $\mathbb{F}$-basis if and only if $p = 2$ and either G is a dihedral 2-group or G is the quaternion group of order 8 and $\mathbb{F}$ contains a primitive cube root of the unity.

In [17] an explicit list of all p-groups G of order p^m with a cyclic subgroup of order p^{m-2} is given, such that the group algebra $\mathbb{F}G$ over a field $\mathbb{F}$ of characteristic p has a filtered multiplicative $\mathbb{F}$-basis. Further Bovdi [17] proved that the group algebras of the powerful groups does not have a filtered multiplicative $\mathbb{F}$-basis.

In the fourth chapter we give a complete list of all p-groups G of order less than p^5, such that the group algebra $\mathbb{F}G$ has a filtered multiplicative $\mathbb{F}$-basis, and we give these bases as well. This result suggests that a group algebra $\mathbb{F}G$ has a filtered multiplicative $\mathbb{F}$-basis only if $p = 2$.

Group algebras of all groups of order 2^5 which contain filtered multiplicative $\mathbb{F}$-basis are also described. For the inquiry we used the computer algebra system GAP [28] and its package LAGUNA [18]. In the theorem, indices that appear in the list of groups are identical with the GAP numbers identifying the groups. Moreover we proved that the group algebras of the groups

$$G = \langle\ a, b\ \mid\ a^{2^n} = b^2 = c^2 = d^2 = 1,\ \ (a,b) = c,\ \ (a,c) = d,\\ (a,d) = (b,c) = (b,d) = (c,d) = 1\ \rangle$$

does not have filtered multiplicative $\mathbb{F}$-basis. Finally we give a filtered multiplicative $\mathbb{F}$-basis of the group algebra $\mathbb{F}G$, where

$$G = \langle\ a, b\ \mid\ a^{2^n} = b^{2^m} = c^2 = 1,\ \ (a,b) = c,\ \ (a,c) = 1,\ \ (b,c) = 1\ \rangle,$$

and $n, m \geq 2$, so we describe the algebra $\mathbb{F}G$.

Chapter 2

Units of group algebras of 2-groups of maximal class

2.1 Preliminary results

This chapter includes results of [6].

We observe some facts about abelian 2-groups and their group algebras. Let $C = \langle\ a \mid a^{2^n} = 1\ \rangle$ be the cyclic group of order 2^n, where $n \geq 2$. For C the order of the unitary subgroup $V_*(\mathbb{F}_2C)$ can be calculate from [15]:

Proposition 2.1.1 (A. Bovdi, A. Sakach [15]). *The order of* $V_*(\mathbb{F}_2C)$ *is*

$$\left|C^2[2]\right| \cdot \left|\mathbb{F}_2\right|^{\frac{1}{2}(|C|+|C[2]|)-1} = 2^{2^{n-1}+1}.$$

Recall that for the group algebra $\mathbb{F}_2C$ of C the subset

$$\left\{1,\, 1+a,\, (1+a)^2, \ldots, (1+a)^{2^n-1}\right\} \tag{2.1}$$

is a basis of $\mathbb{F}_2C$ and a normalized unit $u \in V(\mathbb{F}_2C)$ can be written as

$$1 + \sum_{i=1}^{2^n-1} \alpha_i (a+1)^i.$$

Each ideal of the group algebra $\mathbb{F}_2C$ has the form $\mathbb{F}_2C(1+a)^i$. Clearly $(1+a)^i$ belongs to the augmentation ideal $A(\mathbb{F}_2C)$ and by Jennings' theorem [34]

$$A^i(\mathbb{F}_2C) = A^{i+1}(\mathbb{F}_2C) + (a+1)^i\mathbb{F}_2.$$

Note that the radical of F_2C coincides with the augmentation ideal $A(\mathbb{F}_2C)$.

Proposition 2.1.2 (E. T. Hill [31]). *Let G be a p-group and F_pG be the group ring of G over F_p. If L is the exponent of the radical A of F_pG then the annihilator of A^ω is $A^{L-\omega+1}$.*

Thus the annihilator $A^{2^n-i}(\mathbb{F}_2C)$ of the element $(1+a)^i$ coincides with $\mathbb{F}_2C(1+a)^{2^n-i}$.

Corollary 2.1.3. *The subgroup*

$$S_i = \{\ \gamma \in V(\mathbb{F}_2C)\ \mid\ \gamma(1+a)^i = (1+a)^i\ \}$$

of $V(\mathbb{F}_2C)$ has order 2^i.

Proof. It is easy to see that $1+Ann\big((1+a)^i\big)$ coincides with S_i, and according to Proposition 2.1.2 the cardinality $\big|Ann((1+a)^i)\big|$ is 2^i. □

Recall some well-known facts about a finite abelian 2-group N. Let $N[2]$ be the subgroup generated by the elements of order two. We shall use the following proposition:

Proposition 2.1.4. *Let N be a finite abelian 2-group.*

1. *If $g \in \Phi(N)$ then $H_g = \{\ h \in N\ \mid\ h^2 = g\ \}$ is a coset of N by $N[2]$.*

2. *If $g \notin \Phi(N)$ then $N = \langle\ g\ \rangle \times W$ for some subgroup W.*

2.2 Involutions and unitary subgroups

Let $C = \langle\ a \mid a^{2^n} = 1\ \rangle$ be a cyclic 2-group with $n \geq 2$. First we review some results on involutions of $\mathbb{F}_2C$. Recall that the linear extension of the automorphism $a^i \mapsto a^{-i}$ of G to the automorphism $x \mapsto x^*$ of $\mathbb{F}_2C$ is an involution of $\mathbb{F}_2C$, as we have shown in Section 1.2. Moreover, for $n \geq 3$ we have another involution $x \mapsto x^{\circledast}$, which is generated by the automorphism $a^i \mapsto a^{(2^{n-1}-1)i}$ of order two. For the sake of convenience we assume that σ is either $x \mapsto x^*$ or $x \mapsto x^{\circledast}$.

First we observe some properties of these involutions.

Lemma 2.2.1. *For* $x = \alpha_0 + \alpha_1 a + \cdots + \alpha_{2^n-1}a^{2^n-1} \in \mathbb{F}_2C$ *we have*

$$x^2 = \sum_{i=0}^{2^{n-1}-1} (\alpha_i + \alpha_{i+2^{n-1}})a^{2i}$$

and

$$xx^* = \chi(x) + \sum_{j=1}^{2^{n-1}-1} \Big[\sum_{i=0}^{2^n-1} \alpha_i\alpha_{i-j} \pmod{2^n}\Big] \cdot \Big[a^j + a^{-j}\Big].$$

Proof. Evidently $x^2 = \sum_{i=0}^{2^n-1} \alpha_i a^{2i}$ and $(a^{i+2^{n-1}})^2 = (a^i)^2$, thus the coefficient of a^{2i} is equal to $\alpha_i + \alpha_{i+2^{n-1}}$. Moreover, the equality $(xx^*)^* = xx^*$ yields

$$xx^* = \gamma_0 + \gamma_{2^{n-1}}a^{2^{n-1}} + \sum_{j=1}^{2^{n-1}-1} \gamma_j(a^j + a^{-j}).$$

For each $a^j \in \mathit{supp}\,(xx^*)$, where $0 \leq j \leq 2^{n-1} - 1$ the equality $a^j = a^i a^{-(i-j)}$ shows that $\gamma_j = \sum_{i=0}^{2^n-1} \alpha_i\alpha_{i-j} \pmod{2^n}$.

In particular, $\gamma_0 = \sum_{i=0}^{2^n-1} \alpha_i\alpha_i = \sum_{i=0}^{2^n-1} \alpha_i = \chi(x)$ and

$$\gamma_{2^{n-1}} = \sum_{i=0}^{2^n-1} \alpha_i\alpha_{i-2^{n-1}} \pmod{2^n} = 2 \cdot \sum_{i=0}^{2^{n-1}-1} \alpha_i\alpha_{i-2^{n-1}} \pmod{2^n} = 0.$$

□

We put

$$Q = \{\, 0, 2, 4, \ldots, 2^{n-2} - 2 \,\} \cup \{\, 2^{n-1}, 2^{n-1} + 2, 2^{n-1} + 4, \ldots, 2^{n-1} + 2^{n-2} - 2 \,\},$$

$$P = \{\, 0, 2, 4, \ldots, 2^{n} - 2 \,\},\ \widetilde{P} = P \setminus \{\, 0, 2^{n-1} \,\} \text{ and } R = \{\, 0, 2, 4, \ldots, 2^{n-1} - 2 \,\}.$$

Lemma 2.2.2. *For* $x = \alpha_0 + \alpha_1 a + \cdots + \alpha_{2^n-1} a^{2^n-1} \in \mathbb{F}_2 C$ *we have*

$$xx^{\circledast} = \gamma_0 + \gamma_{2^{n-1}} a^{2^{n-1}} + \sum_{k \in R \setminus \{\, 0 \,\}} \gamma_k (a^k + a^{-k}) + \sum_{k \in 1+Q} \gamma_k (a^k + a^{-k+2^{n-1}}),$$

where

$$\gamma_k = \begin{cases} \displaystyle\sum_{r \in P} \alpha_r \alpha_{r-k \pmod{2^n}} + \sum_{r \in 1+P} \alpha_r \alpha_{r-k+2^{n-1} \pmod{2^n}} & \text{for } k \in \widetilde{P}; \\ \displaystyle\sum_{r \in P} \alpha_r \alpha_{r-k+2^{n-1} \pmod{2^n}} + \sum_{r \in 1+P} \alpha_r \alpha_{r-k \pmod{2^n}} & \text{for } k \in 1 + P; \\ \displaystyle\sum_{r \in 1+P} \alpha_r & \text{for } k = 2^{n-1}; \\ \displaystyle\sum_{r \in P} \alpha_r & \text{for } k = 0. \end{cases}$$

Proof. Since $(xx^{\circledast})$ is $\circledast$-symmetric so

$$xx^{\circledast} = \gamma_0 + \gamma_{2^{n-1}} a^{2^{n-1}} + \sum_{k \in R \setminus \{\, 0 \,\}} \gamma_k (a^k + a^{-k}) + \sum_{k \in 1+Q} \gamma_k (a^k + a^{-k+2^{n-1}}).$$

We define the permutation ρ of the set $\{\, 0, 1, 2, \ldots, 2^n - 1 \,\}$ in the following way:

$$\rho(i) = \begin{cases} i \text{ if } i \text{ is even}; \\ i + 2^{n-1} \pmod{2^n} \text{ if } i \text{ is odd}. \end{cases}$$

Using the permutation ρ, straightforward computations show that $x^{\circledast} = \sum_{i=0}^{2^n-1} \alpha_{\rho(i)} a^{-i}$ and the coefficient of $a^k \in supp\,(xx^{\circledast})$ is equal to the trace $\gamma_k = tr(xx^{\circledast} a^{-k})$. Evidently

$$\gamma_k = tr\Big(\big(\sum_{j=0}^{2^n-1} \alpha_j a^j \big) \cdot \big(\sum_{i=0}^{2^n-1} \alpha_{\rho(i-k)} a^{-i} \big) \Big) = \sum_{r=0}^{2^n-1} \alpha_r \alpha_{\rho(r-k)}.$$

Therefore we have for even k

$$\gamma_k = \sum_{r=0}^{2^n-1} \alpha_r \alpha_{\rho(r-k)} = \sum_{r\in P} \alpha_r\alpha_{r-k} \pmod{2^n} + \sum_{r\in 1+P} \alpha_r\alpha_{r-k+2^{n-1}} \pmod{2^n},$$

and for odd k

$$\gamma_k = \sum_{i\in P} \alpha_i\alpha_{i-k+2^{n-1}} \pmod{2^n} + \sum_{i\in 1+P} \alpha_i\alpha_{i-k} \pmod{2^n}.$$

Specifically for $k = 2^{n-1}$ simple computations show that

$$\gamma_{2^{n-1}} = \sum_{i\in P} \alpha_i\alpha_{i-2^{n-1}} \pmod{2^n} + \sum_{i\in 1+P} \alpha_i\alpha_i = \sum_{i\in 1+P} \alpha_i,$$

and

$$\gamma_0 = \sum_{i\in P} \alpha_i\alpha_i + \sum_{i\in 1+P} \alpha_i\alpha_{i-2^{n-1}} \pmod{2^n} = \sum_{i\in P} \alpha_i.$$

□

Recall that each involution σ of $\mathbb{F}_2C$ determines a σ-unitary subgroup

$$V_\sigma(\mathbb{F}_2C) = \{\ \gamma \in V(\mathbb{F}_2C)\ \mid\ \gamma^{-1} = \gamma^\sigma\ \}$$

of $V(\mathbb{F}_2C)$.

Now we determine the order of the $\circledast$-unitary subgroup $V_\circledast(\mathbb{F}_2C)$, which, as far as we know, has not been investigated so far.

The mapping φ_σ, given by

$$\varphi_\sigma(x) = x^\sigma x^{-1} \quad \text{for} \quad x \in V(\mathbb{F}_2C),$$

is a homomorphism of the group $V(\mathbb{F}_2C)$ onto some subgroup $W_\sigma(C)$ of the σ-unitary subgroup $V_\sigma(\mathbb{F}_2C)$ with kernel

$$S_\sigma(C) = \{\ x \in V(\mathbb{F}_2C)\ \mid\ x = x^\sigma\ \}.$$

The subset D of C determines the element $\widehat{D} = \sum_{g\in D} g$ of F_2C.

Lemma 2.2.3. *The unit* $1+\widehat{C}$ *does not belong to* $W_{\circledast}(C)$ *and* $1+\widehat{C^2}$ *is not an element of the subgroup* $V^2_{\circledast}(\mathbb{F}_2C)$.

Proof. Assume that $1+\widehat{C} \in W_{\circledast}(C)$. Then $1+\widehat{C} = x^{\circledast}x^{-1}$ for some $x \in V(\mathbb{F}_2C)$ and

$$x^{\circledast} = x(1+\widehat{C}) = x + \chi(x)\widehat{C} = x + \widehat{C}. \tag{2.2}$$

Evidently the traces of the elements x and $x^{\circledast}$ are equal, so $tr(x+x^{\circledast})$ is zero and the equality (2.2) leads to a contradiction at characteristic two.

Now, suppose that $1+\widehat{C^2} = x^2$ for some $\circledast$-unitary element x of $V_{\circledast}(\mathbb{F}_2C)$. Since $x^{\circledast} = x^{-1}$ and x has the form $x = y_1 + y_2a$ with $y_i \in \mathbb{F}_2C^2$, so

$$x^{\circledast} + x = x(1+x^{-2}) = x(1+x^2) = \widehat{C^2}\Big(\chi(y_1) + \chi(y_2)a^{\circledast}\Big),$$

and $\chi(y_1) = tr(x^{\circledast}+x) = 0$. This shows that

$$y_1^{\circledast} + y_1 + y_2a + (y_2a)^{\circledast} = \widehat{C^2}a^{\circledast},$$

which implies that $y_1 = y_1^{\circledast}$ and

$$\widehat{C^2} = y_2^{\circledast} + y_2a^{2^{n-1}+2}.$$

The previous equality shows that the set $supp\ (y_2^{\circledast}) \cap supp\ (y_2a^{2^{n-1}+2})$ is empty, so $|supp\ (y_2^{\circledast})| = 2^{n-2}$, thus $\chi(y_2) = 0$, a contradiction.

□

We shall use the next homomorphism of $V(\mathbb{F}_2C)$ later. Evidently, if $\Psi_\sigma(x) = xx^\sigma$ for $x \in V(\mathbb{F}_2C)$ then Ψ_σ is a homomorphism of $V(\mathbb{F}_2C)$ with kernel $V_\sigma(\mathbb{F}_2C)$.

Theorem 2.2.4. *If* $C = \langle\ a \mid a^{2^n} = 1\ \rangle$ *with* $n \geq 3$ *then the order of* $V_{\circledast}(\mathbb{F}_2C)$ *is* $2^{\frac{|C|}{2}}$ *and*

$$V_{\circledast}(\mathbb{F}_2C) = W_{\circledast}(C) \times \langle\ 1+\widehat{C}\rangle.$$

Proof. It is easy to see that the lower layers of the groups $V_{\circledast}(\mathbb{F}_2C)$ and $S_{\circledast}(C)$ coincide. To determine the 2-rank of $V_{\circledast}(\mathbb{F}_2C)$ it suffices to find the order of the lower layer $S_{\circledast}(C)[2]$ of the group $S_{\circledast}(C)$.

Each $\circledast$-symmetric element of $V(\mathbb{F}_2C)$ has the form

$$\gamma_0 + \gamma_{2^{n-1}}a^{2^{n-1}} + \sum_{k\in R\setminus\{\,0\,\}} \gamma_k(a^k + a^{-k}) + \sum_{k\in 1+Q} \gamma_k(a^k + a^{-k+2^{n-1}}),$$

where $\gamma_i \in \mathbb{F}_2$ and $\gamma_0 + \gamma_{2^{n-1}} = 1$. Therefore $|S_{\circledast}(C)| = 2^{\frac{|C|}{2}}$, and analogously $|S_{\circledast}(C)^2| = 2^{\frac{|C^2|}{2}-1}$. Thus the order of the subgroups $S_{\circledast}(C)[2]$ and $V_{\circledast}(\mathbb{F}_2C)[2]$ is $2^{\frac{|C|}{4}+1}$. But the kernel of $\varphi_{\circledast}$ is $S_{\circledast}(C)$, so

$$|W_{\circledast}(C)| = |V(\mathbb{F}_2C)| : |S_{\circledast}(C)| = 2^{\frac{|C|}{2}-1}.$$

Now we are ready to prove by induction on the order of C that $|V_{\circledast}(\mathbb{F}_2C)| = 2^{\frac{|C|}{2}}$. First let $|C| = 2^3$. According to Lemma 2.2.2, for the unit $x = \sum_{i=0}^{7} \alpha_i a^i$ we have

$$xx^{\circledast} = \beta_0 + \beta_1(a + a^3 + a^5 + a^7) + \beta_2(a^2 + a^6) + (\beta_0 + 1)a^4,$$

because $\chi(x) = 1$.

Since $\psi_{\circledast}(x) = xx^{\circledast}$ and the order of $Im(\psi_{\circledast})$ is 2^3, so the order of $V_{\circledast}(\mathbb{F}_2C)$ is

$$|V(\mathbb{F}_2C)| : |Im(\psi_{\circledast})| = 2^4.$$

Evidently $1 + \widehat{C} \in V_{\circledast}(\mathbb{F}_2C)$ and $1 + \widehat{C} \notin W_{\circledast}(C)$ by Lemma 2.2.3. Since the subgroup $\langle\, 1 + \widehat{C}\rangle \times W_{\circledast}(C)$ of $V_{\circledast}(\mathbb{F}_2C)$ has order 2^4, we have

$$V_{\circledast}(\mathbb{F}_2C) = \langle\, 1 + \widehat{C}\rangle \times W_{\circledast}(C).$$

Now let $|C| > 2^3$. Applying the inductive hypothesis for C^2,

$$V_{\circledast}(\mathbb{F}_2C^2) = W(C^2) \times \langle\, 1 + \widehat{C^2}\rangle.$$

Lemma 2.2.3 asserts that $\langle\, 1 + \widehat{C}\rangle \times W_{\circledast}(C)$ is a subgroup of $V_{\circledast}(\mathbb{F}_2C)$ and $\langle\, 1 + \widehat{C^2}\rangle \times V^2_{\circledast}(\mathbb{F}_2C)$ is a subgroup of $V_{\circledast}(\mathbb{F}_2C^2)$. This shows that

$$\big|V^2_{\circledast}(\mathbb{F}_2C)\big| \le \big|V_{\circledast}(\mathbb{F}_2C^2)\big| : \big|\langle\, 1 + \widehat{C^2}\rangle\big| = \big|W(C^2)\big|,$$

so

$$\left|V_{\circledast}(\mathbb{F}_2C)\right| = \left|V^2_{\circledast}(\mathbb{F}_2C)\right|\cdot\left|V_{\circledast}(\mathbb{F}_2C)[2]\right| \leq \left|W(C^2)\right|\cdot\left|V_{\circledast}(\mathbb{F}_2C)[2]\right| = 2^{\frac{|C|}{2}}.$$

But $\langle\, 1+\widehat{C}\rangle \times W_{\circledast}(C)$ is a subgroup of $V_{\circledast}(\mathbb{F}_2C)$ and its order is $2^{\frac{|C|}{2}}$, therefore the order of $V_{\circledast}(\mathbb{F}_2C) = \langle\, 1+\widehat{C}\rangle \times W_{\circledast}(C)$ is $2^{\frac{|C|}{2}}$.

□

Corollary 2.2.5. *If* $C = \langle\, a \mid a^{2^n} = 1 \,\rangle$ *with* $n \geq 3$ *then*

$$\left|V_{\circledast}(F_2C)\right| = \frac{\left|V_*(F_2C)\right|}{2}.$$

2.3 Units of type 1 and 2

As we have shown in Section 1.2 the generalized quaternion group, the dihedral group and the semidihedral group are extensions of the cyclic group C. In the following G is one of these extensions. In $V(\mathbb{F}_2G)$ we divide the units of order two into two classes. It is well known that $x = x_1 + x_2b$ is a unit if and only if $\chi(x_1) + \chi(x_2) = 1$.

Definition 2.3.1. *Let* $x = x_1 + x_2b$ *be a unit. If* x *has order two,* $\chi(x_1) = 1$ *and* $\chi(x_2) = 0$ *then* x *is called a unit of type* 1. *If* x *has order two,* $\chi(x_1) = 0$ *and* $\chi(x_2) = 1$ *then* x *is called a unit of type* 2.

For a fixed non-invertible element $z \in \mathbb{F}_2C$ the set

$$M^\sigma_z = \left\{\, y \in V(\mathbb{F}_2C) \;\middle|\; (y + y^\sigma)z = 0 \,\right\}$$

is a subgroup of $V(\mathbb{F}_2C)$. Indeed, if $y_1, y_2 \in M^\sigma_z$ then $y_1z = y_1^\sigma z$ and $y_2z = y_2^\sigma z$. Hence $y_1y_2z = y_1y_2^\sigma z = y_1^\sigma y_2^\sigma z = (y_1y_2)^\sigma z$, so $y_1y_2 \in M^\sigma_z$.

Lemma 2.3.2. *The number of units of type* 1 *is equal in the two groups* $V(F_2D_{2^{n+1}})$ *and* $V(F_2Q_{2^{n+1}})$.

Proof. A unit $x_1 + x_2 b_2 \in V(\mathbb{F}_2 D_{2^{n+1}})$ has order two if and only if

$$\begin{cases} x_1^2 = x_2 x_2^* + 1; \\ (x_1 + x_1^*)x_2 = 0. \end{cases} \tag{2.3}$$

Similarly, $x_1 + x_2 b_1 \in V(\mathbb{F}_2 Q_{2^{n+1}})$ is a unit of order two if and only if

$$\begin{cases} x_1^2 = x_2 x_2^* a^{2^{n-1}} + 1; \\ (x_1 + x_1^*)x_2 = 0. \end{cases}$$

Let $x_2 \in \mathbb{F}_2 C$ be a fixed non-invertible element. Clearly $x_2 x_2^* + 1$, $x_2 x_2^* a^{2^{n-1}} + 1$ belong to the subgroup M_{x_2} defined before, and the set

$$H_{x_2 x_2^* + 1} = \{\ h \in M_{x_2}^* \ \mid\ h^2 = x_2 x_2^* + 1\ \}$$

is either empty or according to Proposition 2.1.4 it constitutes a coset of $M_{x_2}^*$ by $M_{x_2}^*[2]$. Similarly,

$$H_{x_2 x_2^* a^{2^{n-1}} + 1} = \{\ h \in M_{x_2}^* \ \mid\ h^2 = x_2 x_2^* a^{2^{n-1}} + 1\ \}$$

is either a coset of $M_{x_2}^*$ by $M_{x_2}^*[2]$ or an empty set.

Let us prove that $x_2 x_2^* + 1 \in \Phi(M_{x_2}^*)$ if and only if $x_2 x_2^* a^{2^{n-1}} + 1$ is contained in $\Phi(M_{x_2}^*)$.
Suppose that $u = x_2 x_2^* + 1 \notin \Phi(M_{x_2}^*)$ and $v = x_2 x_2^* a^{2^{n-1}} + 1 \in \Phi(M_{x_2}^*)$. Then for $u \notin \Phi(M_{x_2}^*)$ there exists a direct decomposition

$$M_{x_2}^* = \langle\, u \rangle \times W$$

for some subgroup W. Of course

$$v^2 = (x_2 x_2^* a^{2^{n-1}} + 1)^2 = (x_2 x_2^*)^2 + 1 = u^2,$$

therefore $u^{-1} v \in M_{x_2}^*[2]$ and $v = uy$ for some $y \in M_{x_2}^*[2]$. Obviously, $v \in \Phi(M_{x_2}^*) = \langle\, u^2 \rangle \times W^2$, whence $v = u^{2t} w^2$ for some t and $w \in W$. Moreover, $v = uy$ implies that

$$y = u^{2t-1} w^2 \in M_{x_2}^*[2] \quad \text{and} \quad 1 = y^2 = u^{4t-2} w^4.$$

This shows that $u^{4t-2} = 1$, so $4t \equiv 2 \pmod{|u|}$, where $|u|$ is the order of u. Hence $|u| = 2$ and $(x_2x_2^*)^2 = 0$. According to Lemma 2.2.1, $x_2x_2^* = z(1 + a^{2^{n-1}})$ for some $z \in \mathbb{F}_2C$ and

$$\begin{aligned} v &= x_2x_2^*a^{2^{n-1}} + 1 = z(1 + a^{2^{n-1}})a^{2^{n-1}} + 1 \\ &= z(1 + a^{2^{n-1}}) + 1 = x_2x_2^* + 1 = u \end{aligned}$$

which is impossible.

We have shown that the cardinalities of the subsets $H_{x_2x_2^*+1}$ and $H_{x_2x_2^*a^{2^{n-1}}+1}$ are equal for each non-invertible element x_2, thus the proof of the lemma is complete.

□

2.4 Elements of order two in $V(\mathbb{F}_2G)$

A unit $x_1 + x_2b_3 \in V(\mathbb{F}_2SD_{2^{n+1}})$ has order two if and only if

$$\begin{cases} x_1^2 = x_2x_2^{\circledast} + 1; \\ (x_1 + x_1^{\circledast})x_2 = 0. \end{cases} \tag{2.4}$$

For each non-invertible and nonzero element x_2 there exists an i such that $x_2 = \gamma(1 + a)^i$ for some $\gamma \in V(\mathbb{F}_2C)$. The equalities (2.3) and (2.4) yield

$$x_2x_2^* = \gamma\gamma^*(1 + a)^{2i}a^{-i} \in \mathbb{F}_2C^2,$$

and

$$x_2x_2^{\circledast} = \gamma\gamma^{\circledast}(1 + a)^i(1 + a^{2^{n-1}-1})^i \in \mathbb{F}_2C^2.$$

In particular, if $i = 2l$ is even then

$$(1 + a)^{2l}(1 + a^{2^{n-1}-1})^{2l} = (1 + a^2)^l(1 + a^{-2})^l = (1 + a)^{2l}(1 + a^{-1})^{2l},$$

and $x_2x_2^{\circledast} = \gamma\gamma^{\circledast}(1 + a)^{2i}a^{-i}$.

For each $0 \leq i < 2^n$ we define the set

$$H_i^{\sigma} = \{\ h \in V(\mathbb{F}_2C)\ \mid\ hh^{\sigma}(1 + a)^i(1 + a^{\sigma})^i \in \mathbb{F}_2C^2\ \}.$$

Lemma 2.4.1. *The set H_i^σ has the following properties:*

1. *If $i \geq 2^{n-1}$ then $H_i^\sigma = V(\mathbb{F}_2C)$.*
2. *If $i = 2l+1$ is odd and $i < 2^{n-1}$ then the set H_i^σ is empty.*
3. *If $i = 2l$ is even and $i < 2^{n-1}$ then H_{2l}^σ is a subgroup of $V(\mathbb{F}_2C)$.*
4. *For even indices $i = 2l < 2^{n-1}$*

$$H_0^\sigma \subset H_2^\sigma \subset H_4^\sigma \subset \cdots \subset H_{2l}^\sigma \subset \cdots \subset H_{2^{n-1}-2}^\sigma = V(\mathbb{F}_2C)$$

and the order of the subgroup H_{2l}^σ is $2^{3\cdot 2^{n-2}+l}$.

Proof. 1. Since $(1+a)^{2^{n-1}} = (1+a^\sigma)^{2^{n-1}}$, for $i \geq 2^{n-1}$ we have

$$hh^\sigma(1+a)^i(1+a^\sigma)^i = hh^\sigma(1+a)^{2^n}(1+a)^{i-2^{n-1}}(1+a^\sigma)^{i-2^{n-1}} = 0.$$

Thus $hh^\sigma(1+a)^i(1+a^\sigma)^i \in \mathbb{F}_2C^2$ for each $h \in V(\mathbb{F}_2C)$. Therefore $H_i^\sigma = V(\mathbb{F}_2C)$ for all $i \geq 2^{n-1}$.

2. Let $i = 2l+1$ be a fixed odd integer and $i < 2^{n-1}$.
First, let us prove by induction on l that if $i = 2l+1$ then

$$(a+a^{-1})^i = \sum_{\text{r is odd}} \beta_r(a^r + a^{-r}), \tag{2.5}$$

where $\beta_r \in \mathbb{F}_2$. This is clear for $l = 0$ and assume that

$$(a+a^{-1})^{2l+1} = \sum_{\text{r is odd}} \beta_r(a^r + a^{-r}).$$

By the identity

$$(a^s + a^{-s})(a^k + a^{-k}) = (a^{s+k} + a^{-(s+k)}) + (a^{s-k} + a^{-(s-k)}) \tag{2.6}$$

we have

$$(a+a^{-1})^{2(l+1)+1} = \sum_{\text{r is odd}} \beta_r\big((a^{r+2} + a^{-r-2}) + (a^{r-2} + a^{-r+2})\big),$$

the desired assertion.

Now, we are going to prove that the set H_i^σ is empty. First let σ be the $*$-involution. By Lemma 2.2.1, for $h \in H_i^*$ we have $hh^* = 1+z_1+z_2$, where

$$z_1 = \sum_{j \in R \setminus \{ 0 \}} \alpha_j (a^j + a^{-j}), \quad z_2 = \sum_{k \in 1+R} \alpha_k (a^k + a^{-k}),$$

and $R = \{ 0, 2, 4, \ldots, 2^{n-1} - 2 \}$. By definition,

$$hh^*(a + a^{-1})^i = (1 + z_1)(a + a^{-1})^i + z_2(a + a^{-1})^i \in \mathbb{F}_2 C^2 \tag{2.7}$$

and since $i = 2l + 1$ is odd it is easy to see that

$$(a^k + a^{-k})(a + a^{-1})^i = (a^k + a^{-k})(a + a^{-1})(a^2 + a^{-2})^l,$$

so by (2.5) and (2.6) we have $z_2(a + a^{-1})^i \in \mathbb{F}_2 C^2$ and

$$w = (1 + z_1)(a + a^{-1})^i \notin \mathbb{F}_2 C^2$$

if $w \neq 0$. But by (2.7) $(1+z_1)(a+a^{-1})^i = 0$ and we have $(a+a^{-1})^i = 0$, because $1 + z_1$ is a unit. This is impossible for $i < 2^{n-1}$.

Let σ be the $\circledast$-involution. Lemma 2.2.2 asserts that $hh^\circledast = 1 + z_1 + z_2$, where

$$z_1 = (\gamma_0 + 1)(1 + a^{2^{n-1}}) + \sum_{k \in R \setminus \{ 0 \}} \gamma_k (a^k + a^{-k}),$$

$$z_2 = \sum_{k \in 1+Q} \gamma_k (a^k + a^{-k+2^{n-1}})$$

and

$$Q = \{ 0, 2, 4, \ldots, 2^{n-2} - 2 \} \cup \{ 2^{n-1}, 2^{n-1} + 2, 2^{n-1} + 4, \ldots 2^{n-1} + 2^{n-2} - 2 \}.$$

We remark that

$$hh^\circledast (1 + a)^{2l+1} (1 + a^{2^{n-1}-1})^{2l+1}$$

$$= (1+z_1+z_2)(a+a^{-1})^{2l}\Big((1+a)^{2^{n-1}}+(a+a^{-1})+(1+a)^{2^{n-1}}a^{-1}\Big) \in \mathbb{F}_2C^2.$$

The identity

$$(a^k + a^{-k+2^{n-1}})(a^r + a^{-r}) = (a^{k+r} + a^{-r-k+2^{n-1}}) + (a^{k-r} + a^{-k+r+2^{n-1}})$$

and (2.6) assert that

$$(1+z_1)(a+a^{-1})^{2l}(1+a)^{2^{n-1}} + z_2(a+a^{-1})^{2l}(a+a^{-1}) + z_2(a+a^{-1})^{2l}(1+a)^{2^{n-1}}a^{-1}$$

belongs to $\mathbb{F}_2C^2$, and

$$\begin{aligned} w =&(1 + z_1)(a + a^{-1})^{2l+1} + (a + a^{-1})^{2l}(1 + a)^{2^{n-1}} z_2 \\ &+ (a + a^{-1})^{2l}(1 + a)^{2^{n-1}}(1 + z_1)a^{-1} \end{aligned}$$

is not an element of $\mathbb{F}_2C^2$, if $w \neq 0$. By (2.7), $w \in \mathbb{F}_2C^2$, and this leads again to a contradiction. Therefore

$$(1 + z_1)(a + a^{-1})^{2l+1} + (a + a^{-1})^{2l}(1 + a)^{2^{n-1}}\Big(z_2 + (1 + z_1)a^{-1}\Big) = 0.$$

Since $1 + z_1$ and $e = z_2(1 + z_1)^{-1} + a^{-1}$ are units, it follows that

$$(a + a^{-1})^{2l}\Big((a + a^{-1}) + (1 + a)^{2^{n-1}}e\Big) = 0. \tag{2.8}$$

For $l = 0$ we have $(a + a^{-1}) = (1 + a)^{2^{n-1}}e$, which is impossible, because $(a + a^{-1})^2 \neq 0$. If $l > 0$ then

$$(a + a^{-1})^{2l}(1 + a)^{2^{n-1}}e \in A^{4l+2^{n-1}}(\mathbb{F}_2C).$$

Thus from (2.8) it follows that $(a + a^{-1})^i \in A^{4l+2^{n-1}}(\mathbb{F}_2C)$ and $i < 4l + 2^{n-1}$. This is impossible by Jennings' theory [34]. Thus H_i^σ is empty, as we stated.

3. Now we shall prove that for $i = 2l < 2^{n-1}$ the set H_i^σ is a subgroup of $V(\mathbb{F}_2C)$. Using the basis (2.1), for $h \in H_i^\sigma$ we have

$$hh^\sigma = 1 + \sum_{j=1}^{2^n-1} \alpha_j(1 + a)^j,$$

and

$$hh^{\sigma}(1+a)^{2i} = (1+a)^{2i} + \sum_{j=1}^{2^n-2i-1} \alpha_j (1+a)^{j+2i} \in \mathbb{F}_2 C^2.$$

But it follows that $\alpha_1 = \alpha_3 = \alpha_5 = \cdots = \alpha_{2^n-2i-1} = 0$. Consequently, for $h_1, h_2 \in H_i^{\sigma}$ there exist $u_1, u_2 \in \mathbb{F}_2 C^2$ and $v_1, v_2 \in A^{2^n-2i}(\mathbb{F}_2 C)$ such that

$$h_1 h_1^{\sigma} = 1 + u_1 + v_1 \quad \text{and} \quad h_2 h_2^{\sigma} = 1 + u_2 + v_2.$$

Clearly

$$h_1 h_2 (h_1 h_2)^{\sigma} = h_1 h_1^{\sigma} h_2 h_2^{\sigma} = 1 + u_1 + u_2 + u_1 u_2 + z,$$

where $1 + u_1 + u_2 + u_1 u_2 \in \mathbb{F}_2 C^2$ and

$$z = v_1 + v_1 u_2 + v_2 + u_1 v_2 + v_1 v_2 \in A^{2^n-2i}(\mathbb{F}_2 C).$$

Hence $h_1 h_2 \in H_i^{\sigma}$ and H_i^{σ} is a subgroup of $V(\mathbb{F}_2 C)$.

In the next step we shall verify that $H_{2^{n-1}-2}^{\sigma} = V(\mathbb{F}_2 C)$. A unit u of $\mathbb{F}_2 C$ can be written as

$$u \equiv 1 + \alpha_1(1+a) + \alpha_2(1+a)^2 + \alpha_3(1+a)^3 \pmod{A^4(\mathbb{F}_2 C)}.$$

It is easy to see that

$$\begin{aligned}(1+a^{\sigma}) \equiv (1+a) + (1+a)^2 \\ + (1+a)^3 + \cdots + (1+a)^{2^{n-1}-1} \pmod{A^{2^{n-1}}(\mathbb{F}_2 C)}.\end{aligned} \tag{2.9}$$

It follows that

$$u^{\sigma} \equiv 1 + \alpha_1(1+a) + (\alpha_1+\alpha_2)(1+a)^2 + (\alpha_1+\alpha_3)(1+a)^3 \pmod{A^4(\mathbb{F}_2 C)}$$

and

$$uu^{\sigma} \equiv 1 \pmod{A^4(\mathbb{F}_2 C)}. \tag{2.10}$$

Therefore for each $h \in V(\mathbb{F}_2C)$ and $i = 2^{n-1} - 2$, (2.10) says that

$$hh^\sigma(1+a)^{2i} = hh^\sigma(1+a)^{(2^n-4)} = (1+a)^{(2^n-4)}.$$

This shows that $h \in H^\sigma_{2^{n-1}-2}$ and $H^\sigma_{2^{n-1}-2} = V(\mathbb{F}_2C)$, because h is an arbitrary unit. This completes the proof of this assertion.

4. Now let $i = 2l < 2^{n-1} - 2$. We shall prove that H^σ_i is a proper subgroup of H^σ_{i+2}. Clearly $H^\sigma_i \subseteq H^\sigma_{i+2}$ and it is sufficient to verify that $h = 1 + (1+a)^{2^n-(2i+3)}$ does not belong to H^σ_i and $h \in H^\sigma_{i+2}$.
Note that for an even i the binomial coefficient $\binom{2^n-2i-3}{2}$ is even too and $h^\sigma = 1 + (1+a^\sigma)^{2^n-(2i+3)}$. By the binomial formula and (2.9) we have

$$h^\sigma = 1 + (1+a)^{2^n-(2i+3)} + (1+a)^{2^n-(2i+2)} + (1+a)^{2^n-(2i+1)} + x_\sigma,$$

where $x_\sigma \in A^{2^n-2i}(\mathbb{F}_2C)$. It is easy to see that $2^{n+1} - 4i - j \geq 2^n - 2i$ for $i \leq 2^{n-1} - 4$ and $j = 4, 5, 6$. This shows that hh^σ can be written as

$$hh^\sigma = 1 + (1+a)^{2^n-(2i+2)} + (1+a)^{2^n-(2i+1)} + y_\sigma$$

for some $y_\sigma \in A^{2^n-2i}(\mathbb{F}_2C)$. Thus

$$hh^\sigma(1+a)^{2i} = (1+a)^{2i} + (1+a)^{2^n-2} + (1+a)^{2^n-1}$$

and we have $h \notin H^\sigma_i$. But the equality $hh^\sigma(1+a)^{2i+2} = (1+a)^{2i+2}$ states that $h \in H^\sigma_{i+2}$ and this proves that

$$H^\sigma_0 \subset H^\sigma_2 \subset H^\sigma_4 \subset \cdots \subset H^\sigma_i \subset \cdots \subset H^\sigma_{2^{n-1}-2} = V(\mathbb{F}_2C).$$

Now we shall determine the order of the group H^σ_0. The σ-unitary subgroup $V_\sigma(\mathbb{F}_2C)$ of $V(\mathbb{F}_2C)$ is a subgroup of H^σ_0 and we shall use the subgroup

$$J^\sigma = \left\{ zz^\sigma \;\middle|\; z \in V(\mathbb{F}_2C),\ zz^\sigma \in \mathbb{F}_2C^2 \right\}.$$

With respect to σ we shall distinguish two cases. First let σ be the $*$-involution. We shall prove that $J^* = S_*(C)^2$ and its order is $2^{2^{n-2}-1}$.

Indeed, if $u \in J^*$ then $u = zz^* \in \mathbb{F}_2C^2$ for some $z \in V(\mathbb{F}_2C)$ and by Lemma 2.2.1,

$$u = zz^* = 1 + \sum_{j=1}^{2^{n-2}-1} \alpha_j(a^{2j} + a^{-2j}).$$

Now the $*$-symmetric element $y = 1 + \sum_{j=1}^{2^{n-2}-1} \alpha_j(a^j + a^{-j})$ is such that $y^2 = u$. This shows that J^* is a subgroup of $S_*(C)^2$. Conversely, if $u \in S_*(C)^2$ then $u = u^*$ and there exists $y \in S_*(C)$ with $y^2 = u$. Then $yy^* = y^2 = u$ and $u \in J^*$, so $J^* = S_*(C)^2$. The equality of these groups shows that each $y \in S_*(C)$ satisfies

$$y^2 = yy^* = 1 + \sum_{j=1}^{2^{n-2}-1} \alpha_j(a^{2j} + a^{-2j}) \in S_*(C)^2,$$

hence the order of $S_*(C)^2$ is $2^{2^{n-2}-1}$.

The map $\psi_* : V(\mathbb{F}_2C) \to S_*(C)$ induces the epimorphism $\psi_* : H_0^* \to J^*$, and its kernel is the $*$-unitary subgroup $V_*(\mathbb{F}_2C)$ and according to Proposition 2.1.1 $V_*(\mathbb{F}_2C)$ has order $2^{2^{n-1}+1}$. Thus

$$\left|H_0^*\right| = \left|V_*(\mathbb{F}_2C)\right| \cdot \left|J^*\right| = \left|V_*(\mathbb{F}_2C)\right| \cdot \left|S_*(C)^2\right| = 2^{3 \cdot 2^{n-2}}.$$

Now, let σ be the $\circledast$-involution. We shall show that

$$J^{\circledast} = \langle\, a^{2^{n-1}} \rangle \times S_{\circledast}(C)^2 \quad \text{and} \quad \left|S_{\circledast}(C)^2\right| = 2^{\frac{|C|}{4}-1}.$$

For each $y \in S_{\circledast}(C)$ we have

$$y^2 = yy^{\circledast} = 1 + \sum_{j=1}^{2^{n-2}-1} \beta_j(a^{2j} + a^{-2j}) \in S_{\circledast}(C)^2,$$

and Lemma 2.2.2 says that $a^{2^{n-1}} \notin S_{\circledast}(C)^2$ and $|S_{\circledast}(C)^2| = 2^{\frac{|C|}{4}-1} = 2^{2^{n-2}-1}$.

Let $u \in J^{\circledast}$. Then $u = zz^{\circledast} \in \mathbb{F}_2C^2$ for some $z \in V(\mathbb{F}_2C)$ and again by Lemma 2.2.2 we obtain that

$$\begin{aligned} u = zz^{\circledast} =& \delta_1(1 + a^{2^{n-1}}) \\ &+ a^{2^{n-1}}\Big(1 + \sum_{i=1}^{2^{n-2}-1} \delta_j\big(a^{2j+2^{n-1}} + a^{-(2j+2^{n-1})}\big)\Big), \qquad \delta_i \in \mathbb{F}_2. \end{aligned}$$

If $\delta_1 = 0$ then we consider the $\circledast$-symmetric element

$$\begin{aligned} y_1 = 1 + & \sum_{j \in \{\ 1,3,\ldots,2^{n-2}-1\ \}} \delta_j\big(a^{j+2^{n-2}} + a^{-(j+2^{n-2}+2^{n-1})}\big) \\ & + \sum_{j \in \{\ 2,4,\ldots,2^{n-2}-2\ \}} \delta_j\big(a^{j+2^{n-2}} + a^{-(j+2^{n-2})}\big) \in S_{\circledast}(C), \end{aligned}$$

which has the property

$$y_1^2 = 1 + \sum_{j=1}^{2^{n-2}-1} \delta_j\Big(a^{2j+2^{n-1}} + a^{-(2j+2^{n-1})}\Big) \in S_{\circledast}(C)^2.$$

Therefore $u = a^{2^{n-1}}y_1^2 \in \langle\, a^{2^{n-1}} \rangle \times S_{\circledast}(C)^2$.
Now assume that $\delta_1 = 1$. Then the $\circledast$-symmetric element

$$\begin{aligned} y_2 = 1 + & \sum_{j \in \{\ 1,3,\cdots,2^{n-1}-1\ \}} \delta_j(a^j + a^{-j+2^{n-1}}) \\ & + \sum_{j \in \{\ 2,4,\cdots,2^{n-1}-2\ \}} \delta_j(a^j + a^{-j}) \end{aligned}$$

is such that $u = y_2^2$ and $u \in J^{\circledast} \subseteq \langle\, a^{2^{n-1}} \rangle \times S_{\circledast}(C)^2$. Conversely, if $u \in \langle\, a^{2^{n-1}} \rangle \times S_{\circledast}(C)^2$ then $u = (a^{2^{n-1}})^t d$ for some $d \in S_{\circledast}(C)^2$. Choose $w \in S_{\circledast}(C)$ with $w^2 = d$. Then

$$\begin{aligned} u = (a^{2^{n-1}})^t d =& a^t a^{t(2^{n-1}-1)} w^2 \\ =& a^t w a^{t(2^{n-1}-1)} w = a^t w \cdot (a^t w)^{\circledast} \in J^{\circledast}. \end{aligned}$$

Consequently, $J^{\circledast} = \langle\, a^{2^{n-1}} \rangle \times S_{\circledast}(C)^2$.

Again, $\psi_\circledast : V(\mathbb{F}_2C) \to S_\circledast(C)$ induces the epimorphism $\psi_\circledast : H_0^\circledast \to J^\circledast$ and its kernel is the $\circledast$-unitary subgroup $V_\circledast(\mathbb{F}_2C)$. Using the Corollary 2.2.5 this shows that

$$\left|H_0^\circledast\right| = \left|V_\circledast(\mathbb{F}_2C)\right| \cdot \left|J^\circledast\right| = \left|V_\circledast(\mathbb{F}_2C)\right| \cdot \left|\langle\, a^{2^{n-1}}\rangle \times S_\circledast(C)^2\right| = 2^{3\cdot 2^{n-2}}.$$

We have established

$$H_0^\sigma \subset H_2^\sigma \subset H_4^\sigma \subset \cdots \subset H_{2^{n-1}-2}^\sigma = V(\mathbb{F}_2C),$$

and $|H_0^\sigma| = 2^{3\cdot 2^{n-2}}$ from which it follows that $[V(\mathbb{F}_2C) : H_0^\sigma] = 2^{2^{n-2}-1}$ and by the second part of this lemma, the number of different subgroups H_{2l}^σ is $2^{n-2}-1$. This is possible if and only if $[H_{2l+2}^\sigma : H_{2l}^\sigma] = 2$ and we get that the order of H_{2l}^σ is $2^{3\cdot 2^{n-2}+l}$ for every $2l < 2^{n-1}$.

□

For $0 \le i < 2^n$ the set

$$L_i^\sigma = \left\{\, h \in V(\mathbb{F}_2C)[2] \;\middle|\; (h+h^\sigma)(1+a)^i = 0 \,\right\}$$

is a subgroup of

(2.11)

$$V(\mathbb{F}_2C)[2] = \left\{ \Big(\sum_{j=0}^{2^{n-1}-1} \alpha_j a^j \Big)(1+a)^{2^{n-1}} \in V(\mathbb{F}_2C) \;\middle|\; \alpha_j \in \mathbb{F}_2 \right\}.$$

Indeed, each $h_k \in L_i^\sigma$ is such that $h_k(1+a)^i = h_k^\sigma(1+a)^i$, so

$$h_1h_2(1+a)^i = h_1h_2^\sigma(1+a)^i = h_1^\sigma h_2^\sigma(1+a)^i = (h_1h_2)^\sigma(1+a)^i,$$

and L_i^σ is a subgroup. Moreover, easy calculations show that $h^\circledast = h^*$ for each $h \in V(\mathbb{F}_2C)[2]$. Therefore,

$$L_i^\circledast = L_i^*. \tag{2.12}$$

Consequently it is sufficient to investigate the properties of L_i^*.

Lemma 2.4.2. *The subgroup L_i^* has the following properties:*

1. $L_i^* = V(\mathbb{F}_2C)[2]$ *for* $i \geq 2^{n-1}$.
2. *For even indices* $i = 2l < 2^{n-1}$ *the subgroups* L_{2l}^* *satisfy*

$$L_0^* \subset L_2^* \subset L_4^* \subset \cdots \subset L_{2l}^* \subset \cdots \subset L_{2^{n-1}-2}^* = V(\mathbb{F}_2C)[2],$$

   and the order of L_{2l}^* *is* $2^{2^{n-2}+1+l}$.
3. *For odd index* $i = 2l+1 < 2^{n-1}$ *the subgroup* L_{2l}^* *coincides with* L_{2l+1}^*.

Proof. First let $i \geq 2^{n-1} - 2$. By (2.11) each $h \in V(\mathbb{F}_2C)[2]$ can be represented in the form

$$h = 1 + \alpha_{2^{n-1}}(1+a)^{2^{n-1}} + \alpha_{2^{n-1}+1}(1+a)^{2^{n-1}+1} + u$$

for some $u \in A^{2^{n-1}+2}(\mathbb{F}_2C)$. Formula (2.9) asserts

$$h^* = 1 + \alpha_{2^{n-1}}(1+a)^{2^{n-1}} + \alpha_{2^{n-1}+1}(1+a)^{2^{n-1}+1} + v$$

for some $v \in A^{2^{n-1}+2}(\mathbb{F}_2C)$ and $h + h^* = u + v \in A^{2^{n-1}+2}(\mathbb{F}_2C)$. But $A^{2^{n-1}+2}(\mathbb{F}_2C) \subseteq Ann\big((1+a)^i\big)$ for all $i \geq 2^{n-1} - 2$, and we conclude that $(h + h^*)(1+a)^i = 0$. Therefore $L_i^* = V(\mathbb{F}_2C)[2]$ for all $i \geq 2^{n-1}$ or $i = 2^{n-1} - 2$.

Each $*$-symmetric unit $h \in L_0^*$ can be written as

$$h = 1 + \Big(\alpha_0 + \alpha_{2^{n-2}}a^{2^{n-2}} + \sum_{j=1}^{2^{n-2}-1} \alpha_j(a^j + a^{-j+2^{n-1}})\Big)(1+a)^{2^{n-1}},$$

where $\alpha_j \in \mathbb{F}_2$. This shows that h has $2^{n-2}+1$ independent coefficients, thus the order of L_0^* is $2^{2^{n-2}+1}$.

Now we verify that L_{2l}^* is a proper subgroup of $L_{2(l+1)}^*$ for all indices $2l < 2^{n-1} - 2$. According to (2.9), for $u = 1 + (1+a)^{2^n-(2l+3)}$ we have

$$u^* = 1 + (1+a)^{2^n-(2l+3)} + (1+a)^{2^n-(2l+2)} + z,$$

where $z \in A^{2^n-(2l+1)}(\mathbb{F}_2C)$. This shows that

$$u + u^* = (1+a)^{2^n-(2l+2)} + z,$$

so

$$(u+u^*)(1+a)^{2l} = (1+a)^{2^n-2} + (1+a)^{2l}z \neq 0,$$

and $u \notin L_{2l}$. But $(u+u^*)(1+a)^{2l+2} = (1+a)^{2^n} = 0$, and this means that $u \in L^*_{2l+2}$ and L^*_{2l} is a proper subgroup of L^*_{2l+2}.

Clearly $|V(\mathbb{F}_2C)[2]| = 2^{2^{n-1}}$ and $[V(\mathbb{F}_2C)[2] : L^*_0] = 2^{2^{n-2}-1}$. As we saw above the number of different subgroups L^*_{2l} is $2^{n-2}-1$. The only possibility is that $[L^*_{2l+2} : L^*_{2l}] = 2$ and L^*_{2l} has order $2^{2^{n-2}+1+l}$ for all $2l < 2^{n-1}$.

Finally, we use again the element $u = 1+(1+a)^{2^n-(2l+3)}$. We note that

$$(u+u^*)(1+a)^{2l+1} = (1+a)^{2^n-1} \neq 0,$$

so $u \notin L^*_{2l+1}$ but $u \in L^*_{2l+2}$. It is easy to see that $L^*_{2l} \subseteq L^*_{2l+1} \subset L^*_{2l+2}$ and $[L^*_{2l+2} : L^*_{2l}] = 2$, so L^*_{2l} coincides with L^*_{2l+1}.

□

It is now possible for us to prove the main theorem of this chapter.

Theorem 2.4.3. *Let G be a 2-group of maximal class and let $\Theta_G(2)$ be the number of elements of order two in $V(\mathbb{F}_2G)$. Then*

$$\begin{aligned}\Theta_{D_{2^{n+1}}}(2) &= 2^{2^n+n-1} + 2^{2^n};\\ \Theta_{SD_{2^{n+1}}}(2) &= 2^{2^n+n-1};\\ \Theta_{Q_{2^{n+1}}}(2) &= 2^{2^n+n-1} - 2^{2^n}.\end{aligned}$$

Proof. We divide the proof into three parts. We begin with the dihedral group. Let us determine the number of the units $x_1 + x_2b_2$ of type 1 in $V(\mathbb{F}_2D_{2^{n+1}})$, where $x_2 = 0$ or $x_2 = \gamma(1+a)^i$, γ is a unit and $i > 0$.

If $x_2 = 0$ then by (2.3) we have $x_1^2 = 1$. Therefore the number of units of type 1 with $x_2 = 0$ coincides with the order of $V(\mathbb{F}_2C)[2]$.

Now let $0 < i < 2^{n-1}$ and $x_2 = \gamma(1+a)^i$. Then

$$x_1^2 = \gamma\gamma^*(a+a^{-1})^i + 1; \tag{2.13}$$

$$(x_1 + x_1^*)(1+a)^i = 0. \tag{2.14}$$

By (2.13) the element $\gamma\gamma^*(a+a^{-1})^i$ belongs to $\mathbb{F}_2C^2$, further according to Lemma 2.4.1 the number $i = 2l$ is even and

$$H_{2l}^* = \left\{ \gamma \in V(\mathbb{F}_2C) \;\middle|\; \gamma\gamma^*(a+a^{-1})^{2l} \in \mathbb{F}_2C^2 \right\}$$

is a subgroup of $V(\mathbb{F}_2C)$.

For fixed γ and i we determine the number of units $x_1+x_2b_2$ of type 1, which satisfy the conditions (2.13) and (2.14). If the unit $x_1' + x_2b$ is also of type 1 then $x_1'x_1^{-1}$ is a unit of order two and

$$\left(x_1'x_1^{-1} + (x_1'x_1^{-1})^*\right)(1+a)^{2l} = x_1'(x_1^{-1} + (x_1^{-1})^*)(1+a)^{2l} = 0.$$

Therefore

$$x_1'x_1^{-1} \in L_{2l}^* = \left\{ h \in V(\mathbb{F}_2C)[2] \;\middle|\; (h+h^*)(1+a)^{2l} = 0 \right\},$$

so $x_1' \in x_1 \cdot L_{2l}^*$ and the number of different elements x_1' is $\left|L_{2l}^*\right|$.

Finally, we shall determine the number of elements $x_2 = \gamma(1+a)^i$ for a fixed i, where $\gamma \in V(\mathbb{F}_2C)$. This number coincides with the cardinality of the set

$$K_{2l} = \left\{ \gamma(1+a)^{2l} \;\middle|\; \gamma \in V(\mathbb{F}_2C),\ \gamma\gamma^*(a+a^{-1})^{2l} \in \mathbb{F}_2C^2 \right\}.$$

Clearly K_{2l} coincides with $H_i^*(1+a)^{2l}$. But $\gamma(1+a)^{2l} = \gamma'(1+a)^{2l}$ if and only if $\gamma^{-1}\gamma'(1+a)^{2l} = (1+a)^{2l}$, so $\gamma^{-1}\gamma' \in S_{2l}$. We have established the equality $\left|K_{2l}\right| = \frac{|H_{2l}^*|}{|S_{2l}|}$. Hence the number of units of type 1 of the form $x_1 + x_2b_2$ for a fixed $0 < 2l < 2^{n-1}$ is equal to

$$\frac{\left|H_{2l}^*\right|}{\left|S_{2l}\right|} \cdot \left|L_{2l}^*\right| = 2^{2^{n+1}}.$$

Now consider the case when $2^{n-1} \leq i < 2^n$. Then $(a+a^{-1})^i = 0$, and (2.13) implies that the unit $x_1 + x_2 b_2$ is such that $x_1 \in V(\mathbb{F}_2 C)[2]$ and (2.14) is always satisfied. Thus $x_2 \in V(\mathbb{F}_2 C)(1+a)^i$ and there are

$$\frac{\left|V(\mathbb{F}_2 C)\right|}{\left|S_i\right|} \cdot \left|V(\mathbb{F}_2 C)[2]\right|$$

different units of type 1 in $V(\mathbb{F}_2 D_{2^{n+1}})$. We obtain that in $V(\mathbb{F}_2 D_{2^{n+1}})$ the number of units of type 1 is equal to

$$\left|V(\mathbb{F}_2 C)[2]\right| + \sum_{l=1}^{2^{n-2}-1} \frac{|H_{2l}^*|}{|S_{2l}|} \cdot \left|L_{2l}^*\right| + \sum_{j=2^{n-1}}^{2^n-1} \frac{|V(\mathbb{F}_2 C)|}{|S_j|} \cdot \left|V(\mathbb{F}_2 C)[2]\right|$$

$$2^{2^{n-1}} + \sum_{j=1}^{2^{n-2}-1} 2^{2^n+1} + 2^{2^{n-1}} \sum_{j=2^{n-1}}^{2^n-1} 2^{2^{n-1}} 2^{-j} = 2^{2^n}(2^{n-1}-1).$$

Now let us consider the number of units of type 2 in $V(\mathbb{F}_2 D_{2^{n+1}})$. If $x_1 + x_2 b_2$ is a unit of type 2 then x_2 is a unit and according to (2.4) we have $x_1 = x_1^*$ and $x_2 x_2^* = (1+x_1)^2$. Evidently $1 + x_1$ is a $*$-symmetric unit and $x_2 x_2^* \in V(\mathbb{F}_2 C^2)$. By the first part of Lemma 2.2.1, for a fixed unit x_2, the set

$$\left\{ 1 + x_1 \in S_*(C) \;\middle|\; (1+x_1)^2 = x_2 x_2^* \right\}$$

is a coset of $S_*(C)$ by $S_*(C)[2]$. Therefore the number of the different x_1 is $\left|S_*(C)[2]\right|$. Clearly L_0^* coincides with $S_*(C)[2]$, so for a fixed x_2 the number of the different x_1 is $\left|L_0^*\right|$.

Since $H_0^* = \left\{ h \in V(\mathbb{F}_2 C) \;\middle|\; hh^* \in V(\mathbb{F}_2 C^2) \right\}$, the number of the different x_2 coincides with $|H_0^*|$. This shows that in $V(\mathbb{F}_2 D_{2^{n+1}})$ the number of the units of type 2 is

$$\left|H_0^*\right| \cdot \left|L_0^*\right| = 2^{3 \cdot 2^{n-2} + 2^{n-2} + 1} = 2^{2^n+1}$$

and

$$\Theta_{D_{2^{n+1}}}(2) = 2^{2^n+n-1} + 2^{2^n}.$$

Now let us consider the generalized quaternion group. Let $x_1 + x_2 b_1$ be a unit of type 2. Similarly to the previous case, x_1 is $*$-symmetric and

$$x_1^2 + x_2 x_2^* a^{2^{n-1}} = x_1 x_1^* + x_2 x_2^* a^{2^{n-1}} = 1.$$

Since $1 \notin supp\,(x_1x_1^*)$ and $1 \notin supp\,(x_2x_2^*a^{2^{n-1}})$, by Lemma 2.2.1 this equality is impossible. Therefore, there is no unit of type 2 in $V(\mathbb{F}_2Q_{2^{n+1}})$.

By Lemma 2.3.2, in $V(\mathbb{F}_2Q_{2^{n+1}})$ the number of units of type 1 is $(2^{n-1}-1)2^{2^n}$ and

$$\Theta_{Q_{2^{n+1}}}(2) = 2^{2^n+n-1} - 2^{2^n}.$$

Finally, let us consider the semidihedral group. According to (2.12) and Lemma 2.4.1, we have $\left|H_i^{\circledast}\right| = \left|H_i^*\right|$ and $\left|L_i^{\circledast}\right| = \left|L_i^*\right|$ for each index $i < 2^n$. Thus in $V(\mathbb{F}_2SD_{2^{n+1}})$ the number of units of type 1 is $(2^{n-1}-1)2^{2^n}$ as in the group of units $V(\mathbb{F}_2D_{2^{n+1}})$ for the dihedral group.

We shall determine the number of units $x_1 + x_2b_3 \in V(\mathbb{F}_2SD_{2^{n+1}})$ of type 2. Then x_2 is a unit and from equation (2.4) it follows that $x_2^{\circledast}x_2 = (x_1+1)^2 \in V(\mathbb{F}_2C^2)$ and $(x_1 + x_1^{\circledast})x_2 = 0$. Since x_2 is a unit we get that x_1 is a $\circledast$-symmetric, so $1 + x_1$ is a $\circledast$-symmetric unit as well. Evidently $x_2^{\circledast}x_2 = (1+x_1)^2 \in S_{\circledast}(C)^2$. We have seen that

$$J_{\circledast} = \left\{\, x_2x_2^{\circledast} \;\middle|\; x_2 \in V(\mathbb{F}_2C),\ x_2x_2^{\circledast} \in \mathbb{F}_2C^2 \,\right\} = \langle\, a^{2^{n-1}} \rangle \times S_{\circledast}(C)^2,$$

thus the number of different x_2 is

$$\left|\left\{\, x_2 \in V(\mathbb{F}C) \;\middle|\; x_2x_2^{\circledast} \in S_{\circledast}(C)^2 \,\right\}\right|$$

$$= \left|V_{\circledast}(\mathbb{F}C)\right| \cdot \left|S_{\circledast}(C)^2\right| = \left|V_{\circledast}(\mathbb{F}C)\right| \cdot \tfrac{|J_{\circledast}|}{2} = \tfrac{|H_0^{\circledast}|}{2}.$$

For a fixed unit x_2 the set $\left\{\, 1 + x_1 \in S_{\circledast}(C) \;\middle|\; (1+x_1)^2 = x_2x_2^{\circledast} \,\right\}$ is a coset of $S_{\circledast}(C)$ by $S_{\circledast}(C)[2]$ as the first part of Proposition 2.1.4 asserts. Clearly, $L_0^{\circledast}$ coincides with $S_{\circledast}(C)[2]$, so for a fixed x_2 the number of the different x_1 is $\left|L_0^{\circledast}\right|$. We obtain that the number of units of type 2 is

$$\tfrac{|H_0^{\circledast}|}{2} \cdot \left|L_0^{\circledast}\right| = 2^{3\cdot 2^{n-2}+2^{n-2}} = 2^{2^n}$$

and $\Theta_{SD_{2^{n+1}}}(2) = 2^{2^n+n-1}$, the proof is done.

□

Using this theorem we can solve the isomorphism problem of the normalized group of units for group algebra of 2-group of maximal class over the field of element two.

Corollary 2.4.4. *Let $\mathbb{F}_2$ be the field of two elements, and let G and H be finite 2-groups of maximal class. Then $V(\mathbb{F}_2G)$ is isomorphic to $V(\mathbb{F}_2H)$ if and only if G and H are isomorphic.*

Proof. This follows immediately from the previous theorem.

□

We note that the previous corollary is a generalization of Baginski's result [3].

Chapter 3

Structure of group of units with class p

3.1 Preliminary results

This chapter includes results of [5].

We begin with the description of the center $\zeta\big(V(\mathbb{F}_pG)\big)$ of $V(\mathbb{F}_pG)$, where G is a finite p-group with commutator subgroup G' of order p and $p > 2$. Let $C_{g_1}, \ldots, C_{g_t}$ be all the different conjugacy classes of G which contain at least two elements. It is easy to check that $t = \frac{|G|-|\zeta(G)|}{p}$,

$$\widehat{C_{g_i}} = g_i\widehat{G'}, \qquad \widehat{C_{g_i}}\widehat{C_{g_j}} = 0 \qquad (1 \leq i, j \leq t)$$

and $\widehat{G'}$ is a central element with square 0.

Clearly, the set of all elements of the form $\sum_{i=1}^{t} \alpha_i\widehat{C_{g_i}}$ is an ideal of the center $\zeta(\mathbb{F}_pG)$. It follows that every central unit $x \in \zeta\big(V(\mathbb{F}_pG)\big)$ can be written as

$$x = z + \sum_{i=1}^{t} \alpha_i\widehat{C_{g_i}} = z\Big(1 + \sum_{i=1}^{t} \beta_i\widehat{C_{g_i}}\Big) = z\prod_{i=1}^{t}\big(1 + g_i\widehat{G'}\big)^{\beta_i}, \tag{3.1}$$

where $z \in V\big(\mathbb{F}_p\zeta(G)\big)$ and $\alpha_i, \beta_i \in \mathbb{F}_p$. Also it is easy to check that

$$\big|V\big(\mathbb{F}_p\zeta(G)\big)\big| = p^{|\zeta(G)|-1},$$

$$\left|\zeta\big(V(\mathbb{F}_pG)\big)\right| = p^{\frac{|G|+(p-1)|\zeta(G)|-p}{p}}, \tag{3.2}$$

and according to (3.1) we get

$$\zeta\big(V(\mathbb{F}_pG)\big) = V\big(\mathbb{F}_p\zeta(G)\big) \times N, \tag{3.3}$$

where $N = \prod_{i=1}^{t}\langle 1+\widehat{C_{g_i}}\rangle$ is an elementary abelian subgroup of $V(\mathbb{F}_pG)$.

Further, the commutator subgroup $V(\mathbb{F}_pG)'$ has exponent p because it is a subgroup of $1+I(G')$ and $I(G')^p = 0$, where $I(G')$ is the ideal generated by the elements of the form $h-1$ with $h \in G'$.

We shall need the following results:

Proposition 3.1.1 (Huppert [32], Lemma III.9.6). *Let $U(\mathbb{F}_p)$ be the group of units of $\mathbb{F}_p$ with odd prime p. Then*

$$\sum_{k\in U(\mathbb{F}_p)} k^r = \begin{cases} 0 \text{ for } & 1 \le r \le p-2; \\ p-1 \text{ for } & r = p-1. \end{cases}$$

Proposition 3.1.2 (Hall [29], Theorem 12.4.2). *A finite p-group G is regular if and only if, for any x, y in G we have*

$$x^p y^p = (xy)^p d^p,$$

with d in the commutator subgroup of the group generated by x and y.

Denote by $[\mathbb{F}_pG, \mathbb{F}_pG]$ the span of all ring commutators $xy - yx$ with $x, y \in \mathbb{F}_pG$, which is called the *commutator subspace* of $\mathbb{F}_pG$.

Proposition 3.1.3 (Brauer [23]). *An element $\sum_{g\in G}\alpha_g g$ belongs to the commutator subspace $[\mathbb{F}_pG, \mathbb{F}_pG]$ if and only if $\sum_{g\in C_h}\alpha_g = 0$ for every conjugacy class C_h of G. Moreover*

$$(x+y)^p \equiv x^p + y^p \pmod{[\mathbb{F}_pG, \mathbb{F}_pG]}$$

for any $x, y \in \mathbb{F}_pG$.

Definition 3.1.4. *We say that G is a central product $G_1 \curlyvee G_2$ of its subgroups G_1 and G_2 if the elements of G_1 and G_2 commute and together generate G, and $G_1 \cap G_2$ is the center of one of the factors G_1, G_2.*

Proposition 3.1.5 (Berger, Kovács and Newman [8]). *Every finite p-group ($p > 2$) with cyclic Frattini subgroup has the following representation:*

$$G = E \times (G_0 \curlyvee G_1 \curlyvee \cdots \curlyvee G_s), \tag{3.4}$$

where E is elementary abelian, $G_1, \cdots, G_s$ are nonabelian of order p^3, of exponent p, while $\left|G_0\right| > 1$ if $\left|E\right| > 1$, and G_0 has one of the following types: cyclic $C_{p^n} = \langle\ a_0 \mid a_0^{p^n} = 1\ \rangle$, or nonabelian with cyclic maximal subgroup

$$M_{p^n} = \langle\ a_0, b_0 \mid a_0^{p^{n-1}} = b_0^p = 1, (a_0, b_0) = a_0^{p^{n-2}}\ \rangle,$$

and for $i > 0$

$$G_i = \langle\ a_i, b_i \mid {a_i}^p = {b_i}^p = 1, (a_i, b_i) = c, (a_i, c) = (b_i, c) = 1\ \rangle.$$

3.2 p th powers of normalized group of units

We begin to investigate the p th powers of normalized group of units $V(\mathbb{F}_pG)$.

Theorem 3.2.1. *Let G be a finite p-group with commutator subgroup G' of order $p > 2$. Then $V(\mathbb{F}_pG)^p$ is a subgroup of the center $\zeta\big(V(\mathbb{F}_pG)\big)$.*

Proof. Let H be the subgroup of $V(\mathbb{F}_pG)$ generated by x and y, where $x \in V(\mathbb{F}_pG)$, $g \in G$, and $y = g^{-1}xg$. Evidently,

$$\begin{aligned}(x,y) &= x^{-1}(g,x)x(x,g)\\ &= \big(x,(x,g)\big) \in \gamma_3\big(V(\mathbb{F}_pG)\big),\end{aligned}$$

so the factor group $H\gamma_3\big(V(\mathbb{F}_pG)\big)/\gamma_3\big(V(\mathbb{F}_pG)\big)$ is abelian. Thus H' is contained in $\gamma_3\big(V(\mathbb{F}_pG)\big)$ and the nilpotency class of H is less than p. Then H is a regular p-group and so, according to Proposition 3.1.2, we have

$$x^{-p}y^p = (x^{-1}y)^p d^p = (x,g)^p d^p$$

for some element d of the commutator subgroup of $V(\mathbb{F}_pG)$. But $V(\mathbb{F}_pG)'$ has exponent p, so $x^{-p}y^p = 1$ and $x^p = g^{-1}x^pg$ for all $g \in G$. Thus x^p is central, as asserted.

□

Lemma 3.2.2. *Let H be a group generated by two elements a, b, and suppose that its commutator subgroup H' is central of prime order p. In any group ring of H,*

$$(a+b)^p = a^p + b^p + \sum_{r=1}^{p-1} \frac{1}{p}\binom{p}{r} a^r b^{p-r} \widehat{H'}. \tag{3.5}$$

Proof. As a first step, observe that $\zeta(H) = \langle a^p, b^p\rangle H'$ has index p^2, and that the centralizer of any non-central element h is $\langle h\rangle\zeta(H)$. For $k, r \in \{1, 2, \ldots, p-1\}$ and $c_1, \ldots, c_p \in \{a, b\}$ with $c_1 \cdots c_p \in a^r b^{p-r} H'$,

it follows that no element of the coset $a^r b^{p-r} H'$ can commute with the product $c_1 \cdots c_k$ and so

$$c_{k+1} \cdots c_p c_1 \cdots c_k = (c_1 \cdots c_k)^{-1}(c_1 \cdots c_p)(c_1 \cdots c_k) \neq c_1 \cdots c_p.$$

Next, consider the set of all words $z_1 z_2 \cdots z_p$ of length p in the alphabet $\{x, y\}$, as elements of the free semigroup S freely generated by $\{x, y\}$. The group of order p acts on this set by cyclically permuting the letters of a word. It is easy to see that there are only two words fixed under this action, x^p and y^p. Since p is prime, the length of each non-singleton orbit is p. There are precisely $\binom{p}{r}$ words in which x occurs r times and y occurs $p-r$ times, and we conclude that these are permuted in $\frac{1}{p}\binom{p}{r}$ orbits.

Let $\sigma : S \to H$ be the homomorphism defined by $x \mapsto a,\ y \mapsto b$. The images of the orbits we counted all lie in the coset $a^r b^{p-r} H'$. The point of the first step of our argument was to show that the restriction of σ to each of these orbits is one-to-one. Since each orbit has length p and this is also the number of elements in the coset, it follows that each element of $a^r b^{p-r} H'$ is the image of precisely $\frac{1}{p}\binom{p}{r}$ of the words under consideration.

□

Let $x = \sum_{g \in G} \alpha_g g \in V(\mathbb{F}_p G)$. From Proposition 3.1.3, we know that $x^p = y + u$, where $y = \sum_{g \in G} \alpha_g g^p$ and $u \in [\mathbb{F}_p G, \mathbb{F}_p G]$. Lemma 3.2.1 tells us that x^p and the g^p are central in $\mathbb{F}_p G$; therefore so is y, and then also u. By Lemma 3.1.3 again, the support of u cannot contain any element of $\zeta(G)$, so u must be a linear combination of the $\widehat{C_{g_i}}$. Thus $u^2 = 0$, and then

$$x^{p^2} = (y+u)^p = y^p = \Big(\sum_{g \in G} \alpha_g g^p\Big)^p = \sum_{g \in G} \alpha_g g^{p^2}, \tag{3.6}$$

because each g^p is central. We have proved that $V(\mathbb{F}_p G)^{p^2} = V(\mathbb{F}_p G^{p^2})$. When $\exp G > p$, this shows that the exponents of the groups $V(\mathbb{F}_p G)$ and G coincide. Consider next the case $\exp(G) = p$. Choose $a, b \in G$

with $(a,b) \neq 1$. Then $a+b-1 \in V(\mathbb{F}_pG)$ and by (3.5) we have $(a+b-1)^p = (a+b)^p - 1 \neq 1$. It follows that

$$\exp\big(V(\mathbb{F}_pG)\big) = \begin{cases} \exp(G) & \text{if} \quad \exp(G) > p; \\ p^2 & \text{if} \quad \exp(G) = p. \end{cases} \tag{3.7}$$

Theorem 3.2.3. *Let G be a finite nonabelian p-group with $|\Phi(G)| = p$. Then $V(\mathbb{F}_pG)^p = V\big(\mathbb{F}_pG^p\big) \times N$, where $N = \prod_{i=1}^{t} \langle 1 + \widehat{C_{g_i}} \rangle$.*

Proof. First we shall prove that $N \subseteq V(\mathbb{F}_pG)^p$. Let $\gamma \in U(\mathbb{F}_p)$, $g \in G \setminus \zeta(G)$ and $h \in G$ such that $(g,h) \neq 1$. The commutator subgroup of $\langle h, g^{-1}h \rangle$ coincides with G' and

$$\widehat{G'}h^{-p} = \widehat{G'}, \qquad \big((g^{-1}h)^p - 1\big)\widehat{G'} = 0, \tag{3.8}$$

because h^p, $(g^{-1}h)^p \in G'$.

Clearly, for each $\gamma \in U(\mathbb{F}_p)$ the element $u_\gamma = h + \gamma(g^{-1}h - 1)$ is a unit in $\mathbb{F}_pG$. By (3.5) and (3.8)

$$\begin{aligned} u_\gamma^p &= \big((h + \gamma g^{-1}h) - \gamma\big)^p = (h + \gamma g^{-1}h)^p - \gamma^p \\ &= h^p + \gamma\big((g^{-1}h)^p - 1\big) + \sum_{r=1}^{p-1} \tfrac{1}{p}\tbinom{p}{r} h^r (\gamma g^{-1}h)^{p-r} \widehat{G'}. \end{aligned}$$

It follows that, with γ ranging over $U(\mathbb{F}_p)$,

$$\begin{aligned} \prod_{\gamma \in U(\mathbb{F}_p)} (u_\gamma^p h^{-p}) = 1 &+ \Big(\sum_{\gamma \in U(\mathbb{F}_p)} \gamma\Big)\big((g^{-1}h)^p - 1\big)h^{-p} \\ &+ \sum_{r=1}^{p-1} \tfrac{1}{p}\tbinom{p}{r} \Big(\sum_{\gamma \in U(\mathbb{F}_p)} \gamma^{p-r}\Big) h^r (g^{-1}h)^{p-r} \widehat{G'} \end{aligned}$$

and here, by Proposition 3.1.1, all summands with $r > 1$ vanish, leaving

$$\prod_{\gamma \in U(\mathbb{F}_p)} (u_\gamma^p h^{-p}) = 1 - h(g^{-1}h)^{p-1}\widehat{G'}.$$

Since $(g^{-1}h)^p\widehat{G'} = \widehat{G'}$ by (3.8), we have $h(g^{-1}h)^{-1}(g^{-1}h)^p\widehat{G'} = g\widehat{G'}$ and

$$\prod_{\gamma\in U(\mathbb{F}_p)} (u_\gamma^p h^{-p}) = 1 - g\widehat{G'} = (1 + g\widehat{G'})^{-1}.$$

Thus $1 + g\widehat{G'} = \left(\prod_{\gamma\in U(\mathbb{F}_p)}(u_\gamma^p h^{-p})\right)^{-1} \in V(\mathbb{F}_pG)^p$. Since the elements of the form $1 + g\widehat{G'}$ constitute a generator system of N, we have proved that $N \subseteq V(\mathbb{F}_pG)^p$, as required.

Let G^p be a nontrivial subgroup of G. Since $\Phi(G)$ is cyclic, then $G^p = \langle g^p\rangle$ for some $g \in G$ and

$$V(\mathbb{F}_p\langle g^p\rangle) \subseteq V(\mathbb{F}_p\langle g\rangle)^p \subseteq V(\mathbb{F}_pG)^p.$$

Thus we have proved that $V\left(\mathbb{F}_pG^p\right) \times N \subseteq V(\mathbb{F}_pG)^p$.

Finally, the relation $V(\mathbb{F}_pG)^p \subseteq V\left(\mathbb{F}_pG^p\right) \times N$ follows from (3.6) and the prove is complete.

□

The following question: for which nonabelian p-group G is it true that $G \cap V(\mathbb{F}_pG)^p = G^p$, is due to Johnson [35]. The previous lemma can be applied to conclude the following

Corollary 3.2.4. *Let G be a finite p-group such that $|\Phi(G)| = p > 2$. Then*

$$G \cap V(\mathbb{F}_pG)^p = G^p.$$

Proof. By Lemma 3.2.3 we get $V(\mathbb{F}_pG)^p = V\left(\mathbb{F}_pG^p\right) \times N$, and so

$$G \cap V(\mathbb{F}_pG)^p = G \cap V\left(\mathbb{F}_pG^p\right) = G^p.$$

□

Now we can prove that the normalized group of units $V(\mathbb{F}_pG)$ determines the nonabelian p-group G if G has cyclic Frattini subgroup.

Theorem 3.2.5. *Let G and H be finite nonabelian p-groups with cyclic Frattini subgroup and $p > 2$. Then $V(\mathbb{F}_pG)$ is isomorphic to $V(\mathbb{F}_pH)$ if and only if G and H are isomorphic.*

Proof. It follows from Proposition 3.1.5 that, when $p > 2$, every finite nonabelian p-group G with cyclic Frattini subgroup may be written as

$$G = E \times (K \rtimes L), \tag{3.9}$$

where E is elementary abelian, K is either of order p or an extraspecial group of exponent p, and L is either nontrivial cyclic or nonabelian with a cyclic maximal subgroup, that is, L is either $C_{p^n} = \langle\, a \,|\, a^{p^n} = 1 \,\rangle$ with $n \geq 1$ or

$$M_{p^n} = \langle\ a, b \ \mid\ a^{p^{n-1}} = b^p = 1,\ \ (a,b) = a^{p^{n-2}}\ \rangle \qquad \text{with} \quad n \geq 3.$$

It is obvious that L is cyclic if and only if $\exp(G) = \exp\big(\zeta(G)\big)$; in this case, $\big|L\big| = \exp(G)$ and $\big|K\big| = p \cdot \big|G : \zeta(G)\big|$, and otherwise $\big|L\big| = p \cdot \exp(G)$ and $\big|L\big| = p^{-1} \cdot \big|G : \zeta(G)\big|$. Consequently, the isomorphism type of such a group is determined by the orders and exponents of the group and its center.

The nontrivial part of the proof of the theorem is the claim that these four invariants of G are recognizable from the isomorphism type of $V(\mathbb{F}_pG)$.

First, $\big|G\big|$ is recognizable from $\big|V(\mathbb{F}_pG)\big|$, and then $\big|\zeta(G)\big|$ can be computed from $\big|\zeta\big(V(\mathbb{F}_pG)\big)\big|$ and (3.2). Using (3.1), it is not hard to see that

$$\exp\big(\zeta(G)\big) = \exp\Big(\zeta\big(V(\mathbb{F}_pG)\big)\Big).$$

It remains to show that the exponent of G is also recognizable. By (3.7) if $\exp\big(V(\mathbb{F}_pG)\big) > p^2$ then $\exp\big(V(\mathbb{F}_pG)\big) = \exp(G)$ and so we only have an issue when $\exp\big(V(\mathbb{F}_pG)\big) = p^2$.

In this outstanding case $\exp(G) \leq p^2$, so we obtain that $\big|\Phi(G)\big|$ is equals to p. Indeed, it is clearly for the group G with $\exp(G) = p$. If $\exp(G)$ is equal to p^2 then by (3.9) $\exp(G) = \exp(L) = p^2$. Clearly $\Phi(G) = \Phi(L)$ and from the fact that L is isomorphic to either C_{p^2} or M_{p^3} follows that the subgroup $\Phi(G)$ has order p.

Then with respect to Lemma 3.2.3 $V(\mathbb{F}_pG)^p = V\left(\mathbb{F}_pG^p\right)\times N$, where $\left|N\right| = p^{\frac{|G|-|\zeta(G)|}{p}}$. Therefore we can determine whether $\left|G^p\right|$ is either 1 or p. We have proved that the exponent of G is also recognizable, as required.

□

Chapter 4

Filtered multiplicative basis

4.1 Preliminary results

This chapter includes results of [4].

In this chapter we shall investigate the existence of filtered multiplicative basis of group algebras. Assume that B is a filtered multiplicative $\mathbb{F}$-basis for a finite-dimensional $\mathbb{F}$-algebra A. In the proof of the main results we shall use the following simple properties of B.

Proposition 4.1.1 (V. Bovdi [16]). *$B \cap rad(A)^n$ is an $\mathbb{F}$-basis of $rad(A)^n$ for all $n \geq 1$.*

Proposition 4.1.2 (V. Bovdi [16]). *If $u, v \in B \setminus rad(A)^k$ and $u \equiv v \pmod{rad(A)^k}$ then $u = v$.*

Recall that the *Frattini subalgebra* $\Phi(A)$ of A is defined as the intersection of all maximal subalgebras of A if those exist, and as A otherwise. If A is a nilpotent algebra over a field $\mathbb{F}$ then $\Phi(A) = A^2$ by [24]. This implies

Proposition 4.1.3 (V. Bovdi [16]). *If B is a filtered multiplicative $\mathbb{F}$-basis of A and if $B \setminus \{1\} \subseteq rad(A)$ then all elements of $B \setminus rad(A)^2$ are generators of A over $\mathbb{F}$.*

Proposition 4.1.4 (V. Bovdi [16]). *Let G be a finite metacyclic p-group and $\mathbb{F}$ a field of characteristic p. Then the group algebra $\mathbb{F}G$ possesses a filtered multiplicative $\mathbb{F}$-basis if and only if $p = 2$ and exactly one of the following conditions holds:*

1. *G is a dihedral group;*

2. *$\mathbb{F}$ contains a primitive cube root of the unity and G is the quaternion group Q_8 of order 8.*

Proposition 4.1.5 (V. Bovdi [17]). *Let $\mathbb{F}$ be a field of characteristic p and let G satisfy one of the following conditions:*

1. *G is a nonabelian powerful p-group;*

2. *p is odd, and G is a 2-generated nonabelian p-group with a central cyclic commutator subgroup.*

Then the group algebra $\mathbb{F}G$ does not have a filtered multiplicative $\mathbb{F}$-basis.

Proposition 4.1.6 (V. Bovdi [17]). *Let $\mathbb{F}$ be a field of characteristic p and let G be a nonabelian p-group with a cyclic subgroup of index p^2. Then the group algebra $\mathbb{F}G$ possesses a filtered multiplicative $\mathbb{F}$-basis if and only if $p = 2$ and one of the following conditions is satisfied:*

1. *G is either the dihedral 2-group or $D_{2^m} \times C_2$ or the central product $D_8 \curlyvee C_4$ of D_8 with C_4;*

2. *$\mathbb{F}$ contains a primitive cube root of the unity and G is either $Q_8 \times C_2$ or Q_8;*

3. *G is one of the following groups:*

$$
\begin{aligned}
G_5 = \langle\ a,c,d\ \mid\ & a^{2^{m-2}} = c^2 = d^2 = 1,\\
& (d,a) = (d,c) = 1,\ (c,a) = d\ \rangle,\ \textit{with } m \geq 4;\\
G_{13} = \langle\ a,c,d\ \mid\ & a^{2^{m-2}} = c^2 = d^2 = 1,\\
& (d,a) = (d,c) = 1,\ (c,a) = a^2 d = \ \rangle,\ \textit{with } m \geq 5;\\
G_{14} = \langle\ a,c,d\ \mid\ & a^{2^{m-2}} = d^2 = 1,\ c^2 = a^{2^{m-3}},\\
& (d,a) = (d,c) = 1,\ (c,a) = a^2 d\ \rangle,\ \textit{with } m \geq 5;\\
G_{17} = \langle\ a,c,d\ \mid\ & a^{2^{m-2}} = d^2 = c^2 = 1,\\
& (d,a) = a^{2^{m-3}},\ (d,c) = 1,\ (c,a) = d\ \rangle, m \geq 5;\\
G_{18} = \langle\ a,c,d\ \mid\ & a^{2^{m-2}} = d^2 = 1,\ c^2 = d,\\
& (d,a) = a^{2^{m-3}},\ (c,a) = a^2 d\ \rangle,\ \textit{with } m \geq 4;\\
G_{22} = \langle\ a,c,d\ \mid\ & a^{2^{m-2}} = c^2 = d^2 = 1,\ (d,a) = 1,\\
& (d,c) = a^{2^{m-3}},\ (c,a) = a^{-2^{m-4}} d\ \rangle,\ \textit{with } m \geq 6;\\
G_{23} = \langle\ a,c,d\ \mid\ & a^{2^{m-2}} = c^2 = d^2 = 1,\ (d,a) = 1,\\
& (d,c) = a^{2^{m-3}},\ (c,a) = a^{2-2^{m-4}} d\ \rangle,\ \textit{with } m \geq 6;\\
G_{24} = \langle\ a,c,d\ \mid\ & a^{2^{m-2}} = c^2 = d^2 = 1,\ (d,c) = 1, =\\
& (d,a) = a^{2^{m-3}},\ (c,a) = a^{2-2^{m-4}} d\ \rangle,\ \textit{with } m \geq 6;\\
G_{25} = \langle\ a,c,d\ \mid\ & a^{2^{m-2}} = d^2 = 1,\ c^2 = a^{2^{m-3}},\ (d,c) = 1,\\
& (d,a) = a^{2^{m-3}},\ (c,a) = a^{2-2^{m-4}} d\ \rangle,\ \textit{with } m \geq 5.
\end{aligned}
$$

Proposition 4.1.7 (V. Bovdi [16]). *Let G be the group*

$$H_{16} = \langle\ a,c\ \mid\ a^4 = b^2 = c^2 = 1,\ (a,b) = 1,\ (a,c) = b,\ (b,c) = 1\ \rangle$$

and $\mathbb{F}$ a field of characteristic 2. Then the group algebra $\mathbb{F}G$ possesses a filtered multiplicative $\mathbb{F}$-basis.

Proposition 4.1.8 (B. Huppert [32]). *Let G be a group of order p^4 and $p > 2$. Then G is one of the following groups:*

1. $\langle\ a,b\ \mid\ a^{p^3} = b^p = 1,\ (a,b) = a^{p^2}\ \rangle$;

2. $\langle\ a,b,c\ \mid\ a^{p^2}=b^p=c^p=1,\ \ (a,b)=(a,c)=1,\ \ (b,c)=a^p\ \rangle$;

3. $\langle\ a,b\ \mid\ a^{p^2}=b^{p^2}=1,\ \ (a,b)=a^p\ \rangle$;

4. $\langle\ a,b,c\ \mid\ a^{p^2}=b^p=c^p=1,\ \ (a,b)=(b,c)=1,\ \ (a,c)=a^p,\ \ \rangle$;

5. $\langle\ a,c\ \mid\ a^{p^2}=c^p=1,\ \ (a,b)=(b,c)=1,\ \ (a,c)=b,\ \ \rangle$;

6. $\langle\ a,c\ \mid\ a^{p^2}=c^p=1,\ \ (a,b)=a^p,\ \ (a,c)=b,\ \ (b,c)=1\ \rangle$;

7. *a) for* $p=3$ $\langle\ a,c\ \mid\ a^9=1,\ \ c^3=a^3,\ \ (a,b)=a^3,$
$(a,c)=b^{-1},\ \ (b,c)=1\ \rangle$;

b) for $p>3$ $\langle\ a,c\ \mid\ a^{p^2}=c^p=1,\ \ (a,b)=a^p,$
$(a,c)=b,\ \ (b,c)=a^p\ \rangle$;

8. *a) for* $p=3$ $\langle\ a,c\ \mid\ a^9=1,\ \ c^3=a^{-3},\ \ (a,b)=a^3,$
$(a,c)=b^{-1},\ \ (b,c)=1\ \rangle$;

b) for $p>3$ $\langle\ a,c\ \mid\ a^{p^2}=c^p=1,\ \ (a,b)=a^p,$
$(a,c)=b,\ \ (b,c)=a^{\alpha p}\ \rangle$;
and α *is any nonresidue modulo* p;

9. $\langle\ a,c\ \mid\ a^p=c^p=1,\ (a,c)=d,(c,d)=(a,d)=1\ \rangle$
$\times\langle\ h\ \mid\ h^p=1\ \rangle$;

10. *for* $p>3$

$\langle\ a,c\ \mid\ a^p=c^p=1,\ \ (a,c)=d,(d,c)=f,$
$(a,d)=(a,f)=(c,f)=(d,f)=1\ \rangle$;

11. *for* $p=3$ $\langle\ a,b,c\ \mid\ a^9=b^3=c^3=1,\ \ (a,b)=1,$
$(a,c)=b,\ \ (b,c)=a^{-3}\ \rangle$.

4.2 Lazard-Jennings series

We define the *Lazard-Jennings series* $M_i(G)$ of a finite p-group G by induction. Put

$$M_1(G) = G \qquad \text{and} \qquad M_i(G) = \langle\ (M_{i-1}(G), G), M^p_{[\frac{i}{p}]}(G)\ \rangle,$$

where

- $[\frac{i}{p}]$ is the smallest integer not less than $\frac{i}{p}$;
- $\big(M_{i-1}(G), G\big) = \langle\ (u,v)\ \mid\ u \in M_{i-1}(G),\ \ v \in\ G\ \rangle$;
- $M^p_i(G)$ is the subgroup generated by the p-powers of the elements of $M_i(G)$.

Evidently,

$$M_1(G) \supseteq M_2(G) \supseteq \cdots \supseteq M_t(G) = 1.$$

Let $\mathbb{F}$ be a field of characteristic p. Since G is a finite p-group, $A(\mathbb{F}G)$ is nilpotent, and

$$A(\mathbb{F}G) \supset A^2(\mathbb{F}G) \supset \cdots \supset A^s(\mathbb{F}G) \supset A^{s+1}(\mathbb{F}G) = 0.$$

Then the subgroup $\mathfrak{D}_n(G) = \left\{\ g \in G\ \mid\ g - 1 \in A^n(\mathbb{F}G)\ \right\}$ is called the nth *dimensional subgroup* of $\mathbb{F}G$. It is well known fact that for a finite p-group G, $M_i(G)$ coincides with $\mathfrak{D}_i(G)$ for all i.

Let $\mathbb{I} = \left\{\ i \in \mathbb{N}\ \mid\ \mathfrak{D}_i(G) \neq \mathfrak{D}_{i+1}(G)\ \right\}$. For $i \in \mathbb{I}$, let p^{d_i} be the order of the elementary abelian p-group

$$\mathfrak{D}_i(G)/\mathfrak{D}_{i+1}(G) = \prod_{j=1}^{d_i} \langle u_{ij}\mathfrak{D}_{i+1}(G)\rangle.$$

Hence each $g \in G$ can be written uniquely in the form

$$g = u_{11}^{\alpha_{11}} u_{12}^{\alpha_{12}} \cdots u_{1d_1}^{\alpha_{1d_1}} u_{21}^{\alpha_{21}} \cdots u_{2d_2}^{\alpha_{2d_2}} \ldots u_{i1}^{\alpha_{i1}} \cdots u_{id_i}^{\alpha_{id_i}} \cdots u_{s1}^{\alpha_{s1}} \cdots u_{sd_s}^{\alpha_{sd_s}},$$

where the indices are in lexicographic order, $i \in \mathbb{I}$, $0 \le \alpha_{ij} < p$, and s is defined as above.

Let $w = \prod_{l\in\mathbb{I}} \big(\prod_{k=1}^{d_l}(u_{lk}-1)^{y_{lk}}\big) \in A(\mathbb{F}G)$, where $0 \le y_{lk} < p$ and the indices of the factors are in lexicographic order. Then w is called a *regular element* of weight $\mu(w) = \sum_{l\in\mathbb{I}} \big(\sum_{k=1}^{d_l} l y_{lk}\big)$. By Jennings' theory [34] the regular elements with weight not less than t constitute an $\mathbb{F}$-basis for the ideal $A^t(\mathbb{F}G)$. Clearly,

$$\big\{\ (u_{1j}-1) + A^2(\mathbb{F}G)\ \big|\ j = 1, \dots, d_1\ \big\}$$

is an $\mathbb{F}$-basis of $A(\mathbb{F}G)/A^2(\mathbb{F}G)$. Note that $\mathfrak{D}_2(G)$ coincides with the Frattini subgroup of G, so the set $\big\{u_{11}, u_{12}, \dots, u_{1d_1}\big\}$ is a minimal generator system of G.

Suppose that $B_1 = \{1\} \cup \big\{b_1, b_2, \dots, b_{|G|-1}\big\}$ is a filtered multiplicative $\mathbb{F}$-basis for $\mathbb{F}G$. Then $B = B_1 \setminus \big\{1\big\}$ is a filtered multiplicative $\mathbb{F}$-basis of $A(\mathbb{F}G)$ and contains $\big|G\big| - 1$ elements.

Let $B \setminus \big(B \cap A^2(\mathbb{F}G)\big) = \big\{b_1, b_2, \dots, b_n\big\}$. Evidently, $n = d_1$ and

$$b_k \equiv \sum_{i=1}^{n} \alpha_{ki}(u_{1i}-1) \pmod{A^2(\mathbb{F}G)}, \tag{4.1}$$

where $\alpha_{ki} \in \mathbb{F}$ and $\Delta = det(\alpha_{ki}) \neq 0$. For units x, y of $\mathbb{F}G$ we have

$$\begin{aligned}(y-1)(x-1) = \big[(x-1)(y-1) + (x-1) + (y-1)\big](z-1)\\ + (x-1)(y-1) + (z-1),\end{aligned} \tag{4.2}$$

where $z = (y, x)$. Since $z_{ji} = (u_{1j}, u_{1i}) \in \mathfrak{D}_2(G)$ and $z_{ji} - 1 \in A^2(\mathbb{F}G)$, using (4.2) we obtain that

$$(u_{1j}-1)(u_{1i}-1) \equiv (u_{1i}-1)(u_{1j}-1) + (z_{ji}-1) \pmod{A^3(\mathbb{F}G)}.$$

Thus simple computations give that

$$\begin{aligned}b_k b_s \equiv \sum_{i=1}^{n} \alpha_{ki}\alpha_{si}(u_{1i}-1)^2 + \sum_{\substack{i,j=1\\ i<j}}^{n} (\alpha_{ki}\alpha_{sj} + \alpha_{kj}\alpha_{si})(u_{1i}-1)(u_{1j}-1)\\ + \sum_{\substack{i,j=1\\ i<j}}^{n} \alpha_{kj}\alpha_{si}(z_{ji}-1) \pmod{A^3(\mathbb{F}G)},\end{aligned}$$

where $k, s = 1, \dots, n$.

4.3 On filtered multiplicative $\mathbb{F}$-basis

Denote by $\mathfrak{A}$ the set of those groups which belong to one of the following types of nonabelian p-groups:

1. either metacyclic or powerful groups;
2. p-groups with cyclic subgroup of index p^2;
3. two generated p-groups ($p \neq 2$) with central cyclic commutator subgroup.

Note that if B_1 and B_2 are filtered multiplicative $\mathbb{F}$-bases of $\mathbb{F}G_1$ and $\mathbb{F}G_2$, respectively, then $B_1 \times B_2$ is a filtered multiplicative $\mathbb{F}$-basis of the group algebra $\mathbb{F}[G_1 \times G_2]$.

Theorem 4.3.1. *Let $\mathbb{F}G$ be the group algebra of a finite nonabelian p-group G of order p^n over a field $\mathbb{F}$ of characteristic p, where $n < 5$. Then $\mathbb{F}G$ possesses a filtered multiplicative $\mathbb{F}$-basis if and only if $p = 2$ and G is one of the following groups:*

1. *dihedral group D_n of order n, where n equals either 8 or 16;*
2. *either the quaternion group Q_8 of order 8 or $Q_8 \times C_2$, and $\mathbb{F}$ contains a primitive cube root of the unity;*
3. *either $D_8 \times C_2$, or the central product $D_8 \curlyvee C_4$ of D_8 with the cyclic group C_4 of order 4;*
4. $$H_{16} = \langle\ a, c \mid a^4 = b^2 = c^2 = 1,\ (a,b) = 1, (a,c) = b, (b,c) = 1\ \rangle.$$

Proof. Let $\mathbb{F}$ be a field of characteristic p (p is odd) and G a p-group of order p^4. The classification of these groups can be found in Proposition 4.1.8. According to Propositions 4.1.4, 4.1.5 and 4.1.6 if

G belongs to $\mathfrak{A}$ then G has no filtered multiplicative $\mathbb{F}$-basis. If G does not belong to $\mathfrak{A}$ then it is one of the following two groups:

$$H_1 = \langle\ a, c\ \mid\ a^p = c^p = 1,\ \ (a,c) = d, (d,c) = f, \\ (a,d) = (a,f) = (c,f) = (d,f) = 1\ \rangle,\ \text{with } p > 3;$$

and

$$H_2 = \langle\ a, c\ \mid\ a^p = c^p = 1, (a,c) = d, (c,d) = (a,d) = 1\ \rangle \\ \times \langle\ h \mid h^p = 1\ \rangle, \qquad \text{with } p \geq 3.$$

It is easy to check that in both group algebras $\mathbb{F}H_1$ and $\mathbb{F}H_2$:

$$(c-1)(a-1) \equiv (a-1)(c-1) - (d-1) \pmod{A^3(\mathbb{F}G)}. \tag{4.3}$$

Let us consider the following cases:

Case 1. Let $G = H_1$. Since

$$M_1(G) = G, \qquad M_2(G) = \langle G', G^p\rangle = \langle d, f\rangle, \\ M_3(G) = \langle\ (\langle d, f\rangle, G),\ G^p\ \rangle = \langle f\rangle,$$

we have that $\mu(d) = 2$ and $\mu(f) = 3$, where μ is the weight of these elements. Let

$$b_1 \equiv \alpha_1(a-1) + \alpha_2(c-1) \pmod{A^2(\mathbb{F}G)}$$

and

$$b_2 \equiv \beta_1(a-1) + \beta_2(c-1) \pmod{A^2(\mathbb{F}G)}$$

as in (4.1). Using (4.3) and

$$(d-1)(c-1) \equiv (c-1)(d-1) + (f-1) \pmod{A^4(\mathbb{F}G)},$$

let us compute $b_{i_1}b_{i_2}b_{i_3}$ modulo $A^4(\mathbb{F}G)$, where $(i_k = 1, 2)$. The result of our computations will be written in a table, consisting of the coefficients of the decomposition $b_{i_1}b_{i_2}b_{i_3}$ with respect to the basis

$$\Big\{\ (a-1)^{j_1}(c-1)^{j_2}(d-1)^{j_3}(f-1)^{j_4}\ \Big|\ j_1 + j_2 + 2j_3 + 3j_4 = 3; \\ j_1, j_2 = 0, 1, 2, 3;\ j_3, j_4 = 0, 1\ \Big\}$$

of the ideal $A^3(\mathbb{F}G)/A^4(\mathbb{F}G)$. We shall divide the table into two parts (the second part written below the first part). The coefficients corresponding to the first four basis elements will be in the first part of the table, while the next three will be in the second one. Thus

	$(a-1)^3$	$(a-1)^2(c-1)$	$(a-1)(d-1)$	$(a-1)(c-1)^2$
$b_1b_2b_1$	$\alpha_1^2\beta_1$	$2\alpha_1\alpha_2\beta_1+\alpha_1^2\beta_2$	$-2\alpha_1\alpha_2\beta_1-\alpha_1^2\beta_2$	$2\alpha_1\alpha_2\beta_2+\alpha_2^2\beta_1$
$b_1b_2^2$	$\alpha_1\beta_1^2$	$2\alpha_1\beta_1\beta_2+\alpha_2\beta_1^2$	$-2\alpha_2\beta_1^2-\alpha_1\beta_1\beta_2$	$2\alpha_2\beta_1\beta_2+\alpha_1\beta_2^2$
$b_2b_1^2$	$\alpha_1^2\beta_1$	$2\alpha_1\alpha_2\beta_2+\alpha_2^2\beta_1$	$-2\alpha_1^2\beta_2-\alpha_1\alpha_2\beta_1$	$2\alpha_1\alpha_2\beta_2+\alpha_2^2\beta_1$
$b_2b_1b_2$	$\alpha_1\beta_1^2$	$2\alpha_1\beta_1\beta_2+\alpha_2\beta_1^2$	$-2\alpha_1\beta_1\beta_2-\alpha_2\beta_1^2$	$2\alpha_2\beta_1\beta_2+\alpha_1\beta_2^2$
b_1^3	α_1^3	$3\alpha_1^2\alpha_2$	$-3\alpha_1^2\alpha_2$	$3\alpha_1\alpha_2^2$
$b_1^2b_2$	$\alpha_1^2\beta_1$	$2\alpha_1\alpha_2\beta_1+\alpha_1^2\beta_2$	$-3\alpha_1\alpha_2\beta_1$	$2\alpha_1\alpha_2\beta_2+\alpha_2^2\beta_1$
$b_2^2b_1$	$\alpha_1\beta_1^2$	$2\alpha_1\beta_1\beta_2+\alpha_2\beta_1^2$	$-3\alpha_1\beta_1\beta_2$	$2\alpha_2\beta_1\beta_2+\alpha_1\beta_2^2$
b_2^3	β_1^3	$3\beta_1^2\beta_2$	$-3\beta_1^2\beta_2$	$3\beta_1\beta_2^2$

	$(c-1)(d-1)$	$(f-1)$	$(c-1)^3$
$b_1b_2b_1$	$-2\alpha_1\alpha_2\beta_2-\alpha_2^2\beta_1$	$-\alpha_2^2\beta_1-\alpha_1\alpha_2\beta_2$	$\alpha_2^2\beta_2$
$b_1b_2^2$	$-3\alpha_2\beta_1\beta_2$	$-2\alpha_2\beta_1\beta_2$	$\alpha_2\beta_2^2$
$b_2b_1^2$	$-3\alpha_1\alpha_2\beta_2$	$-2\alpha_1\alpha_2\beta_2$	$\alpha_2^2\beta_2$
$b_2b_1b_2$	$-2\alpha_2\beta_1\beta_2-\alpha_1\beta_2^2$	$-\alpha_1\beta_2^2-\alpha_2\beta_1\beta_2$	$\alpha_2\beta_2^2$
b_1^3	$-3\alpha_1\alpha_2^2$	$-2\alpha_1\alpha_2^2$	α_2^3
$b_1^2b_2$	$-2\alpha_2^2\beta_1-\alpha_1\alpha_2\beta_2$	$-\alpha_1\alpha_2\beta_2-\alpha_2^2\beta_1$	$\alpha_2^2\beta_2$
$b_2^2b_1$	$-2\alpha_1\beta_2^2-\alpha_2\beta_1\beta_2$	$-\alpha_2\beta_1\beta_2-\alpha_1\beta_2^2$	$\alpha_2\beta_2^2$
b_2^3	$-3\beta_2\beta_2^2$	$-2\beta_1\beta_2^2$	β_2^3

We have obtained 8 elements, but the $\mathbb{F}$-dimension of the factor algebra $A^3(\mathbb{F}G)/A^4(\mathbb{F}G)$ equals 7. From (4.2) the determinant Δ is equal to $\begin{pmatrix}\alpha_1 & \alpha_2\\ \beta_1 & \beta_2\end{pmatrix}$. Since $\Delta\neq 0$, we see that one of these products $b_{i_1}b_{i_2}b_{i_3}$ either equals zero modulo the ideal $A^4(\mathbb{F}G)$ or coincides with another one.

It is easy to see that none of the lines is equal to zero. Indeed, for example, if $b_1b_2b_1\equiv 0 \pmod{A^4(\mathbb{F}G)}$ then from the second column of the first part and the fourth column of the second part of the table we get that $\alpha_1^2\beta_1=0$ and $\alpha_2^2\beta_2=0$. Since $\Delta\neq 0$, this case is impossible by the third and fifth column of the first part of this table. In a similar manner we can prove this statement for all lines.

If we assume that two of the lines are equal then we also get a contradiction. For instance, if $b_1b_2b_1\equiv b_1b_2^2 \pmod{A^4(\mathbb{F}G)}$ then from

the second column of the first part and the fourth column of the second part of the table it follows that

$$\alpha_1\beta_1(\alpha_1-\beta_1)=0 \quad \text{and} \quad \alpha_2\beta_2(\alpha_2-\beta_2)=0.$$

Since $\Delta\neq 0$, the third column of the first part of the table leads to a contradiction.

Similar calculations for any two lines also lead to a contradiction, so we have got that $\mathbb{F}G$ has no filtered multiplicative basis.

Case 2. Let $G=H_2$. Using (4.3) let us compute $b_{i_1}b_{i_2}$ modulo $A^3(\mathbb{F}G)$ where $(i_k=1,2,3)$. The result of our computations will be written in the following table, consisting of the coefficients of the decomposition $b_{i_1}b_{i_2}$ with respect to the basis

$$\Big\{\ (a-1)^{j_1}(c-1)^{j_2}(h-1)^{j_3}(d-1)^{j_4}\ \Big|\ j_1+j_2+j_3+2j_4=2;\\ j_1,j_2,j_3=0,1,2;\ j_4=0,1\ \Big\}$$

of the ideal $A^2(\mathbb{F}G)/A^3(\mathbb{F}G)$:

	$(a-1)^2$	$(a-1)(c-1)$	$(a-1)(h-1)$	$(c-1)^2$	$(c-1)(h-1)$	$(h-1)^2$	$(d-1)$
b_1b_2	$\alpha_1\beta_1$	$\alpha_1\beta_2+\alpha_2\beta_1$	$\alpha_1\beta_3+\alpha_3\beta_1$	$\alpha_2\beta_2$	$\alpha_2\beta_3+\alpha_3\beta_2$	$\alpha_3\beta_3$	$-\alpha_2\beta_1$
b_2b_1	$\alpha_1\beta_1$	$\alpha_1\beta_2+\alpha_2\beta_1$	$\alpha_1\beta_3+\alpha_3\beta_1$	$\alpha_2\beta_2$	$\alpha_2\beta_3+\alpha_3\beta_2$	$\alpha_3\beta_3$	$-\alpha_1\beta_2$
b_1b_3	$\gamma_1\alpha_1$	$\alpha_1\gamma_2+\alpha_2\gamma_1$	$\alpha_1\gamma_3+\alpha_3\gamma_1$	$\alpha_2\gamma_2$	$\alpha_2\gamma_3+\alpha_3\gamma_2$	$\alpha_3\gamma_3$	$-\alpha_2\gamma_1$
b_3b_1	$\gamma_1\alpha_1$	$\alpha_1\gamma_2+\alpha_2\gamma_1$	$\alpha_1\gamma_3+\alpha_3\gamma_1$	$\alpha_2\gamma_2$	$\alpha_2\gamma_3+\alpha_3\gamma_2$	$\alpha_3\gamma_3$	$-\alpha_1\gamma_2$
b_2b_3	$\beta_1\gamma_1$	$\beta_1\gamma_2+\beta_2\gamma_1$	$\beta_1\gamma_3+\beta_3\gamma_1$	$\beta_2\gamma_2$	$\beta_2\gamma_3+\beta_3\gamma_2$	$\beta_3\gamma_3$	$-\beta_2\gamma_1$
b_3b_2	$\beta_1\gamma_1$	$\beta_1\gamma_2+\beta_2\gamma_1$	$\beta_1\gamma_3+\beta_3\gamma_1$	$\beta_2\gamma_2$	$\beta_2\gamma_3+\beta_3\gamma_2$	$\beta_3\gamma_3$	$-\beta_1\gamma_2$
b_1^2	α_1^2	$2\alpha_1\alpha_2$	$2\alpha_1\alpha_3$	α_2^2	$2\alpha_2\alpha_3$	α_3^2	$-\alpha_1\alpha_2$
b_2^2	β_1^2	$2\beta_1\beta_2$	$2\beta_1\beta_3$	β_2^2	$2\beta_2\beta_3$	β_3^2	$-\beta_1\beta_2$
b_3^2	γ_1^2	$2\gamma_1\gamma_2$	$2\gamma_1\gamma_3$	γ_2^2	$2\gamma_2\gamma_3$	γ_3^2	$-\gamma_1\gamma_2$

We have obtained 9 elements, but the $\mathbb{F}$-dimension of factor algebra $A^2(\mathbb{F}G)/A^3(\mathbb{F}G)$ equals 7, so we conclude that some lines of the table either are equal to zero modulo the ideal $A^3(\mathbb{F}G)$ or coincide with some other lines.

Denote the determinant of the coefficients of b_i $(i=1,2,3)$ by Δ as in (4.1). Since $\Delta\neq 0$, simple computations show that

$$b_i^2\not\equiv 0 \pmod{A^3(\mathbb{F}G)} \quad \text{and} \quad b_ib_j\not\equiv 0 \pmod{A^3(\mathbb{F}G)}.$$

According to the last three lines of the table, if $b_i^2\equiv b_j^2 \pmod{A^3(\mathbb{F}G)}$ then either $b_i\equiv b_j \pmod{A^3(\mathbb{F}G)}$ or $b_i\equiv -b_j \pmod{A^3(\mathbb{F}G)}$, so we have that

$$b_1b_2\equiv b_2b_1 \pmod{A^3(\mathbb{F}G)}, \qquad b_1b_3\equiv b_3b_1 \pmod{A^3(\mathbb{F}G)},$$

$$b_2b_3 \not\equiv b_3b_2 \pmod{A^3(\mathbb{F}G)},$$

because the other cases are symmetric to this one.

Simple computations show that if either $\alpha_1 \neq 0$ or $\beta_1 \neq 0$ then $\mathbb{F}G$ is a commutative algebra which is a contradiction, so we can assume that $\alpha_1 = \beta_1 = 0$. From the 8th column we have $\alpha_2\gamma_1 = 0$. Since $\Delta \neq 0$ we conclude that $\alpha_2 = 0$ and we have the following basis of $A(\mathbb{F}G)/A^2(\mathbb{F}G)$:

$$\begin{cases} b_1 \equiv (h-1) \pmod{A^2(\mathbb{F}G)}; \\ b_2 \equiv (c-1) + \beta_3(h-1) \pmod{A^2(\mathbb{F}G)}; \\ b_3 \equiv (a-1) + \gamma_2(c-1) + \gamma_3(h-1) \pmod{A^2(\mathbb{F}G)}. \end{cases}$$

Let us compute $b_{i_1}b_{i_2}b_{i_3}$ modulo $A^4(\mathbb{F}G)$ where $i_k = 1, 2, 3$ with respect to the basis

$$\left\{ (a-1)^{j_1}(c-1)^{j_2}(h-1)^{j_3}(d-1)^{j_4} \;\middle|\; \begin{array}{r} j_1 + j_2 + j_3 + 2j_4 = 3; \\ j_1, j_2, j_3 = 0, 1, 2, 3;\ j_4 = 0, 1 \end{array} \right\}$$

of the ideal $A^3(\mathbb{F}G)/A^4(\mathbb{F}G)$.

Assume that $p = 3$. Since the dimension of $A^3(\mathbb{F}G)/A^4(\mathbb{F}G)$ is 10, we conclude that

$$b_1^2b_2 \equiv b_1b_2^2, \qquad b_2^2b_3 \equiv b_3b_2^2, \qquad b_3^2b_2 \equiv b_3b_2b_3, \qquad b_1^3 \equiv 0, \qquad b_2^3 \equiv 0$$

modulo $A^4(\mathbb{F}G)$. These congruences give that $\beta_3 = \gamma_2 = \gamma_3 = 0$.

Now suppose that $p > 3$. In this case the dimension of the factor algebra $A^3(\mathbb{F}G)/A^4(\mathbb{F}G)$ is 15, so we conclude that

$$b_1^2b_2 \equiv b_1b_2^2 \pmod{A^4(\mathbb{F}G)}, \quad b_3^2b_2 \equiv b_3b_2b_3 \pmod{A^4(\mathbb{F}G)},$$

and we also get that $\beta_3 = \gamma_2 = \gamma_3 = 0$.

Assume that $\mathbb{F}G$ has a filtered multiplicative $\mathbb{F}$-basis. With respect to the equation $\mathbb{F}G = \mathbb{F}[G_1 \times G_2]$, where $G_1 = \langle\ h \mid h^p = 1\ \rangle$ and

$$G_2 = \langle\ a, c \mid a^p = c^p = 1,\ (a, c) = d, (c, d) = (a, d) = 1\ \rangle,$$

we have established that

$$\begin{cases} b_1 \equiv (h-1) \pmod{A^2(\mathbb{F}G)}; \\ b_2 \equiv (c-1) \pmod{A^2(\mathbb{F}G)}; \\ b_3 \equiv (a-1) \pmod{A^2(\mathbb{F}G)}, \end{cases}$$

and $b_1 \in FG_1$, $b_2, b_3 \in FG_2$, we conclude that $\mathbb{F}G_2$ also has a filtered multiplicative $\mathbb{F}$-basis, which is a contradiction by second part of Proposition 4.1.5.

If G is a group of order p^3 $(p \neq 2)$ then also by Proposition 4.1.5 the group algebra $\mathbb{F}G$ has no filtered multiplicative $\mathbb{F}$-basis. Let $\mathbb{F}$ be a field of characteristic 2. If $\left|G\right| \leq 2^4$ then $\mathbb{F}G$ has a filtered multiplicative basis if and only if G and $\mathbb{F}$ satisfy the conditions of Proposition 4.1.6 and 4.1.7, so the proof of the theorem is complete.

□

In the following we investigate the existence of filtered multiplicative $\mathbb{F}$-basis of algebras $\mathbb{F}G$, where G is a nonabelian 2-groups.

Theorem 4.3.2. *Let $\mathbb{F}$ be a field of characteristic 2 and*

$$G = \langle\ a, b \mid a^{2^n} = b^{2^m} = c^2 = 1,\ (a,b) = c,\ (a,c) = 1,\ (b,c) = 1\ \rangle,$$

with $n, m \geq 2$. Then $\mathbb{F}G$ possesses a filtered multiplicative $\mathbb{F}$-basis.

Proof. Let G be the group as in this Theorem and put

$$b_1^1 = u \equiv (1+a) \pmod{A^2(\mathbb{F}G)},\ b_1^2 = v \equiv (1+b) \pmod{A^2(\mathbb{F}G)}.$$

Using the identity

$$(1+b)(1+a) \equiv (1+a)(1+b) + (1+c) \pmod{A^3(\mathbb{F}G)},$$

we get that the elements

$$\begin{aligned} b_2^1 &= uv \equiv (1+a)(1+b) \pmod{A^3(\mathbb{F}G)}, \\ b_2^2 &= vu \equiv (1+a)(1+b) + (1+c) \pmod{A^3(\mathbb{F}G)}, \\ b_2^3 &= u^2 \equiv (1+a)^2 \pmod{A^3(\mathbb{F}G)}, \\ b_2^4 &= v^2 \equiv (1+b)^2 \pmod{A^3(\mathbb{F}G)} \end{aligned}$$

form a basis of $A^2(\mathbb{F}G)/A^3(\mathbb{F}G)$ and

$$\begin{aligned}
b_3^1 &= uvu \equiv (1+a)^2(1+b) + (1+a)(1+c) \pmod{A^4(\mathbb{F}G)},\\
b_3^2 &= u^2v \equiv (1+a)^2(1+b) \pmod{A^4(\mathbb{F}G)},\\
b_3^3 &= u^3 \equiv (1+a)^3 \pmod{A^4(\mathbb{F}G)},\\
b_3^4 &= uv^2 \equiv (1+a)(1+b)^2 \pmod{A^4(\mathbb{F}G)},\\
b_3^5 &= vuv \equiv (1+a)(1+b)^2 + (1+b)(1+c) \pmod{A^4(\mathbb{F}G)},\\
b_3^6 &= v^3 \equiv (1+b)^3 \pmod{A^4(\mathbb{F}G)}
\end{aligned}$$

is a basis for $A^3(\mathbb{F}G)/A^4(\mathbb{F}G)$. Let Δ_i be the determinant, consisting of the coefficients of b_i^k $(k = 1, \cdots, n_i)$, where the elements b_i^k form a basis of $A^i(\mathbb{F}G)/A^{i+1}(\mathbb{F}G)$. We shall create an $\mathbb{F}$-basis of $A^i(\mathbb{F}G)/A^{i+1}(\mathbb{F}G)$ by induction. Evidently, b_1^1, b_1^2 is a basis of $A(\mathbb{F}G)/A^2(\mathbb{F}G)$. Assume that

$$b_{i-1}^1,\ b_{i-1}^2, \ldots,\ b_{i-1}^{n-1},\ b_{i-1}^n$$

is a basis for $A^{i-1}(\mathbb{F}G)/A^i(\mathbb{F}G)$. Evidently, the determinant of this basis Δ_{i-1} is not zero. Simple computations show that the determinant Δ_i of the elements

$$b_1^1 b_{i-1}^1,\ b_1^1 b_{i-1}^2,\ \cdots,\ b_1^1 b_{i-1}^{n-1},\ b_1^1 b_{i-1}^n,\ b_{i-1}^{n-1} b_1^2,\ b_{i-1}^n b_1^2$$

is equal to $\Delta_{i-1} \cdot \left|\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right| \neq 0$, so we have got $n+2$ linearly independent elements. Since $dim\,[A^i(\mathbb{F}G)/A^{i+1}(\mathbb{F}G)]$ is also $n+2$ we have obtained that $\mathbb{F}G$ has a filtered multiplicative $\mathbb{F}$-basis.

□

Theorem 4.3.3. *Let G be the following group*

$$\begin{aligned}
G = \langle\ a, b\ \mid\ a^{2^n} = b^2 = &c^2 = d^2 = 1,\ (a,b) = c,\ (a,c) = d,\\
&(a,d) = (b,c) = (b,d) = (c,d) = 1\ \rangle
\end{aligned}$$

with $n > 1$ and $\mathbb{F}$ a field of characteristic 2. Then $\mathbb{F}G$ has no filtered multiplicative $\mathbb{F}$-basis.

Proof. Let G be the group as in this Theorem. Let us compute the *Lazard-Jennings series* of this group:

$$M_1(G) = G, \quad M_2(G) = \langle a^2, c, d\rangle, \quad M_3(G) = \langle d\rangle, \quad M_4(G) = \langle 1\rangle.$$

We conclude that $\mu(c) = 2$ and $\mu(d) = 3$.

Let

$$b_1 \equiv \alpha_1(1+a) + \alpha_2(1+b) \pmod{A^2(\mathbb{F}G)}$$

and

$$b_2 \equiv \beta_1(1+a) + \beta_2(1+b) \pmod{A^2(\mathbb{F}G)}$$

as in (4.1). Using the identity

$$(1+b)(1+a) \equiv (1+a)(1+b) + (1+c) \pmod{A^3(\mathbb{F}G)}, \tag{4.4}$$

it follows that

$$\begin{cases} b_1b_2 \equiv \alpha_1\beta_1(1+a)^2 + (\alpha_1\beta_2+\alpha_2\beta_1)(1+a)(1+b) + \alpha_2\beta_1(1+c) \pmod{A^3(\mathbb{F}G)};\\ b_2b_1 \equiv \alpha_1\beta_1(1+a)^2 + (\alpha_1\beta_2+\alpha_2\beta_1)(1+a)(1+b) + \alpha_1\beta_2(1+c) \pmod{A^3(\mathbb{F}G)};\\ b_1^2 \equiv \alpha_1^2(1+a)^2 + \alpha_1\alpha_2(1+c) \pmod{A^3(\mathbb{F}G)};\\ b_2^2 \equiv \beta_1^2(1+a)^2 + \beta_1\beta_2(1+c) \pmod{A^3(\mathbb{F}G)}. \end{cases}$$

We have obtained 4 elements, but the $\mathbb{F}$-dimension of $A^2(\mathbb{F}G)/A^3(\mathbb{F}G)$ equals 3. Let Δ be the determinant $\begin{pmatrix}\alpha_1 & \alpha_2\\ \beta_2 & \beta_2\end{pmatrix}$. Since $\Delta \neq 0$, we get that $b_1b_2 \not\equiv b_2b_1, b_1^2, b_2^2$ and $b_1b_2,\ b_2b_1 \not\equiv 0$ and $b_1^2 \not\equiv b_2^2 \pmod{A^3(\mathbb{F}G)}$. Thus either $b_1^2 \equiv 0 \pmod{A^3(\mathbb{F}G)}$ or $b_2^2 \equiv 0 \pmod{A^3(\mathbb{F}G)}$. It is easy to see that the second case is symmetric to the first one, so we consider the second one. Let $\beta_1 = 0$ and we can put $\alpha_1 = \beta_2 = 1$ and

$$\begin{aligned} u = b_1 &\equiv (1+a) + \alpha_2(1+b) \pmod{A^2(\mathbb{F}G)};\\ v = b_2 &\equiv (1+b) \pmod{A^2(\mathbb{F}G)}. \end{aligned}$$

Using (4.4) and the identity

$$(1+c)(1+a) \equiv (1+a)(1+c) + (1+d) \pmod{A^4(\mathbb{F}G)},$$

straightforward computations show that

$$\begin{cases} uvu^2 \equiv (1+a)^3(1+b) + \alpha_2(1+a)(1+b)(1+c) \\ \qquad\qquad + (1+a)(1+d) \pmod{A^5(\mathbb{F}G)}; \\ vu^3 \equiv (1+a)^3(1+b) + (1+a)^2(1+c) + \alpha_2(1+a)(1+b)(1+c) \\ \qquad\qquad + (1+a)(1+d) \pmod{A^5(\mathbb{F}G)}; \\ vuvu \equiv (1+b)(1+d) + (1+a)(1+b)(1+c) \pmod{A^5(\mathbb{F}G)}; \\ u^2vu \equiv (1+a)^3(1+b) + (1+a)^2(1+c) + \alpha_2(1+a)(1+b)(1+c) \\ \qquad\qquad + \alpha_2(1+b)(1+d) \pmod{A^5(\mathbb{F}G)}; \\ uvuv \equiv (1+a)(1+b)(1+c) \pmod{A^5(\mathbb{F}G)}; \\ vu^2v \equiv (1+b)(1+d) \pmod{A^5(\mathbb{F}G)}; \\ u^3v \equiv (1+a)^3(1+b) + \alpha_2(1+a)(1+b)(1+c) \\ \qquad\qquad + \alpha_2(1+b)(1+d) \pmod{A^5(\mathbb{F}G)}. \end{cases}$$

We have obtained 7 different elements, but this is a contradiction because $dim[A^4(\mathbb{F}G)/A^5(\mathbb{F}G)] = 5$.

□

Theorem 4.3.4. *Let $\mathbb{F}G$ be the group algebra of a finite nonabelian 2-group G of order 2^5 over a field $\mathbb{F}$ of characteristic 2. Then $\mathbb{F}G$ possesses a filtered multiplicative $\mathbb{F}$-basis if and only if G is one of the following groups:*

1. $G_{18} = D_{32}$, $G_{25} = D_8 \times C_4$, $G_{39} = D_{16} \times C_2$ *or* $G_{46} = D_8 \times C_2 \times C_2$;

2. $G_{26} = Q_8 \times C_4$, *or* $G_{47} = Q_8 \times C_2 \times C_2$ *and* $\mathbb{F}$ *contains a primitive cube root of the unity;*

3. $G_{22} = H_{16} \times C_2$, $G_{48} = (D_8 \curlyvee C_4) \times C_2$;

4. $G_2 = \langle\ a, b \mid a^4 = b^4 = c^2 = 1,\ (a,b) = c,\ (a,c) = 1,\ (b,c) = 1\ \rangle$;

$$
\begin{aligned}
G_5 =& \langle\ a, b\ \mid\ a^8 = b^2 = c^2 = 1,\ (a,b) = c,\ (a,c) = (b,c) = 1\ \rangle;\\
G_7 =& \langle\ a, b, c\mid\ a^8 = b^2 = c^2 = 1,\ (a,c) = a^4,\\
&\qquad\qquad (a,b) = a^4c,\ (b,c) = 1\ \rangle;\\
G_8 =& \langle\ a, b, c\mid\ a^8 = c^2 = 1,\ b^2 = a^4,\ (a,c) = a^4,\\
&\qquad\qquad (a,b) = a^4c,\ (b,c) = 1\ \rangle;\\
G_9 =& \langle\ a, b, c\mid\ a^2 = b^8 = c^2 = 1,\ (b,c) = ab^6,\ (a,c) = (a,b) = 1\ \rangle;\\
G_{10} =& \langle\ a, b, c\mid\ a^8 = b^4 = c^2 = 1,\ a^4 = b^2,\ (a,b) = a^6c,\\
&\qquad\qquad (a,c) = (b,c) = 1\ \rangle;\\
G_{11} =& \langle\ a, b, c\mid\ a^4 = b^4 = c^2 = 1,\ (b,c) = ab^2,\ (a,c) = (a,b) = 1\ \rangle;\\
G_{49} =& \langle\ a, b, c, d\mid a^4 = 1,\ b^2 = c^2 = d^2 = a^2,\ (a,b) = a^2,\ (c,d) = a^2,\\
&\qquad\qquad (a,c) = (a,d) = (b,c) = (b,d) = 1\ \rangle.
\end{aligned}
$$

Proof. Let G be a nonabelian 2-group of order 2^5. If G is one of the groups $\{G_5, G_7, G_8, G_9, G_{10}, G_{11}\}$ then G has a cyclic subgroup of index p^2 and by Proposition 4.1.6 $\mathbb{F}G$ has a filtered multiplicative basis, but if G is one of the following groups:

$$
\begin{aligned}
G_{40} =& SD_{16} \times C_2; \qquad G_{41} = Q_{16} \times C_2;\\
G_{42} =& \langle\ a, b, c\ \mid a^8 = b^4 = c^4 = 1\ \ a^4 = b^2 = c^2,\\
&\qquad\qquad (a,b) = a^6\ \ (a,c) = (b,c) = 1\ \rangle;\\
G_{43} =& \langle\ a, b, c\ \mid a^8 = b^2 = c^2 = 1,\ \ (a,b) = a^6,\ \ (a,c) = a^4,\\
&\qquad\qquad (b,c) = 1\ \rangle;\\
G_{44} =& \langle\ a, b, c\ \mid a^8 = c^2 = 1,\ \ b^2 = a^4,\ \ (a,c) = a^4,\\
&\qquad\qquad (a,b) = a^6,\ \ (b,c) = 1\ \rangle
\end{aligned}
$$

then $\mathbb{F}G$ has no filtered multiplicative $\mathbb{F}$-basis.

If G is one of the following groups:

$$
\begin{aligned}
G_4 =& \langle\ a, b\ \mid\ a^8 = b^4 = 1,\ \ (a,b) = a^4\ \rangle;\\
G_{37} =& MD_{16} \times C_2;\\
G_{38} =& \langle\ a, b, c\ \mid\ a^8 = b^2 = c^2 = 1,\ \ (b,c) = a^4,\\
&\qquad\qquad (a,b) = (a,c) = 1\ \rangle
\end{aligned}
$$

then they are powerful groups and by Proposition 4.1.5 $\mathbb{F}G$ has no filtered multiplicative $\mathbb{F}$-basis. If G is one of the following groups:

$$\begin{aligned}
G_{12} =& \langle\ a, b \mid a^4 = b^8 = 1,\ (a,b) = a^2\ \rangle;\\
G_{13} =& \langle\ a, b \mid a^8 = b^4 = 1,\ (a,b) = a^2\ \rangle;\\
G_{14} =& \langle\ a, b \mid a^8 = b^4 = 1,\ (a,b) = a^6\ \rangle;\\
G_{15} =& \langle\ a, b \mid a^8 = 1,\ b^4 = a^4,\ (a,b) = a^6\ \rangle;\\
G_{17} =& MD_{32},\ G_{18} = D_{32},\ G_{19} = SD_{32},\ G_{20} = Q_{32}
\end{aligned}$$

then G is metacyclic, so by Proposition 4.1.4 $\mathbb{F}G$ has a filtered multiplicative $\mathbb{F}$-basis if and only if $G = G_{18}$.

According to Propositions 4.1.5, 4.1.6 and 4.1.7 we get that for the following direct products $G_{22} = H_{16} \times C_2$, $G_{25} = D_8 \times C_4$, $G_{26} = Q_8 \times C_4$, $G_{39} = D_{16} \times C_2$, $G_{46} = D_8 \times C_2 \times C_2$, $G_{47} = Q_8 \times C_2 \times C_2$, $G_{48} = (D_8 \curlyvee C_4) \times C_2$ $\mathbb{F}G$ has a filtered multiplicative basis.

For $n = m = 2$ the group in Theorem 4.3.2 is isomorphic to G_2 and so $\mathbb{F}G_2$ has a filtered multiplicative $\mathbb{F}$-basis.

Let G be the group

$$\begin{aligned}
G_6 = \langle\ a, b \mid a^4 = b^2 = 1,\ (a,b) = c,\ (a,c) = d,\\
(a,d) = (b,c) = (b,d) = (c,d) = 1\ \rangle.
\end{aligned}$$

For $n = 2$ the group in Theorem 4.3.3 is isomorphic to G_6, so the group algebra $\mathbb{F}G_6$ has no filtered multiplicative $\mathbb{F}$-basis.

Now we shall consider the following 7 cases.

Case 1. Let G be the group

$$G_{23} = \langle\ a, b, c \mid a^4 = b^4 = c^2 = 1,\ (a,c) = (b,c) = 1,\ (a,b) = a^2\ \rangle.$$

Using the identity

$$(1+b)(1+a) \equiv (1+a)(1+b) + (1+a)^2 \pmod{A^3(\mathbb{F}G)},$$

let us compute $b_{i_1} b_{i_2}$ modulo $A^3(\mathbb{F}G)$, where $(i_k = 1, 2, 3)$. The result of our computation will be written in a table, consisting of the

coefficients of the decomposition $b_{i_1}b_{i_2}$ with respect to the basis

$$\left\{ (1+a)^{j_1}(1+b)^{j_2}(1+c)^{j_3} \;\middle|\; \begin{array}{l} j_1+j_2+j_3=2; \\ j_1,j_2=0,1,2;\ j_3=0,1 \end{array} \right\}$$

of the ideal $A^2(\mathbb{F}G)$.

	$(1+a)^2$	$(1+a)(1+b)$	$(1+a)(1+c)$	$(1+b)(1+c)$	$(1+b)^2$
b_1b_2	$\alpha_1\beta_1+\alpha_2\beta_1$	$\alpha_1\beta_2+\alpha_2\beta_1$	$\alpha_1\beta_3+\alpha_3\beta_1$	$\alpha_2\beta_3+\alpha_3\beta_2$	$\alpha_2\beta_2$
b_2b_1	$\alpha_1\beta_1+\alpha_1\beta_2$	$\alpha_1\beta_2+\alpha_2\beta_1$	$\alpha_1\beta_3+\alpha_3\beta_1$	$\alpha_2\beta_3+\alpha_3\beta_2$	$\alpha_2\beta_2$
b_1b_3	$\alpha_1\gamma_1+\alpha_2\gamma_1$	$\alpha_1\gamma_2+\alpha_2\gamma_1$	$\alpha_1\gamma_3+\alpha_3\gamma_1$	$\alpha_2\gamma_3+\alpha_3\gamma_2$	$\alpha_2\gamma_2$
b_3b_1	$\alpha_1\gamma_1+\alpha_1\gamma_2$	$\alpha_1\gamma_2+\alpha_2\gamma_1$	$\alpha_1\gamma_3+\alpha_3\gamma_1$	$\alpha_2\gamma_3+\alpha_3\gamma_2$	$\alpha_2\gamma_2$
b_2b_3	$\beta_1\gamma_1+\beta_2\gamma_1$	$\beta_1\gamma_2+\beta_2\gamma_1$	$\beta_1\gamma_3+\beta_3\gamma_1$	$\beta_2\gamma_3+\beta_3\gamma_2$	$\beta_2\gamma_2$
b_3b_2	$\beta_1\gamma_1+\beta_1\gamma_2$	$\beta_1\gamma_2+\beta_2\gamma_1$	$\beta_1\gamma_3+\beta_3\gamma_1$	$\beta_2\gamma_3+\beta_3\gamma_2$	$\beta_2\gamma_2$
b_1^2	$\alpha_1^2+\alpha_2\alpha_3$	0	0	0	α_2^2
b_2^2	$\beta_1^2+\beta_2\beta_3$	0	0	0	β_2^2
b_3^2	$\gamma_1^2+\gamma_2\gamma_3$	0	0	0	γ_2^2

Since $\Delta \neq 0$, it is easy to see that the first six lines are not equal to either zero or the last three lines. Remark that the dimension of $A^2(\mathbb{F}G)/A^3(\mathbb{F}G)$ is equal to 5 and $\mathbb{F}G$ is not a commutative algebra. The fact $b_i^2 \equiv b_j^2 \equiv 0 \pmod{A^3(\mathbb{F}G)}$, $i \neq j$ implies that b_i linearly depends on b_j, so we shall consider two interesting cases.

In the first case $b_1^2 \equiv 0 \pmod{A^3(\mathbb{F}G)}$, $b_2^2 \equiv b_3^2 \not\equiv 0 \pmod{A^3(\mathbb{F}G)}$ and we get that $b_1 \equiv \alpha_3(1+c) \pmod{A^2(\mathbb{F}G)}$ and by Proposition 4.1.2 $b_2^2 = b_3^2$. From the condition $b_2^2 \equiv b_3^2 \pmod{A^3(\mathbb{F}G)}$ we have that

$$\beta_2 = \gamma_2 \neq 0 \qquad \text{and} \qquad (\beta_1+\gamma_1)(\beta_1+\gamma_1+\gamma_2) = 0.$$

Since $\Delta \neq 0$ so $\beta_1 = \gamma_1 + \gamma_2$ and we conclude that

$$b_2 = (\lambda+1)(1+a) + (1+b) + \mu(1+c)$$

and

$$b_3 = \lambda(1+a) + (1+b) + \eta(1+c),$$

where $\lambda = \frac{\gamma_1}{\gamma_2}$, $\mu = \frac{\beta_3}{\gamma_2}$ and $\eta = \frac{\gamma_3}{\gamma_2}$. The fact $b_2^2 = b_3^2$ gives that

$$1 + a^2 + ab + a^3b = 0,$$

which is impossible.

In the second case $b_1^2 \equiv b_2^2 \equiv b_3^2 \not\equiv 0 \pmod{A^3(\mathbb{F}G)}$ and we can assume that

$$b_1b_2 \equiv b_2b_1 \pmod{A^3(\mathbb{F}G)}, \qquad b_1b_3 \equiv b_3b_1 \pmod{A^3(\mathbb{F}G)},$$

$$b_3b_2 \not\equiv b_2b_3 \pmod{A^3(\mathbb{F}G)}.$$

Since $b_1b_2 \equiv b_2b_1 \pmod{A^3(\mathbb{F}G)}$ and $b_1b_3 \equiv b_3b_1 \pmod{A^3(\mathbb{F}G)}$ we have that $\alpha_2\beta_1 = \alpha_1\beta_2$ and $\alpha_2\gamma_1 = \alpha_1\gamma_2$. From the fact that

$$b_1^2 \equiv b_2^2 \equiv b_3^2 \not\equiv 0 \pmod{A^3(\mathbb{F}G)}$$

the sixth column asserts that $\alpha_2 = \beta_2 = \gamma_2$ and the second column yields $\alpha_1 = \beta_1 = \gamma_1$, so we conclude that $b_3b_2 \equiv b_2b_3 \pmod{A^3(\mathbb{F}G)}$, which is a contradiction. These facts give that $\mathbb{F}G$ has no filtered multiplicative $\mathbb{F}$-basis.

Case 2. Let G be the group

$$G_{24} = \langle\ a, b, c \mid a^4 = b^4 = c^2 = 1,\ (a,b) = (a,c) = 1,\ (b,c) = a^2\ \rangle.$$

Using the identity

$$(1+c)(1+b) \equiv (1+b)(1+c) + (1+a)^2 \qquad \pmod{A^3(\mathbb{F}G)},$$

let us compute $b_{i_1}b_{i_2}$ modulo $A^3(\mathbb{F}G)$, where $(i_k = 1,2,3)$. The result of our computation will be written in a table, consisting of the coefficients of the decomposition $b_{i_1}b_{i_2}$ with respect to the basis

$$\Big\{\ (1+a)^{j_1}(1+b)^{j_2}(1+c)^{j_3} \ \Big|\ j_1+j_2+j_3 = 2; \quad j_1, j_2 = 0,1,2;\ j_3 = 0,1\ \Big\}$$

of the ideal $A^2(\mathbb{F}G)$.

	$(1+a)^2$	$(1+a)(1+b)$	$(1+a)(1+c)$	$(1+b)(1+c)$	$(1+b)^2$
b_1b_2	$\alpha_1\beta_1 + \alpha_3\beta_2$	$\alpha_1\beta_2 + \alpha_2\beta_1$	$\alpha_1\beta_3 + \alpha_3\beta_1$	$\alpha_2\beta_3 + \alpha_3\beta_2$	$\alpha_2\beta_2$
b_2b_1	$\alpha_1\beta_1 + \alpha_2\beta_3$	$\alpha_1\beta_2 + \alpha_2\beta_1$	$\alpha_1\beta_3 + \alpha_3\beta_1$	$\alpha_2\beta_3 + \alpha_3\beta_2$	$\alpha_2\beta_2$
b_1b_3	$\alpha_1\gamma_1 + \alpha_3\gamma_2$	$\alpha_1\gamma_2 + \alpha_2\gamma_1$	$\alpha_1\gamma_3 + \alpha_3\gamma_1$	$\alpha_2\gamma_3 + \alpha_3\gamma_2$	$\alpha_2\gamma_2$
b_3b_1	$\alpha_1\gamma_1 + \alpha_2\gamma_3$	$\alpha_1\gamma_2 + \alpha_2\gamma_1$	$\alpha_1\gamma_3 + \alpha_3\gamma_1$	$\alpha_2\gamma_3 + \alpha_3\gamma_2$	$\alpha_2\gamma_2$
b_2b_3	$\beta_1\gamma_1 + \beta_3\gamma_2$	$\beta_1\gamma_2 + \beta_2\gamma_1$	$\beta_1\gamma_3 + \beta_3\gamma_1$	$\beta_2\gamma_3 + \beta_3\gamma_2$	$\beta_2\gamma_2$
b_3b_2	$\beta_1\gamma_1 + \beta_2\gamma_3$	$\beta_1\gamma_2 + \beta_2\gamma_1$	$\beta_1\gamma_3 + \beta_3\gamma_1$	$\beta_2\gamma_3 + \beta_3\gamma_2$	$\beta_2\gamma_2$
b_1^2	$\alpha_1^2 + \alpha_2\alpha_3$	0	0	0	α_2^2
b_2^2	$\beta_1^2 + \beta_2\beta_3$	0	0	0	β_2^2
b_3^2	$\gamma_1^2 + \gamma_2\gamma_3$	0	0	0	γ_2^2

It is easy to see that the first six lines are not equal to either zero or the last three lines. Since the dimension of $A^2(\mathbb{F}G)/A^3(\mathbb{F}G)$ equals 5 and $\mathbb{F}G$ is not commutative, we have either

$$b_1b_2 \equiv b_2b_1, \qquad b_1b_3 \not\equiv b_3b_1, \qquad b_2b_3 \not\equiv b_3b_2$$

or

$$b_1b_2 \equiv b_2b_1, \qquad b_1b_3 \equiv b_3b_1, \qquad b_2b_3 \not\equiv b_3b_2$$

by modulo $A^3(\mathbb{F}G)$, because the other cases are symmetric to these.

In the first case we get that $b_1^2 \equiv b_2^2 \equiv b_3^2 \equiv 0 \pmod{A^3(\mathbb{F}G)}$, so $\Delta = 0$, where Δ is as in (4.1), which is impossible. In the second case consider the following subcases:

1. $b_1^2 \equiv b_2^2 \equiv b_3^2 \not\equiv 0 \pmod{A^3(\mathbb{F}G)}$;
2. $b_i^2 \equiv b_j^2 \equiv 0$ and $b_k^2 \not\equiv 0 \pmod{A^3(\mathbb{F}G)}$;
3. $b_i^2 \equiv b_j^2 \not\equiv 0$ and $b_k^2 \equiv 0 \pmod{A^3(\mathbb{F}G)}$.

Since $\Delta \neq 0$ the subcase 1 is impossible. Consider the subcase 2 and for example put $b_1^2 \equiv b_2^2 \equiv 0 \pmod{A^3(\mathbb{F}G)}$ and $b_3^2 \not\equiv 0 \pmod{A^3(\mathbb{F}G)}$. We get that $\alpha_2 = \beta_2 = 0$ and $\alpha_1 = \beta_1 = 0$ by the second and sixth columns, so $\Delta = 0$, which is a contradiction. The other cases also lead to a contradiction.

In the final case we assume that $b_i^2 \equiv b_j^2 \not\equiv 0 \pmod{A^3(\mathbb{F}G)}$ and $b_k^2 \equiv 0 \pmod{A^3(\mathbb{F}G)}$, for instance $b_1^2 \equiv b_2^2 \not\equiv 0 \pmod{A^3(\mathbb{F}G)}$ and $b_3^2 \equiv 0 \pmod{A^3(\mathbb{F}G)}$. According to the second and sixth columns

$$\alpha_2 = \beta_2 \neq 0 \qquad \text{and} \qquad (\alpha_1 + \beta_1)^2 = \alpha_2(\alpha_3 + \beta_3).$$

Since $b_1b_2 \equiv b_2b_1$, the second column gives that $\alpha_3\beta_2 = \alpha_2\beta_3$, so $\Delta = 0$ which is a contradiction. Thus $\mathbb{F}G$ has no filtered multiplicative basis.

Case 3. Let

$$\begin{aligned} G = G_{27} = \langle\ a, b, c \mid\ & a^2 = b^2 = c^2 = 1,\ \ (a,c) = d,\ \ (b,c) = e, \\ & (a,b) = (a,d) = (a,e) = (b,d) = 1, \\ & (b,e) = (c,d) = (c,e) = (d,e) = 1\ \rangle. \end{aligned}$$

Since

$$M_1(G) = G, \quad M_2(G) = \langle d,\ e\rangle, \ \ M_3(G) = \langle 1\rangle$$

we obtain that $\mu(d) = \mu(e) = 2$. Let us compute $b_{i_1}b_{i_2}$ modulo $A^3(\mathbb{F}G)$, where $(i_k = 1, 2, 3)$. The result of our computation will again be written in a table, consisting of the coefficients of the decomposition $b_{i_1}b_{i_2}$ with respect to the basis

$$\Big\{\ (1+a)^{j_1}(1+b)^{j_2}(1+c)^{j_3}(1+d)^{j_4}(1+e)^{j_5} \ \Big|\ j_1+j_2+j_3+2j_4 + 2j_5 = 2,\ \ j_1, j_2, j_3 = 0, 1;\ j_4, j_5 = 0, 1\ \Big\}$$

of the ideal $A^2(\mathbb{F}G)$. Using the identities:

$$(1+c)(1+a) \equiv (1+a)(1+c) + (1+d) \pmod{A^3(\mathbb{F}G)};$$
$$(1+c)(1+b) \equiv (1+b)(1+c) + (1+e) \pmod{A^3(\mathbb{F}G)},$$

we have

	$(1+a)(1+b)$	$(1+a)(1+c)$	$(1+b)(1+c)$	$(1+d)$	$(1+e)$
b_1b_2	$\alpha_1\beta_2+\alpha_2\beta_1$	$\alpha_1\beta_3+\alpha_3\beta_1$	$\alpha_2\beta_3+\alpha_3\beta_2$	$\alpha_3\beta_1$	$\alpha_3\beta_2$
b_2b_1	$\alpha_1\beta_2+\alpha_2\beta_1$	$\alpha_1\beta_3+\alpha_3\beta_1$	$\alpha_2\beta_3+\alpha_3\beta_2$	$\alpha_1\beta_3$	$\alpha_2\beta_3$
b_1b_3	$\alpha_1\gamma_2+\alpha_2\gamma_1$	$\alpha_1\gamma_3+\alpha_3\gamma_1$	$\alpha_2\gamma_3+\alpha_3\gamma_2$	$\alpha_3\gamma_1$	$\alpha_3\gamma_2$
b_3b_1	$\alpha_1\gamma_2+\alpha_2\gamma_1$	$\alpha_1\gamma_3+\alpha_3\gamma_1$	$\alpha_2\gamma_3+\alpha_3\gamma_2$	$\alpha_1\gamma_3$	$\alpha_2\gamma_3$
b_2b_3	$\beta_1\gamma_2+\beta_2\gamma_1$	$\beta_1\gamma_3+\beta_3\gamma_1$	$\beta_2\gamma_3+\beta_3\gamma_2$	$\beta_3\gamma_1$	$\beta_3\gamma_2$
b_3b_2	$\beta_1\gamma_2+\beta_2\gamma_1$	$\beta_1\gamma_3+\beta_3\gamma_1$	$\beta_2\gamma_3+\beta_3\gamma_2$	$\beta_1\gamma_3$	$\beta_2\gamma_3$
b_1^2	0	0	0	$\alpha_1\alpha_3$	$\alpha_2\alpha_3$
b_2^2	0	0	0	$\beta_1\beta_3$	$\beta_2\beta_3$
b_3^2	0	0	0	$\gamma_1\gamma_3$	$\gamma_2\gamma_3$

It is easy to see that the first six lines are not equal to either zero or the last three lines. Since the dimension of $A^2(\mathbb{F}G)/A^3(\mathbb{F}G)$ equals 5 and $\mathbb{F}G$ is not commutative, we have by modulo $A^3(\mathbb{F}G)$ either

$$b_1b_2 \equiv b_2b_1, \qquad b_1b_3 \not\equiv b_3b_1, \qquad b_2b_3 \not\equiv b_3b_2$$

or

$$b_1b_2 \equiv b_2b_1, \qquad b_1b_3 \equiv b_3b_1, \qquad b_2b_3 \not\equiv b_3b_2,$$

because the other cases are symmetric to these.

In the first case we get that $b_1^2 \equiv b_2^2 \equiv b_3^2 \equiv 0 \pmod{A^3(\mathbb{F}G)}$ and

$$\alpha_3 = \beta_3 = \gamma_1 = \gamma_2 = 0.$$

Let us compute $b_{i_1}b_{i_2}b_{i_3}$ modulo $A^4(\mathbb{F}G)$, where $(i_k = 1, 2, 3)$. Since the dimension of $A^3(\mathbb{F}G)/A^4(\mathbb{F}G)$ is equal to 7 but we have got 8 different elements this case is impossible. In the second case

$$b_1b_2 \equiv b_2b_1 \pmod{A^3(\mathbb{F}G)} \quad \text{and} \quad b_1b_3 \equiv b_3b_1 \pmod{A^3(\mathbb{F}G)}.$$

Assume that α_3 is equal to zero. The fifth and sixth columns implies that $\beta_3 = \gamma_3 = 0$ which is impossible, so $\alpha_3, \beta_3, \gamma_3 \neq 0$. These columns give that $b_2 \equiv \beta_3\alpha_3^{-1}b_1 \pmod{A^2(\mathbb{F}G)}$ which is a contradiction, therefore $\mathbb{F}G$ has no filtered multiplicative $\mathbb{F}$-basis.

Case 4. Let G be one of the following groups:

$$\begin{aligned}
G_{28} =\langle\ a, b, c \mid\ & a^4 = b^2 = c^2 = 1,\ (a, c) = a^2,\ (b, c) = d, \\
& (a, b) = (a, d) = (b, d) = (c, d) = 1\ \rangle; \\
G_{29} =\langle\ a, b, c \mid\ & a^4 = b^2 = 1,\ a^2 = c^2,\ (a, c) = a^2,\ (b, c) = d, \\
& (a, b) = (a, d) = (b, d) = (c, d) = 1\ \rangle; \\
G_{30} =\langle\ a, b, c \mid\ & a^4 = b^2 = c^2 = 1,\ (a, c) = d,\ (b, c) = a^2, \\
& (a, b) = (a, d) = (b, d) = (c, d) = 1\ \rangle.
\end{aligned}$$

If G is either G_{28} or G_{29} then we have

$$\begin{aligned}
(1 + c)(1 + a) &\equiv (1 + a)(1 + c) + (1 + a)^2 \pmod{A^3(\mathbb{F}G)}; \\
(1 + c)(1 + b) &\equiv (1 + b)(1 + c) + (1 + d) \pmod{A^3(\mathbb{F}G)}.
\end{aligned}$$

If $G = G_{30}$ then

$$\begin{aligned}
(1 + c)(1 + a) &\equiv (1 + a)(1 + c) + (1 + d) \pmod{A^3(\mathbb{F}G)}; \\
(1 + c)(1 + b) &\equiv (1 + b)(1 + c) + (1 + a)^2 \pmod{A^3(\mathbb{F}G)}.
\end{aligned}$$

Using the last four identities let us compute $b_{i_1}b_{i_2}$ modulo $A^3(\mathbb{F}G)$, where $(i_k = 1, 2, 3)$. The result of our computation will be written in

a table as above, consisting of the coefficients of the decomposition $b_{i_1}b_{i_2}$ with respect to the basis

$$\left\{ (1+a)^{j_1}(1+b)^{j_2}(1+c)^{j_3}(1+d)^{j_4} \;\middle|\; \begin{array}{r} j_1+j_2+j_3+2j_4=2; \\ j_1,j_2,j_3=0,1,2;\ j_4=0,1 \end{array} \right\}$$

of the ideal $A^3(\mathbb{F}G)$:

	$(1+a)^2$	$(1+a)(1+b)$	$(1+a)(1+c)$	$(1+b)(1+c)$	$(1+d)$
b_1b_2	$\alpha_1\beta_1+\Delta(\alpha,\beta)$	$\alpha_1\beta_2+\alpha_2\beta_1$	$\alpha_1\beta_3+\alpha_3\beta_1$	$\alpha_2\beta_3+\alpha_3\beta_2$	$\Omega(\alpha,\beta)$
b_2b_1	$\alpha_1\beta_1+\Delta(\beta,\alpha)$	$\alpha_1\beta_2+\alpha_2\beta_1$	$\alpha_1\beta_3+\alpha_3\beta_1$	$\alpha_2\beta_3+\alpha_3\beta_2$	$\Omega(\beta,\alpha)$
b_1b_3	$\alpha_1\gamma_1+\Delta(\alpha,\gamma)$	$\alpha_1\gamma_2+\alpha_2\gamma_1$	$\alpha_1\gamma_3+\alpha_3\gamma_1$	$\alpha_2\gamma_3+\alpha_3\gamma_2$	$\Omega(\alpha,\gamma)$
b_3b_1	$\alpha_1\gamma_1+\Delta(\gamma,\alpha)$	$\alpha_1\gamma_2+\alpha_2\gamma_1$	$\alpha_1\gamma_3+\alpha_3\gamma_1$	$\alpha_2\gamma_3+\alpha_3\gamma_2$	$\Omega(\gamma,\alpha)$
b_2b_3	$\beta_1\gamma_1+\Delta(\beta,\gamma)$	$\beta_1\gamma_2+\beta_2\gamma_1$	$\beta_1\gamma_3+\beta_3\gamma_1$	$\beta_2\gamma_3+\beta_3\gamma_2$	$\Omega(\beta,\gamma)$
b_3b_2	$\beta_1\gamma_1+\Delta(\gamma,\beta)$	$\beta_1\gamma_2+\beta_2\gamma_1$	$\beta_1\gamma_3+\beta_3\gamma_1$	$\beta_2\gamma_3+\beta_3\gamma_2$	$\Omega(\gamma,\beta)$
b_1^2	$\alpha_1^2+\Delta(\alpha,\alpha)$	0	0	0	$\Omega(\alpha,\alpha)$
b_2^2	$\beta_1^2+\Delta(\beta,\beta)$	0	0	0	$\Omega(\beta,\beta)$
b_3^2	$\gamma_1^2+\Delta(\gamma,\gamma)$	0	0	0	$\Omega(\gamma,\gamma)$

Here, if $G=G_{28}$ then $\Delta(\delta,\epsilon)=\delta_3\epsilon_1$, $\Omega(\delta,\epsilon)=\delta_3\epsilon_2$, if $G=G_{29}$ then $\Delta(\delta,\epsilon)=\delta_3\epsilon_1+\delta_3\epsilon_3$, $\Omega(\delta,\epsilon)=\delta_3\epsilon_2$ and if $G=G_{30}$ then $\Delta(\delta,\epsilon)=\delta_3\epsilon_2$, $\Omega(\delta,\epsilon)=\delta_3\epsilon_1$.

It is easy to see that the first six lines are not equal to either zero or the last three lines. Since the dimension of $A^2(\mathbb{F}G)/A^3(\mathbb{F}G)$ is equal to 5 and $\mathbb{F}G$ is not commutative we have modulo $A^3(\mathbb{F}G)$ either

$$b_1b_2\equiv b_2b_1, \qquad b_1b_3\not\equiv b_3b_1, \qquad b_2b_3\not\equiv b_3b_2$$

or

$$b_1b_2\equiv b_2b_1, \qquad b_1b_3\equiv b_3b_1, \qquad b_2b_3\not\equiv b_3b_2,$$

because the other cases are symmetric to these.

In the first case we get that $b_1^2\equiv b_2^2\equiv b_3^2\equiv 0 \pmod{A^3(\mathbb{F}G)}$, so $\Delta=0$, where Δ is as in (4.1), which is impossible. In the second case

$$b_1b_2\equiv b_2b_1 \pmod{A^3(\mathbb{F}G)} \qquad \text{and} \qquad b_1b_3\equiv b_3b_1 \pmod{A^3(\mathbb{F}G)}.$$

Assume that α_3 is equal to zero. The second and sixth columns give that $\beta_3=\gamma_3=0$ which is impossible, so $\alpha_3,\beta_3,\gamma_3\neq 0$. From columns 2 and 6 we obtain $b_2\equiv\beta_3\alpha_3^{-1}b_1 \pmod{A^2(\mathbb{F}G)}$ which is a contradiction. Thus these group algebras have no filtered multiplicative basis.

Case 5. Let G be one of the following groups:

$$G_{31} = \langle\ a,b,c \mid a^4 = b^4 = c^2 = 1,\ (b,c) = a^2b^2,\ (a,c) = a^2,\ (a,b) = 1\ \rangle;$$
$$G_{32} = \langle\ a,b,c \mid a^4 = b^4 = 1,\ c^2 = a^2b^2,\ (b,c) = a^2b^2,\ (a,c) = a^2,\ (a,b) = 1\ \rangle;$$
$$G_{33} = \langle\ a,b,c \mid a^4 = b^4 = c^2 = 1,\ (b,c) = a^2,\ (a,c) = a^2b^2,\ (a,b) = 1\ \rangle;$$
$$G_{34} = \langle\ a,b,c \mid a^4 = b^4 = c^2 = 1,\ (b,c) = b^2,\ (a,c) = a^2,\ (a,b) = 1\ \rangle;$$
$$G_{35} = \langle\ a,b,c \mid a^4 = b^4 = 1,\ c^2 = a^2,\ (b,c) = b^2,\ (a,c) = a^2,\ (a,b) = 1\ \rangle.$$

Let us compute $b_{i_1}b_{i_2}$ modulo $A^3(\mathbb{F}G)$, $(i_k = 1,2,3)$. The result of our computations will be written as before, in a table, with respect to the basis

$$\left\{\ (1+a)^{j_1}(1+b)^{j_2}(1+c)^{j_3}\ \middle|\ j_1+j_2+j_3 = 2;\ j_1,j_2,j_3 = 0,1,2\ \right\}$$

of the ideal $A^3(\mathbb{F}G)$. If $G = G_{31}$ then

$$(1+c)(1+a) \equiv (1+a)(1+c) + (1+a)^2 \pmod{A^3(\mathbb{F}G)};$$
$$(1+c)(1+b) \equiv (1+b)(1+c) + (1+a)^2 + (1+b)^2 \pmod{A^3(\mathbb{F}G)}.$$

If $G = G_{32}$ then

$$(1+c)(1+a) \equiv (1+a)(1+c) + (1+a)^2 \pmod{A^3(\mathbb{F}G)};$$
$$(1+c)(1+b) \equiv (1+b)(1+c) + (1+a)^2 + (1+b)^2 \pmod{A^3(\mathbb{F}G)};$$
$$(1+c)^2 \equiv (1+a)^2 + (1+b)^2 \pmod{A^3(\mathbb{F}G)}.$$

If $G = G_{33}$ then

$$(1+c)(1+a) \equiv (1+a)(1+c) + (1+a)^2 + (1+b)^2 \pmod{A^3(\mathbb{F}G)};$$
$$(1+c)(1+b) \equiv (1+b)(1+c) + (1+a)^2 \pmod{A^3(\mathbb{F}G)}.$$

If $G = G_{34}$ then

$$(1+c)(1+a) \equiv (1+a)(1+c) + (1+a)^2 \pmod{A^3(\mathbb{F}G)};$$
$$(1+c)(1+b) \equiv (1+b)(1+c) + (1+b)^2 \pmod{A^3(\mathbb{F}G)}.$$

If $G = G_{35}$ then

$$(1+c)(1+a) \equiv (1+a)(1+c) + (1+a)^2 \pmod{A^3(\mathbb{F}G)};$$
$$(1+c)(1+b) \equiv (1+b)(1+c) + (1+b)^2 \pmod{A^3(\mathbb{F}G)};$$
$$(1+c)^2 \equiv (1+a)^2 \pmod{A^3(\mathbb{F}G)}.$$

Using the last 12 identities we get

	$(1+a)^2$	$(1+a)(1+b)$	$(1+a)(1+c)$	$(1+b)(1+c)$	$(1+b)^2$
b_1b_2	$\Delta(\alpha,\beta)$	$\alpha_1\beta_2+\alpha_2\beta_1$	$\alpha_1\beta_3+\alpha_3\beta_1$	$\alpha_2\beta_3+\alpha_3\beta_2$	$\Omega(\alpha,\beta)$
b_2b_1	$\Delta(\beta,\alpha)$	$\alpha_1\beta_2+\alpha_2\beta_1$	$\alpha_1\beta_3+\alpha_3\beta_1$	$\alpha_2\beta_3+\alpha_3\beta_2$	$\Omega(\beta,\alpha)$
b_1b_3	$\Delta(\gamma,\alpha)$	$\alpha_1\gamma_2+\alpha_2\gamma_1$	$\alpha_1\gamma_3+\alpha_3\gamma_1$	$\alpha_2\gamma_3+\alpha_3\gamma_2$	$\Omega(\gamma,\alpha)$
b_3b_1	$\Delta(\alpha,\gamma)$	$\alpha_1\gamma_2+\alpha_2\gamma_1$	$\alpha_1\gamma_3+\alpha_3\gamma_1$	$\alpha_2\gamma_3+\alpha_3\gamma_2$	$\Omega(\alpha,\gamma)$
b_2b_3	$\Delta(\gamma,\beta)$	$\beta_1\gamma_2+\beta_2\gamma_1$	$\beta_1\gamma_3+\beta_3\gamma_1$	$\beta_2\gamma_3+\beta_3\gamma_2$	$\Omega(\gamma,\beta)$
b_3b_2	$\Delta(\beta,\gamma)$	$\beta_1\gamma_2+\beta_2\gamma_1$	$\beta_1\gamma_3+\beta_3\gamma_1$	$\beta_2\gamma_3+\beta_3\gamma_2$	$\Omega(\beta,\gamma)$
b_1^2	$\Delta(\alpha,\alpha)$	0	0	0	$\Omega(\alpha,\alpha)$
b_2^2	$\Delta(\beta,\beta)$	0	0	0	$\Omega(\beta,\beta)$
b_3^2	$\Delta(\gamma,\gamma)$	0	0	0	$\Omega(\gamma,\gamma)$

where $\Delta(\delta,\epsilon)$ and $\Omega(\delta,\epsilon)$ are the following:

	$\Delta(\delta,\epsilon)$	$\Omega(\delta,\epsilon)$
G_{31}	$\delta_1\epsilon_1+\delta_3\epsilon_1+\delta_3\epsilon_2$	$\delta_2\epsilon_2+\delta_3\epsilon_2$
G_{32}	$\delta_1\epsilon_1+\delta_3\epsilon_1+\delta_3\epsilon_2+\delta_3\epsilon_3$	$\delta_2\epsilon_2+\delta_3\epsilon_2+\delta_3\epsilon_3$
G_{33}	$\delta_1\epsilon_1+\delta_3\epsilon_1+\delta_3\epsilon_2$	$\delta_2\epsilon_2+\delta_3\epsilon_1$
G_{34}	$\delta_1\epsilon_1+\delta_3\epsilon_1$	$\delta_2\epsilon_2+\delta_3\epsilon_2$
G_{35}	$\delta_1\epsilon_1+\delta_3\epsilon_1+\delta_3\epsilon_3$	$\delta_2\epsilon_2+\delta_3\epsilon_2$

It is easy to see that the first six lines are not equal to either zero or the last three lines. Since the dimension of $A^2(\mathbb{F}G)/A^3(\mathbb{F}G)$ is equal to 5 and $\mathbb{F}G$ is not commutative, we have by modulo $A^3(\mathbb{F}G)$ either

$$b_1b_2 \equiv b_2b_1, \qquad b_1b_3 \not\equiv b_3b_1, \qquad b_2b_3 \not\equiv b_3b_2$$

or

$$b_1b_2 \equiv b_2b_1, \qquad b_1b_3 \equiv b_3b_1, \qquad b_2b_3 \not\equiv b_3b_2,$$

because the other cases are symmetric to these.

We can see in both cases that $b_1b_2 \equiv b_2b_1 \pmod{A^3(\mathbb{F}G)}$. Assume that $\alpha_3 = 0$. The second and sixth columns give that $\beta_3 = \gamma_3 = 0$ which is impossible, so $\alpha_3, \beta_3, \gamma_3$ are not zero. From columns 2 and 6 it follows that b_2 depends on b_1 modulo $A^2(\mathbb{F}G)$ which is a contradiction, so these group algebras have no filtered multiplicative basis.

Case 6. Let $G = G_{49}$ and put

$$\begin{aligned} u &\equiv (1+a)+(1+c) \pmod{A^2(\mathbb{F}G)},\\ v &\equiv (1+b)+(1+d) \pmod{A^2(\mathbb{F}G)},\\ w &\equiv (1+b)+(1+c)+(1+d) \pmod{A^2(\mathbb{F}G)},\\ z &\equiv (1+a)+(1+b)+(1+c) \pmod{A^2(\mathbb{F}G)}. \end{aligned}$$

Using the identities:

$$\begin{aligned} (1+b)(1+a) &\equiv (1+a)(1+b)+(1+a)^2 \pmod{A^3(\mathbb{F}G)};\\ (1+d)(1+c) &\equiv (1+c)(1+d)+(1+a)^2 \pmod{A^3(\mathbb{F}G)};\\ (1+a)^2 &\equiv (1+b)^2 \equiv (1+c)^2 \equiv (1+d)^2 \pmod{A^3(\mathbb{F}G)}, \end{aligned}$$

we get the following facts:

- $\{uv, uw, uz, zu, vw, vz, wz \pmod{A^3(\mathbb{F}G)}\}$ is a basis of $A^2(\mathbb{F}G)/A^3(\mathbb{F}G)$;
- $\{uzu, uvw, vzu, wzu, vuz, uzw, vwz, zuz \pmod{A^4(\mathbb{F}G)}\}$ is a basis for $A^3(\mathbb{F}G)/A^4(\mathbb{F}G)$;
- $\{vuzu, wuzu, zuzu, vzuz, wzuz, uvwz, vwzu \pmod{A^5(\mathbb{F}G)}\}$ is a basis of $A^4(\mathbb{F}G)/A^5(\mathbb{F}G)$;
- $\{vzuz, wzuz, vwuzu, vwzuz \pmod{A^6(\mathbb{F}G)}\}$ is a basis of $A^5(\mathbb{F}G)/A^6(\mathbb{F}G)$,

and the element $vwzuzu$ form a basis for $A^6(\mathbb{F}G)$.

Case 7. Let

$$\begin{aligned} G = G_{50} = \langle\ a,b,c,d \mid\ & a^4 = b^2 = c^2 = d^4 = 1,\ a^2 = d^2,\\ & (a,d) = (b,c) = (c,d) = a^2,\ (a,b) = (a,c) = (b,d) = 1\ \rangle. \end{aligned}$$

Using the identities:

$$\begin{aligned}(1+d)(1+a) &\equiv (1+a)(1+d)+(1+a)^2 \pmod{A^3(\mathbb{F}G)};\\ (1+c)(1+b) &\equiv (1+b)(1+c)+(1+a)^2 \pmod{A^3(\mathbb{F}G)};\\ (1+d)(1+c) &\equiv (1+c)(1+d)+(1+a)^2 \pmod{A^3(\mathbb{F}G)};\\ (1+a)^2 &\equiv (1+d)^2 \pmod{A^3(\mathbb{F}G)},\end{aligned}$$

let us compute $b_{i_1}b_{i_2}$ modulo $A^3(\mathbb{F}G)$, where b_{i_k} and Δ are as in (4.1) and $i_k = 1,2,3,4$. We shall write the result of our computations in a table, similarly to the previous cases with respect to the basis

$$\left\{ (1+a)^{j_1}(1+b)^{j_2}(1+c)^{j_3}(1+d)^{j_4} \;\middle|\; \begin{array}{r} j_1+j_2+j_3+j_4=2;\\ j_1=0,1,2;\ j_2,j_3,j_4=0,1 \end{array} \right\}$$

of the ideal $A^2(\mathbb{F}G)$:

	$(1+a)(1+b)$	$(1+a)(1+c)$	$(1+a)(1+d)$	$(1+b)(1+c)$	$(1+b)(1+d)$	$(1+c)(1+d)$	$(1+a)^2$
b_1b_2	$\Delta^{1,2}(\alpha,\beta)$	$\Delta^{1,3}(\alpha,\beta)$	$\Delta^{1,4}(\alpha,\beta)$	$\Delta^{2,3}(\alpha,\beta)$	$\Delta^{2,4}(\alpha,\beta)$	$\Delta^{3,4}(\alpha,\beta)$	$\Omega_{\alpha,\beta}$
b_2b_1	$\Delta^{1,2}(\alpha,\beta)$	$\Delta^{1,3}(\alpha,\beta)$	$\Delta^{1,4}(\alpha,\beta)$	$\Delta^{2,3}(\alpha,\beta)$	$\Delta^{2,4}(\alpha,\beta)$	$\Delta^{3,4}(\alpha,\beta)$	$\Omega_{\beta,\alpha}$
b_1b_3	$\Delta^{1,2}(\alpha,\gamma)$	$\Delta^{1,3}(\alpha,\gamma)$	$\Delta^{1,4}(\alpha,\gamma)$	$\Delta^{2,3}(\alpha,\gamma)$	$\Delta^{2,4}(\alpha,\gamma)$	$\Delta^{3,4}(\alpha,\gamma)$	$\Omega_{\alpha,\gamma}$
b_3b_1	$\Delta^{1,2}(\alpha,\gamma)$	$\Delta^{1,3}(\alpha,\gamma)$	$\Delta^{1,4}(\alpha,\gamma)$	$\Delta^{2,3}(\alpha,\gamma)$	$\Delta^{2,4}(\alpha,\gamma)$	$\Delta^{3,4}(\alpha,\gamma)$	$\Omega_{\gamma,\alpha}$
b_1b_4	$\Delta^{1,2}(\alpha,\delta)$	$\Delta^{1,3}(\alpha,\delta)$	$\Delta^{1,4}(\alpha,\delta)$	$\Delta^{2,3}(\alpha,\delta)$	$\Delta^{2,4}(\alpha,\delta)$	$\Delta^{3,4}(\alpha,\delta)$	$\Omega_{\alpha,\delta}$
b_4b_1	$\Delta^{1,2}(\alpha,\delta)$	$\Delta^{1,3}(\alpha,\delta)$	$\Delta^{1,4}(\alpha,\delta)$	$\Delta^{2,3}(\alpha,\delta)$	$\Delta^{2,4}(\alpha,\delta)$	$\Delta^{3,4}(\alpha,\delta)$	$\Omega_{\delta,\alpha}$
b_2b_3	$\Delta^{1,2}(\beta,\gamma)$	$\Delta^{1,3}(\beta,\gamma)$	$\Delta^{1,4}(\beta,\gamma)$	$\Delta^{2,3}(\beta,\gamma)$	$\Delta^{2,4}(\beta,\gamma)$	$\Delta^{3,4}(\beta,\gamma)$	$\Omega_{\beta,\gamma}$
b_3b_2	$\Delta^{1,2}(\beta,\gamma)$	$\Delta^{1,3}(\beta,\gamma)$	$\Delta^{1,4}(\beta,\gamma)$	$\Delta^{2,3}(\beta,\gamma)$	$\Delta^{2,4}(\beta,\gamma)$	$\Delta^{3,4}(\beta,\gamma)$	$\Omega_{\gamma,\beta}$
b_2b_4	$\Delta^{1,2}(\beta,\delta)$	$\Delta^{1,3}(\beta,\delta)$	$\Delta^{1,4}(\beta,\delta)$	$\Delta^{2,3}(\beta,\delta)$	$\Delta^{2,4}(\beta,\delta)$	$\Delta^{3,4}(\beta,\delta)$	$\Omega_{\beta,\delta}$
b_4b_2	$\Delta^{1,2}(\beta,\delta)$	$\Delta^{1,3}(\beta,\delta)$	$\Delta^{1,4}(\beta,\delta)$	$\Delta^{2,3}(\beta,\delta)$	$\Delta^{2,4}(\beta,\delta)$	$\Delta^{3,4}(\delta,\beta)$	$\Omega_{\beta,\delta}$
b_3b_4	$\Delta^{1,2}(\gamma,\delta)$	$\Delta^{1,3}(\gamma,\delta)$	$\Delta^{1,4}(\gamma,\delta)$	$\Delta^{2,3}(\gamma,\delta)$	$\Delta^{2,4}(\gamma,\delta)$	$\Delta^{3,4}(\gamma,\delta)$	$\Omega_{\gamma,\delta}$
b_4b_3	$\Delta^{1,2}(\gamma,\delta)$	$\Delta^{1,3}(\gamma,\delta)$	$\Delta^{1,4}(\gamma,\delta)$	$\Delta^{2,3}(\gamma,\delta)$	$\Delta^{2,4}(\gamma,\delta)$	$\Delta^{3,4}(\delta,\gamma)$	$\Omega_{\gamma,\delta}$
b_1^2	0	0	0	0	0	0	$\Omega_{\alpha,\alpha}$
b_2^2	0	0	0	0	0	0	$\Omega_{\beta,\beta}$
b_3^2	0	0	0	0	0	0	$\Omega_{\gamma,\gamma}$
b_4^2	0	0	0	0	0	0	$\Omega_{\delta,\delta}$

where $\Omega_{\varepsilon,\eta} = \varepsilon_1\eta_1+\varepsilon_4\eta_4+\varepsilon_3\eta_2+\varepsilon_4\eta_1+\varepsilon_4\eta_3$ and $\Delta^{i,j}(\varepsilon,\eta) = \varepsilon_i\eta_j+\varepsilon_j\eta_i$.

It is easy to see that the first twelve lines are not equal to either zero or the last four lines.

Since $\Delta^{i,j}(\varepsilon,\eta)$ is a subdeterminant of Δ and $\Delta \neq 0$, by expansion theorem of determinant b_ib_j cannot be equivalent other else $b_kb_l \pmod{A^3(\mathbb{F}G)}$ apart from the case when $k=j$ and $l=i$.

Assume that $\left\{u \equiv b_1, v \equiv b_2, w \equiv b_3, z \equiv b_4 \pmod{A^2(\mathbb{F}G)}\right\}$ and the coefficients of u,v,w,z will be denoted by $\alpha_i,\beta_i,\gamma_i,\delta_i$, respectively.

Since the dimension of $A^2(\mathbb{F}G)/A^3(\mathbb{F}G)$ is equal to 7 and this group algebra is not commutative, we have that

$$\begin{aligned} &uv \equiv vu, \quad uw \equiv wu, \quad uz \equiv zu, \quad vw \equiv wv, \\ &vz \equiv zv, \quad wz \not\equiv zw, \quad u^2 \equiv v^2 \equiv w^2 \equiv z^2 \equiv 0, \end{aligned} \tag{4.5}$$

and the other cases are analogous to this one.

Assume that $\mathbb{F}G$ has a filtered multiplicative basis and the set

$$\{u, v, w, z \pmod{A^2(\mathbb{F}G)}\}$$

is a basis of $A(\mathbb{F}G)/A^2(\mathbb{F}G)$. Using (4.5) simple computations show that

- $\{uv, uw, uz, vw, vz, wz, zw \pmod{A^3(\mathbb{F}G)}\}$ is a basis for $A^2(\mathbb{F}G)/A^3(\mathbb{F}G)$;
- $\{uvw, uvz, uwz, uzw, vwz, vzw, wzw, zwz \pmod{A^4(\mathbb{F}G)}\}$ is a basis of $A^3(\mathbb{F}G)/A^4(\mathbb{F}G)$;
- $\{uvwz, uvzw, uwzw, uzwz, vwzw, vzwz, wzwz \pmod{A^5(\mathbb{F}G)}\}$ is a basis for $A^4(\mathbb{F}G)/A^5(\mathbb{F}G)$;
- $\{uvwzw, uvzwz, uwzwz, vwzwz \pmod{A^6(\mathbb{F}G)}\}$ is a basis for $A^5(\mathbb{F}G)/A^6(\mathbb{F}G)$;
- $\{uvwzwz\}$ is a basis of $A^6(\mathbb{F}G)$.

This is the requirement of existence of filtered multiplicative $\mathbb{F}$-basis. Suppose that $\alpha_4 = 0$ and there exists $b \in \{v, w, z\}$ such that b is congruent with $\varepsilon_1(1+a)+\varepsilon_2(1+b)+\varepsilon_3(1+c)+\varepsilon_4(1+d) \pmod{A^2(\mathbb{F}G)}$ and $\varepsilon_4 = 0$. The facts $u^2 \equiv b^2 \equiv 0$ and $ub \equiv bu \pmod{A^3(\mathbb{F}G)}$ give that $\alpha_3\varepsilon_2 + \alpha_2\varepsilon_3 = 0$ and $\alpha_1^2 + \alpha_2\alpha_3 = \varepsilon_1^2 + \varepsilon_2\varepsilon_3 = 0$. It is very simple to prove that either $b_1 \equiv 0$ or $b_1 \equiv b_i \pmod{A^2(\mathbb{F}G)}$, which is impossible.

Now, we shall consider two subcases.

Subcase 1. Suppose that $\alpha_4 = 0$ and without loss of generality we can assume that $\beta_4 = \gamma_4 = 1$. For $\alpha_2 = 0$ it follows that $\Delta = 0$, so we can also assume that $\alpha_2 = 1$. According to eighth column of the previous table

$$\begin{aligned} \alpha_1^2 + \alpha_3 &= 0; \\ \beta_1 + \beta_3 + 1 &= \beta_1^2 + \beta_2\beta_3; \\ \gamma_1 + \gamma_3 + 1 &= \gamma_1^2 + \gamma_2\gamma_3. \end{aligned} \tag{4.6}$$

Since $vw \equiv wv \pmod{A^3(\mathbb{F}G)}$ we get

$$\beta_3\gamma_2 + \gamma_1 + \gamma_3 + 1 = \beta_2\beta_3 + \beta_1 + \beta_3 + 1$$

and using (4.6) it follows that

$$(\beta_1 + \gamma_1)^2 = (\beta_2 + \gamma_2)(\beta_3 + \gamma_3). \tag{4.7}$$

Also eighth column of the previous table and $uv \equiv vu$, $uw \equiv wu \pmod{A^3(\mathbb{F}G)}$ give that $\alpha_1^2\beta_2 + \beta_3 = \alpha_1^2\gamma_2 + \gamma_3$, so

$$\alpha_1^2(\beta_2 + \gamma_2) = \beta_3 + \gamma_3. \tag{4.8}$$

Thus (4.7) and (4.8) give the equation $\beta_1 + \gamma_1 = \alpha_1(\beta_2 + \gamma_2)$.

Since $\alpha_1^2 = \alpha_3$ we have got that $v + w \equiv (\beta_2 + \gamma_2)u \pmod{A^3(\mathbb{F}G)}$ which is a contradiction.

Subcase 2. Suppose that $\alpha_4, \beta_4 \neq 0$ and without loss of generality we can assume that $\alpha_4 = \beta_4 = 1$. Simple computations show that $\{u \equiv b_1 + b_2, v \equiv b_2, w \equiv b_3, z \equiv b_4 \pmod{A^2(\mathbb{F}G)}\}$ form a basis of $A(\mathbb{F}G)/A^2(\mathbb{F}G)$, satisfies conditions (4.5) and the requirement of existence of filtered multiplicative $\mathbb{F}$-basis, but it is a contradiction to subcase 1, so this group algebra has no filtered multiplicative basis. This completes the proof of the theorem.

□

Summary

After the simple groups had been described, the structure of finite p-groups became the focus of studies on group theory, the study of groups of units of group algebras of finite p-groups has become topical.

In Chapter Two we examine the structure of the normalized group of units $V(\mathbb{F}_2G)$ of the group algebra $\mathbb{F}_2G$, if G is a group of maximal class of order 2^n, that is, its nilpotency class is $n-1$. It is well known that the 2-groups of maximal class are the following extensions of $C = \langle\ a \mid a^{2^n} = 1\ \rangle$:

$$Q_{2^{n+1}} = \langle\ a, b_1 \mid a^{2^n} = 1, b_1^2 = a^{2^{n-1}}, (a, b_1) = a^{-2}\rangle \text{ with } n \geq 2;$$
$$D_{2^{n+1}} = \langle\ a, b_2 \mid a^{2^n} = 1, b_2^2 = 1, (a, b_2) = a^{-2}\rangle \text{ with } n \geq 2;$$
$$SD_{2^{n+1}} = \langle\ a, b_3 \mid a^{2^n} = 1, b_3^2 = 1, (a, b_3) = a^{-2+2^{n-1}}\rangle \text{ with } n \geq 3.$$

The set

$$V_\sigma(\mathbb{F}_pG) = \left\{\ x \in V(\mathbb{F}_pG) \ \middle|\ x^{-1} = x^\sigma\ \right\}$$

pertaining to the involution σ is a subgroup of the group $V(\mathbb{F}_pG)$, which is called *σ-unitary subgroup*.

Let us denote by $\circledast$ the linearly extension of the automorphism $a^i \mapsto a^{(2^{n-1}-1)i}$ of the group C to the group algebra $\mathbb{F}_2C$. This extension is an involution of the algebra $\mathbb{F}_2C$. We proved the following lemma and corollary:

Theorem (2.2.4). *The order of the $\circledast$-unitary subgroup $V_\circledast(\mathbb{F}_2C)$ is $2^{\frac{|C|}{2}}$ and*

$$V_\circledast(\mathbb{F}_2C) = W_\circledast(C) \times \langle\ 1 + \widehat{C}\rangle,$$

where $\widehat{C}$ *is the sum of the elements of the group* C *and* $W_{\circledast}(C)$ *is equal to* $\varphi\big(V(\mathbb{F}_2C)\big)$ *and the homomorphism* $\varphi : V(\mathbb{F}_2C) \to V(\mathbb{F}_2C)$ *is defined by* $\varphi(x) = x^{\circledast}x^{-1}$.

Corollary. *Denote the canonical involution of* $\mathbb{F}_2C$ *by* $*$. *Then*

$$\big|V_{\circledast}(\mathbb{F}_2C)\big| = \frac{|V_*(\mathbb{F}_2C)|}{2}.$$

Using the previous results we showed that there is a strong correlation between elements of order two of the normalized group of units $V(\mathbb{F}_2G)$, where G is a 2-group of maximal class and the unitary subgroups of $V(\mathbb{F}_2C)$. The main theorem of the chapter:

Theorem. *Let* G *be a 2-group of maximal class and let* $\Theta_G(2)$ *be the number of elements of order two in* $V(\mathbb{F}_2G)$. *Then*

$$\begin{aligned}\Theta_{D_{2^{n+1}}}(2) &= 2^{2^n+n-1} + 2^{2^n};\\ \Theta_{SD_{2^{n+1}}}(2) &= 2^{2^n+n-1};\\ \Theta_{Q_{2^{n+1}}}(2) &= 2^{2^n+n-1} - 2^{2^n}.\end{aligned}$$

The corollary of this theorem is the solution of the Berman's question for 2-group of maximal class:

Corollary. *Let* $\mathbb{F}_2$ *be the field of two elements, and let* G *and* H *be finite 2-groups of maximal class. Then* $V(\mathbb{F}_2G)$ *is isomorphic to* $V(\mathbb{F}_2H)$ *if and only if* G *and* H *are isomorphic.*

Let us mention that this corollary is a generalization of Baginski's result [3].

An other actual problem in the theory of finite p-groups is the description of the pth power structure. In Chapter Three we examine the power structure of $V(\mathbb{F}_pG)$.

Theorem. *Let* G *be a finite* p*-group with commutator subgroup* G' *of order* $p > 2$. *Then* $V(\mathbb{F}_pG)^p$ *is a subgroup of the center* $\zeta\big(V(\mathbb{F}_pG)\big)$.

Consequently the further powers can be easy determined. Moreover, if the Frattini subgroup of G is of order p then we described the structure of the group $V(\mathbb{F}_pG)^p$. Let $C_{g_1}, C_{g_2}, \ldots, C_{g_t}$ be the all conjugacy classes of G, which consists of at least two elements and $\widehat{C_{g_i}}$ is the sum of all elements of C_{g_i}. We proved that:

Theorem. *Let G be a finite nonabelian p-group with Frattini subgroup of order p. Then $V(\mathbb{F}_pG)^p = V\left(\mathbb{F}_pG^p\right) \times N$, where $N = \prod_{i=1}^{t} \langle 1 + \widehat{C_{g_i}} \rangle$.*

The following question which is also attached to the power structure of normalized group of units can be found in Johnson's paper [35]. Is it true that

$$G^p = V(\mathbb{F}_pG)^p \cap G?$$

We proved that:

Corollary. *Let G be a p-group with Frattini subgroup of order p and $p > 2$. Then*

$$G^p = V(\mathbb{F}_pG)^p \cap G.$$

Using the previous results of the power structure, we proved that the Berman's question is true for groups with Frattini subgroup of order $p > 2$:

Theorem. *Let G and H be finite nonabelian p-groups with cyclic Frattini subgroup and $p > 2$. Then $V(\mathbb{F}_pG)$ is isomorphic to $V(\mathbb{F}_pH)$ if and only if G and H are isomorphic.*

In the fourth chapter of this thesis we investigate the existence of filtered multiplicative $\mathbb{F}$-basis of the algebra $\mathbb{F}G$ over a field of characteristic p. we gave a complete list of all p-groups G of order less than p^5, such that the group algebra $\mathbb{F}G$ has a filtered multiplicative $\mathbb{F}$-basis, and we gave these bases as well.

Theorem. *Let $\mathbb{F}G$ be the group algebra of a finite nonabelian p-group G of order p^n over a field $\mathbb{F}$ of characteristic p, where $n < 5$. Then $\mathbb{F}G$ possesses a filtered multiplicative $\mathbb{F}$-basis if and only if $p = 2$ and G is one of the following groups:*

1. *dihedral group D_n of order n, where n equals either 8 or 16;*

2. *either the quaternion group Q_8 of order 8 or $Q_8 \times C_2$, and $\mathbb{F}$ contains a primitive cube root of the unity;*

3. *either $D_8 \times C_2$, or the central product $D_8 \curlyvee C_4$ of D_8 with the cyclic group C_4 of order 4;*

4. $$H_{16} = \langle\ a, c \mid a^4 = b^2 = c^2 = 1,\ (a,b) = 1, (a,c) = b, \\ (b,c) = 1\ \rangle.$$

Let us mention that this result suggests that a group algebra $\mathbb{F}G$ has a filtered multiplicative $\mathbb{F}$-basis only if $p = 2$.

Group algebras of all groups of order 2^5 which contain filtered multiplicative $\mathbb{F}$-basis are also described. For the inquiry we used the computer algebra system GAP [28] and its package LAGUNA [18]. In the theorem, indices that appear in the list of groups are identical with the GAP numbers identifying the groups.

Theorem. *Let $\mathbb{F}G$ be the group algebra of a finite nonabelian 2-group G of order 2^5 over a field $\mathbb{F}$ of characteristic 2. Then $\mathbb{F}G$ possesses a filtered multiplicative $\mathbb{F}$-basis if and only if G is one of the following groups:*

1. $G_{18} = D_{32}$, $G_{25} = D_8 \times C_4$, $G_{39} = D_{16} \times C_2$ *or* $G_{46} = D_8 \times C_2 \times C_2$;

2. $G_{26} = Q_8 \times C_4$, *or* $G_{47} = Q_8 \times C_2 \times C_2$ *and* $\mathbb{F}$ *contains a primitive cube root of the unity;*

3. $G_{22} = H_{16} \times C_2$, $G_{48} = (D_8 \curlyvee C_4) \times C_2$;

4.

$$G_2 = \langle\ a, b\ \mid\ a^4 = b^4 = c^2 = 1,\ (a,b) = c,\ (a,c) = 1,\ (b,c) = 1\ \rangle;$$
$$G_5 = \langle\ a, b\ \mid\ a^8 = b^2 = c^2 = 1,\ (a,b) = c,\ (a,c) = (b,c) = 1\ \rangle;$$
$$G_7 = \langle\ a, b, c\ \mid\ a^8 = b^2 = c^2 = 1,\ (a,c) = a^4,\ (a,b) = a^4c,\ (b,c) = 1\ \rangle;$$
$$G_8 = \langle\ a, b, c\ \mid\ a^8 = c^2 = 1,\ b^2 = a^4,\ (a,c) = a^4,\ (a,b) = a^4c,\ (b,c) = 1\ \rangle;$$
$$G_9 = \langle\ a, b, c\ \mid\ a^2 = b^8 = c^2 = 1,\ (b,c) = ab^6,\ (a,c) = (a,b) = 1\ \rangle;$$
$$G_{10} = \langle\ a, b, c\ \mid\ a^8 = b^4 = c^2 = 1,\ a^4 = b^2,\ (a,b) = a^6c,\ (a,c) = (b,c) = 1\ \rangle;$$
$$G_{11} = \langle\ a, b, c\ \mid\ a^4 = b^4 = c^2 = 1,\ (b,c) = ab^2,\ (a,c) = (a,b) = 1\ \rangle;$$
$$G_{49} = \langle\ a, b, c, d\ \mid\ a^4 = 1,\ b^2 = c^2 = d^2 = a^2,\ (a,b) = a^2,\ (c,d) = a^2,\ (a,c) = (a,d) = (b,c) = (b,d) = 1\ \rangle.$$

Apart from these, we proved the following theorem:

Theorem. *Let* $char(\mathbb{F}) = 2$.

1. *If*

$$G = \langle\ a, b\ \mid\ a^{2^n} = b^2 = c^2 = d^2 = 1,\ (a,b) = c,\ (a,c) = d,\ (a,d) = (b,c) = (b,d) = (c,d) = 1\ \rangle,$$

   where $n > 1$, *then the group algebra* $\mathbb{F}G$ *does not have filtered multiplicative* $\mathbb{F}$*-basis.*

2. *If*

$$G = \langle\ a, b\ \mid\ a^{2^n} = b^{2^m} = c^2 = 1,\ (a,b) = c,\ (a,c) = 1,\ (b,c) = 1\ \rangle,$$

   where $n, m \geq 2$, *then the group algebra* $\mathbb{F}G$ *have a filtered multiplicative basis.*

Összefoglalás

Bevezetés.
A csoportalgebrák a csoportok reprezentációinak vizsgálata során keletkeztek, azonban a matematika számos területén, így a homológia és a kohomológia elméletben, valamint az algebrai topológiában is alkalmazzák őket. Először Frobenius használta ezt a testekből és csoportokból felépülő érdekes algebrai konstrukciót, mely segítségével a véges csoportok reprezentációit tanulmányozta. A csoportalgebra elnevezés azonban Noether névéhez fűződik.

A csoportalgebrák kutatása a múlt század 30-as éveinek elején kezdődött főleg Frobenius, Schur, Magnus, Noether, Higman és Jennings eredményeivel. Alapvető struktúratételek az 1960-as évektől születnek, és azóta a csoportalgebrák elméletén belül nagy kutatási területek alakultak ki. Ma ilyen meghatározó kutatási irányok a gyűrűelméleti tulajdonságok vizsgálata mellett a csoportalgebrák egységcsoportjának, valamint asszociált Lie algebrájának a tanulmányozása.

Ebben az értekezésben a p karakterisztikájú testek feletti véges p-csoportok csoportalgebráival foglalkozunk. Az egységcsoportjának struktúráját valamint multiplikatív filtrációs bázis létezését vizsgáljuk.

Az első fejezet tartalmazza a csoportalgebrák alapfogalmait, és az értekezés során használt jelöléseket és definíciókat. A következő három fejezet tartalmazza az új eredményeket.

Alapfogalmak és jelölések.
Legyen G egy csoport és $\mathbb{F}$ egy test, melynek az egységeleme 1. Jelöljük $\mathbb{F}G$-vel az összes $\sum_{g\in G}\alpha_g g$ alakú formális összegek halmazát, ahol csak véges sok $\alpha_g \in \mathbb{F}$ együttható nem nulla. Nyilván $\mathbb{F}G$ vektortér az $\mathbb{F}$ test felett, amelynek G a bázisa és a G csoport szorzásművelete indukál egy szorzást az $\mathbb{F}G$ halmazon. Könnyen belátható, hogy $\mathbb{F}G$ algebra az $\mathbb{F}$ test felett, melyet *csoportalgebrának* nevezünk. Abban az esetben, ha $\mathbb{F}$ egy p karakterisztikájú test, és G tartalmaz p-rendű elemet, *moduláris csoportalgebráról* beszélünk.

Most megemlítünk egy problémát, amely Higmantól és Thralltól származik, és nagy hatást gyakorolt a csoportalgebrák szerkezetének a tanulmányozására, és az egységcsoport vizsgálatára.

Legyenek az $\mathbb{F}G$ és $\mathbb{F}H$ csoportalgebrák izmorfak mint algebrák az $\mathbb{F}$ test felett. Milyen összefüggés van a G és a H csoportok között, milyen feltételek kellenek a G és a H csoportok izomorfiájához?

Deskins [26] véges Abel p-csoportok esetén pozitív választ adott erre az izomorfia kérdésre, azaz ha az algebrák izomorfak, akkor a csoportok is izomorfak. Nem Abel-csoportokra sok szerző vizsgálta ezt a kérdést, amely máig sem megoldott. Baginski [3] bebizonyította, hogy maximális osztályú 2-csoportok csoportalgebrái a két elemű test felett egyértelműen meghatározzák a csoportokat. A további ide vonatkozó eredmények Sandling [42] áttekintő cikkében megtalálhatóak.

A csoportalgebrák egységeinek $U(\mathbb{F}G)$ halmaza csoportot alkot, és a

$$V(\mathbb{F}G) = \Big\{ \sum_{g\in G}\alpha_g g \in U(\mathbb{F}G) \;\Big|\; \sum_{g\in G}\alpha_g = 1 \Big\}$$

részhalmaza normális részcsoport, melyet *normalizált egységcsoportnak* nevezünk. Ismert, hogy $U(\mathbb{F}G) = V(\mathbb{F}G) \times U(\mathbb{F})$, ahol $U(\mathbb{F})$ az $\mathbb{F}$ test egységcsoportja, így a teljes egységcsoport vizsgálata helyett annak $V(\mathbb{F}G)$ normalizált egységcsoportját vizsgálva juthatunk információkhoz az egységcsoportról. Ez az elmélet áttekintő jelleggel megtalálható Artamonov és Bódi [1], Bódi [11] cikkeiben, valamint Bódi [22] könyvében.

A G csoport Frattini részcsoportját $\Phi(G)$, a centrumát pedig $\zeta(G)$ jelöli. Jól ismert, hogy a Frattini részcsoport véges G p-csoportok

esetén egybeesik a $G'G^p$ részcsoporttal, ahol $G^p = \langle\ g^p\ \mid\ g \in G\ \rangle$, és G' a G csoport kommutátor részcsoportja.

Új eredmények.
Az értekezés témája a csoportalgebra multiplikatív filtrációs bázisának tanulmányozása és az egységcsoport egyes tulajdonságainak a vizsgálata.

Legyen G véges p-csoport és $\mathbb{F}_p$ a p elemű test. Ekkor az $A(\mathbb{F}_pG)$ fundamentális ideál nilpotens és a $V(\mathbb{F}_pG)$ normalizált egységcsoport egybeesik $1 + A(\mathbb{F}_pG)$-vel. Tehát az $\mathbb{F}_pG$ csoportalgebra $\sum_{g\in G}\alpha_g g$ eleme akkor és csak akkor tartozik a normalizált egységcsoporthoz, ha $\sum_{g\in G}\alpha_g = 1$. Emiatt a $V(\mathbb{F}_pG)$ normalizált egységcsoport rendje $p^{|G|-1}$.

Mivel a véges egyszerű csoportok leírása után a véges p-csoportok szerkezete került a csoportelméleti vizsgálatok középpontjába, így aktuálissá vált a véges p-csoportok csoportalgebra egységcsoportjának tanulmányozása.

A disszertáció első részében a $V(\mathbb{F}_2G)$ normalizált egységcsoport struktúráját vizsgáljuk, ha G egy 2^n-rendű maximális osztályú csoport, azaz a G csoport nilpotencia osztálya $n-1$. Ismert, hogy a maximális osztályú 2-csoportok a $C = \langle\ a\ \mid\ a^{2^n} = 1\ \rangle$ ciklikus csoport következő bővítései:

$$\begin{aligned} Q_{2^{n+1}} &= \langle\ a, b_1\ \mid\ a^{2^n} = 1, b_1^2 = a^{2^{n-1}}, (a, b_1) = a^{-2}\rangle \text{ és } n \geq 2; \\ D_{2^{n+1}} &= \langle\ a, b_2\ \mid\ a^{2^n} = 1, b_2^2 = 1, (a, b_2) = a^{-2}\rangle \text{ és } n \geq 2; \\ SD_{2^{n+1}} &= \langle\ a, b_3\ \mid\ a^{2^n} = 1, b_3^2 = 1, (a, b_3) = a^{-2+2^{n-1}}\rangle \text{ és } n \geq 3. \end{aligned}$$

Megemlítjük, hogy az $\mathbb{F}_pG$ csoportalgebra $x \mapsto x^\sigma$ leképezését *involúciónak* nevezzük, ha

$$(x+y)^\sigma = x^\sigma + y^\sigma, \quad (xy)^\sigma = y^\sigma x^\sigma, \quad \text{és} \quad (x^\sigma)^\sigma = x.$$

Egy adott σ involúcióra a

$$V_\sigma(\mathbb{F}_pC) = \left\{\ x \in V(\mathbb{F}_pC)\ \middle|\ x^{-1} = x^\sigma\ \right\}$$

halmaz a normalizált egységcsoport részcsoportja, melyet *σ-unitér részcsoportnak* nevezünk.

Az $\mathbb{F}_2C$ algebra kanonikus involúciója a C csoport $a^i \mapsto a^{-i}$ automorfizmusának $x \mapsto x^*$ lineáris kiterjesztése az $\mathbb{F}_2C$ csoportalgebrára. Az $\mathbb{F}_2C$ csoportalgebrának van egy másik $x \mapsto x^{\circledast}$ involúciója, amely a C csoport $a^i \mapsto a^{(2^{n-1}-1)i}$ automorfizmusának lineáris kiterjesztése az $\mathbb{F}_2C$ csoportalgebrára.

A második fejezetben a $V(\mathbb{F}_2G)$ normalizált egységcsoport másodrendű elemeinek struktúráját határozzuk meg maximális osztályú 2-csoportok esetén. Megmutatjuk, hogy szoros összefüggés van a $V(\mathbb{F}_2G)$ csoport másodrendű elemei és a $V(\mathbb{F}_2C)$ csoport unitér részcsoportjai között, ha G maximális osztályú 2-csoport. A fejezet főtételének bizonyításához szükségünk van a $V_{\circledast}(\mathbb{F}_2C)$ csoport rendjére és a következő felbontására:

Tétel. *A $V_{\circledast}(\mathbb{F}_2C)$ unitér részcsoport rendje $2^{\frac{|C|}{2}}$ és*

$$V_{\circledast}(\mathbb{F}_2C) = W_{\circledast}(C) \times \langle\, 1 + \widehat{C} \rangle,$$

ahol $\widehat{C}$ a C csoport elemeinek az összege, $W_{\circledast}(C)$ pedig a $\varphi(x) = x^{\circledast}x^{-1}$ $\big(x \in V(\mathbb{F}_2C)\big)$ homomorfizmus képe.

A kanonikus involúció által meghatározott unitér részcsoport és a fent definiált $\circledast$ involúció unitér részcsoportjának rendje között fennáll a következő összefüggés:

Következmény. *Legyen C ciklikus csoport, ekkor*

$$\big|V_{\circledast}(\mathbb{F}_2C)\big| = \frac{|V_*(\mathbb{F}_2C)|}{2}.$$

Az előző eredmények felhasználásával bebizonyítjuk a fejezet főtételét:

Tétel. *Jelölje $\Theta_G(2)$ a másodrendű elemek számát a $V(\mathbb{F}_2G)$ normalizált egységcsoportban. Ekkor*

$$\begin{aligned}
\Theta_{D_{2^{n+1}}}(2) &= 2^{2^n+n-1} + 2^{2^n};\\
\Theta_{SD_{2^{n+1}}}(2) &= 2^{2^n+n-1};\\
\Theta_{Q_{2^{n+1}}}(2) &= 2^{2^n+n-1} - 2^{2^n}.
\end{aligned}$$

Természetes az a kérdés, amely Berman nevéhez fűződik és a normalizált egységcsoport izomorfia problémájának nevezünk. Vajon a $V(\mathbb{F}_pG)$ csoport egyértelműen határozza-e meg a G csoportot? Berman [9] igazolta, hogy véges G Abel p-csoportok esetén a $V(\mathbb{F}_pG)$ csoport egyértelműen meghatározza a G csoportot izomorfia erejéig. A főtétel következményeként azonnal adódik a normalizált egységcsoport izomorfia problémájának megoldása maximális osztályú 2-csoportokra:

Következmény. *Legyen G és H maximális osztályú 2-csoport. Ekkor $V(\mathbb{F}_2G)$ izomorf a $V(\mathbb{F}_2H)$ normalizált egységcsoporttal akkor és csak akkor, ha G és a H izomorfak.*

Megjegyezzük, hogy ez a következmény Baginski [3] eredményének az általánosítása.

Másik időszerű probléma a véges p-csoportok elméletében a p-hatványstruktúra leírása. Ezekből származó eredmények sok tétel bizonyítását tették lehetővé a véges p-csoportok elméletében. A csoportalgebra $V(\mathbb{F}_pG)$ normalizált egységcsoportjára ilyen vizsgálatok nem terjedtek ki.

A harmadik fejezetben a normalizált egységcsoport p-hatványstruktúrájának tulajdonságait vizsgáljuk, ha a $V(\mathbb{F}_pG)$ csoport nilpotencia osztálya p. Baginski [2], Shalev és Mann [39, 43] bebizonyították, hogy a $V(\mathbb{F}_pG)$ nilpotencia osztálya akkor és csak akkor p, ha a G' kommutátor részcsoport rendje p.

Tétel. *Legyen G olyan p-csoport, melynek a kommutátor részcsoportja p prímrendű. A $V(\mathbb{F}_pG)^p$ csoport részcsoportja a $\zeta\big(V(\mathbb{F}_pG)\big)$ centrumnak.*

Jelölje $C_{g_1}, C_{g_2}, \ldots, C_{g_t}$ a G csoport összes különböző, legalább kételemű konjugált osztályát és legyen $\widehat{C_{g_i}}$ a C_{g_i} konjugált osztály elemeinek az összege.

Tétel. *Legyen G véges nem Abel p-csoport ciklikus p-rendű Frattini részcsoporttal és $N = \prod_{i=1}^{t} \langle 1 + \widehat{C_{g_i}} \rangle$. Ekkor a $V(F_pG)^p$ centrális részcsoport a $V\big(F_pG^p\big)$ és az N csoportok direkt szorzata.*

Johnson [35] cikkében található a következő kérdés: Igaz-e hogy $G^p = V(\mathbb{F}_pG)^p \cap G$? Az előző eredmények következményeként bebizonyítjuk:

Következmény. *Legyen $p > 2$ és G p-csoport, p-rendű Frattini részcsoporttal. Ekkor*

$$G^p = V(\mathbb{F}_pG)^p \cap G.$$

Berger, Kovács és Newman [8] leírták azokat a G véges p-csoportokat, melyek Frattini részcsoportja ciklikus. Ez és a normalizált egységcsoport struktúrájára vonatkozó eddigi eredményeink lehetővé tették a következő tétel bizonyítását:

Tétel. *Legyen G és H p-csoport ($p > 2$) ciklikus Frattini részcsoporttal. Ekkor $V(\mathbb{F}_pG)$ izomorf $V(\mathbb{F}_pH)$ akkor és csak akkor, ha G és a H izomorfak.*

Az értekezés negyedik fejezetében a csoportalgebra multiplikatív filtrációs bázisát vizsgáljuk p karakterisztikájú $\mathbb{F}$ testek felett, melyet 1965-ben Kupisch vezetett be.

Legyen A egy véges dimenziós algebra az $\mathbb{F}$ test felett, melynek $rad(A)$ a Jacobson radikálja és B az algebra $\mathbb{F}$ test feletti bázisa. Tegyük fel, hogy a B bázis a következő tulajdonságú:

1. ha $u, v \in B$, akkor vagy $u \cdot v = 0$ vagy $u \cdot v \in B$,
2. $B \cap rad(A)$ a $rad(A)$ radikál egy $\mathbb{F}$-bázisa.

Az ilyen B bázist az A algebra *multiplikatív filtrációs $\mathbb{F}$-bázisának* nevezzük.

A multiplikatív filtrációs bázis jelentőségét Bautista, Gabriel, Roiter, és Salmeron [7] reprezentációelméleti vizsgálatai adták meg. Bebizonyították, hogy ha egy algebrailag zárt $\mathbb{F}$ test felett az A algebrának csak véges sok felbonthatatlan reprezentációja van, akkor A-nak van multiplikatív filtrációs $\mathbb{F}$-bázisa. A problémát, hogy az $\mathbb{F}G$ csoportalgebrának mikor létezik multiplikatív filtrációs bázisa Bautista, Gabriel, Roiter, és Salmeron vetették fel [7] cikkükben.

Csoportalgebrák esetében Higman [30] bebizonyította, hogy az $\mathbb{F}G$ csoportalgebra véges reprezentáció típusú akkor és csak akkor, ha az $\mathbb{F}$ test karakterisztikája p és G Sylow p-csoportjai ciklikusak.

Landrock és Michler [38] 1978-ban megmutatták, hogy a legkisebb Janko csoport csoportalgebrája 2 karakterisztikájú test felett nem tartalmaz multiplikatív filtrációs $\mathbb{F}$-bázist. 1987-ben Parisnak [40] sikerült példát adnia olyan nem kommutatív $\mathbb{F}G$ csoportalgebrára, melynek van multiplikatív filtrációs $\mathbb{F}$-bázisa.

A multiplikatív filtrációs bázis szisztematikus tanulmányozása Bódi dolgozataiban található meg. A [16] és [17] cikkekben megadta az összes metaciklikus csoportot, amely csoportalgebrája tartalmaz multiplikatív filtrációs bázist, továbbá az összes olyan p^m-rendű csoportot, amely tartalmaz p^{m-2}-rendű ciklikus részcsoportot, és a csoportalgebrája tartalmaz multiplikatív filtrációs bázist. Bebizonyította továbbá, hogy a hatványteljes, azaz powerful csoportok csoportalgebrái nem tartalmaznak ilyen bázist.

Ezen kutatásokhoz kapcsolódva a negyedik fejezetben megadjuk az összes olyan p^5-nél kisebb rendű p-csoportot, amely csoportalgebrájának van multiplikatív filtrációs $\mathbb{F}$-bázisa, és megadjuk a bázist is:

Tétel. *Legyen G egy nem Abel p-csoport, melynek a rendje kisebb vagy egyenlő mint p^4 és $\mathbb{F}$ egy p karakterisztikájú test. Az $\mathbb{F}G$ csoportalgebrának akkor és csak akkor van multiplikatív filtrációs $\mathbb{F}$-bázisa, ha G egybeesik a következő csoportok egyikével:*

1. *8-ad vagy 16-od rendű D_n diédercsoport,*

2. *Q_8 nyolcadrendű kvaterniócsoport vagy Q_8 és a C_2 másodrendű ciklikus csoport direkt szorzata és $\mathbb{F}$ tartalmaz primitív harmadik egységgyököt,*

3. *D_8 nyolcadrendű diédercsoport és a C_2 másodrendű ciklikus csoport direkt szorzata, vagy D_8 és a C_4 negyedrendű ciklikus csoport centrális szorzata,*

4.

$$H_{16} = \langle\ a, c\ \mid\ a^4 = b^2 = c^2 = 1,\ (a,b) = 1, (a,c) = b, \\ (b,c) = 1\ \rangle.$$

Ennek a következménye, hogy $\mathbb{F}G$-ben, ahol G teljesíti az előző tétel feltételeit, filtrációs bázis csak akkor létezik, ha $p = 2$.

Teljes leírást adunk az összes 2^5-rendű csoportok csoportalgebráiról, amelyek tartalmaznak multiplikatív filtrációs bázist. A vizsgálathoz felhasználtuk a GAP [28] computer algebrai rendszert és a LAGUNA [18] csomagját. A tételben a csoportok felsorolásában szereplő indexek megegyeznek a GAP csoportazonosító sorszámával.

Tétel. *Legyen G egy 2^5-rendű nem Abel 2-csoport és $\mathbb{F}$ egy 2 karakterisztikájú test. Ekkor az $\mathbb{F}G$ csoportalgebrának akkor és csak akkor van multiplikatív filtrációs $\mathbb{F}$-bázisa, ha G a következő csoportok valamelyike:*

1. $G_{25} = D_8 \times C_4$, $G_{46} = D_8 \times C_2 \times C_2$, $G_{39} = D_{16} \times C_2$ *vagy* $G_{18} = D_{32}$;

2. $G_{26} = Q_8 \times C_4$, *vagy* $G_{47} = Q_8 \times C_2 \times C_2$ *és* $\mathbb{F}$ *tartalmaz primitív harmadik egységgyököt;*

3. $G_{22} = H_{16} \times C_2$, *ahol* H_{16} *az előző tételben definiált;*

4. $G_{48} = (D_8 \curlyvee C_4) \times C_2$, *ahol* $\curlyvee$ *centrális szorzást jelöl;*

5.

$$G_2 = \langle\ a, b \mid a^4 = b^4 = c^2 = 1,\ (a,b) = c,\ (a,c) = 1,\ (b,c) = 1\ \rangle;$$
$$G_5 = \langle\ a, b \mid a^8 = b^2 = c^2 = 1,\ (a,b) = c,\ (a,c) = (b,c) = 1\ \rangle;$$
$$G_7 = \langle\ a, b, c \mid a^8 = b^2 = c^2 = 1,\ (a,c) = a^4,\ (a,b) = a^4c,\ (b,c) = 1\ \rangle;$$
$$G_8 = \langle\ a, b, c \mid a^8 = c^2 = 1,\ b^2 = a^4,\ (a,c) = a^4,\ (a,b) = a^4c,\ (b,c) = 1\ \rangle;$$
$$G_9 = \langle\ a, b, c \mid a^2 = b^8 = c^2 = 1,\ (b,c) = ab^6,\ (a,c) = (a,b) = 1\ \rangle;$$
$$G_{10} = \langle\ a, b, c \mid a^8 = b^4 = c^2 = 1,\ a^4 = b^2,\ (a,b) = a^6c,\ (a,c) = (b,c) = 1\ \rangle;$$
$$G_{11} = \langle\ a, b, c \mid a^4 = b^4 = c^2 = 1,\ (b,c) = ab^2,\ (a,c) = (a,b) = 1\ \rangle;$$
$$G_{49} = \langle\ a, b, c, d \mid a^4 = 1,\ b^2 = c^2 = d^2 = a^2,\ (a,b) = a^2,\ (c,d) = a^2,\ (a,c) = (a,d) = (b,c) = (b,d) = 1\ \rangle.$$

Ezenkívül bebizonyítottuk 2-csoportokra a következő tételt:

Tétel. *Legyen $\mathbb{F}$ kettő karakterisztikájú test.*

1. *Ha*

$$G = \langle\ a, b \mid a^{2^n} = b^2 = c^2 = d^2 = 1,\ (a,b) = c,\ (a,c) = d,\ (a,d) = (b,c) = (b,d) = (c,d) = 1\ \rangle,$$

ahol $n > 1$, akkor az $\mathbb{F}G$ csoportalgebrának nincs multiplikatív filtrációs $\mathbb{F}$-bázisa.

2. *Ha*

$$G = \langle\ a, b \mid a^{2^n} = b^{2^m} = c^2 = 1,\ (a,b) = c,\ (a,c) = 1,\ (b,c) = 1\ \rangle,$$

ahol $n, m \geq 2$, akkor az $\mathbb{F}G$ csoportalgebrának van multiplikatív filtrációs $\mathbb{F}$-bázisa.

Bibliography

[1] V. Artamonov and A. Bovdi, *Integral group rings: group of invertible elements and classical k-theory.*, Itogi Nauki i Tekhniki, Algebra. Topology. Geometry. **27** (1989), 3–43.

[2] C. Baginski, *Groups of units of modular group algebras*, Proc. Amer. Math. Soc. **101** (1987), no. 4, 619–624.

[3] ———, *Modular group algebras of 2-groups of maximal class*, Comm. algebra **20** (1992), no. 5, 1229–1241.

[4] Zs. Balogh, *On existing of filtered multiplicative bases in group algebras*, Acta Acad. Paed. Nyíregyháziensis **20** (2004), 11–30.

[5] Zs. Balogh and A. Bovdi, *Group algebras with unit group of class p*, Publ. Math. Debrecen **65** (2004), no. 3-4, 261–268.

[6] ———, *On units of group algebras of 2-groups of maximal class*, Comm. Algebra **32** (2004), no. 8, 3227–3245.

[7] R. Bautista, P. Gabriel, A. V. Roiter, and L. Salmeron, *Representation-finite algebras and multiplicative bases*, Invent. Math. **81** (1985), no. 2, 217–285.

[8] T. R. Berger, L. G. Kovács, and M. F. Newman, *Groups of prime power order with cyclic Frattini subgroup*, Nederl. Akad. Wetensch. Indag. Math. **42** (1980), no. 1, 13–18.

[9] S. D. Berman, *Group algebras of countable abelian p-group*, Publ. Math. Debrecen **14** (1967), 365–405.

[10] N. Blackburn, *On prime-power groups with two generators*, Proc. Camb. Philos. Soc. **54** (1958), 327–337.

[11] A. Bovdi, *The group of units of a group algebra of characteristic p*, Publ. Math. Debrecen **52** (1998), no. 1–2, 193–244.

[12] A. Bovdi and I. I. Khripta, *Generalized Lie nilpotent group rings*, Mat. Sb. **129** (1986), no. 1, 154–158.

[13] A. Bovdi and J. Kurdics, *Lie properties of the group algebra and the nilpotency class of the group of units*, J. Algebra **212** (1999), no. 1, 28–64.

[14] A. Bovdi and C. Polcino Milies, *Normal subgroups of the group of units in group rings of torsion groups*, Publ. Math. Debrecen **59** (2001), no. 1–2, 235–242.

[15] A. A. Bovdi and A. Sakach, *The unitary subgroup of the multiplicative group of the modular group algebra of a finite alelian p-group*, Math. Zametki **45** (1989), no. 6, 23–29.

[16] V. Bovdi, *On a filtered multiplicative bases of group algebras*, Arch. Math. (Basel) **74** (2000), no. 2, 81–88.

[17] ———, *On a filtered multiplicative bases of group algebras II.*, Algebr. Represent. Theory **6** (2003), no. 3, 353–368.

[18] V Bovdi, A. B. Konovalov, A. R. Rossmanith, and Cs. Schneider, *Laguna — Lie AlGebras and UNits of group Algebras. (http://ukrgap.exponenta.ru/ laguna.htm)*, Version 3.0, 2003.

[19] V. Bovdi, L. G. Kovács, and S. K. Sehgal, *Symmetric units in modular group algebras*, Comm. Algebra **24** (1996), no. 3, 803–808.

[20] V. Bovdi and A. L. Rosa, *On the order of the unitary subgroup of a modular group algebra*, Comm. Algebra **28** (2000), no. 4, 1897–1905.

[21] V. Bovdi and T. Rozgonyi, *On the unitary subgroup of modular group algebras*, Acta Acad. Paedagogicae Nyíregyháza **13/D** (1992), 13–17.

[22] A. Bovdi (Bódi B.), *Bevezetés a csoportgyűrűk elméletébe*, Kossuth Egyetemi Kiadó, Debrecen, 1996.

[23] R. Brauer, *Zur Darstellungstheorie der Gruppen endlicher Ordnung*, Math. Z. **63** (1956), 406–444.

[24] G. L. Carns and C. Y. Chao, *On the radical of the group algebra of a p-group over a modular field*, Proc. Amer. Math. Soc. **33** (1972), 323–328.

[25] D. B. Coleman and D. S. Passman, *Units in modular group rings*, Proc Amer. Math. Soc. **25** (1970), 510–512.

[26] W. E. Deskins, *Finite abelian groups with isomorphic group algebras*, Duke Math. J. **23** (1956), 35–40.

[27] X. Du, *The centers of a radical ring*, Canad. Math. Bull. **35** (1992), no. 2, 174–179.

[28] The GAP Group, *Gap — Groups, Algorithms, and Programming, Version 4.2 (http://www.gap-system.org)*, Aachen, St. Andrews, 1999.

[29] M. Hall, *The theory of groups*, The Macmillan Co., New-York, 1959.

[30] G. Higman, *The units of group-rings*, Proc. London Math. Soc. **46** (1940), 231–248.

[31] E. T. Hill, *The annihilator of radical powers in the modular group ring of a p-group*, Proc. Amer. Math. Soc. **25** (1970), 811–815.

[32] B. Huppert, *Endliche gruppen I.*, Springer-Verlag, Berlin-New York, 1967.

[33] B. Huppert and N. Blackburn, *Finite groups. II.*, Springer-Verlag, Berlin-New-York, 1982.

[34] S. A. Jennings, *The structure of the group ring of a p-group over a modular field*, Trans. Amer. Math. Soc. **50** (1941), 175–185.

[35] D. L. Johnson, *The modular group-ring of a finite p-group*, Proc. Amer. Math. Soc. **68** (1978), no. 1, 19–22.

[36] I. I. Khripta, *The nilpotency of the multiplicative group of a group ring*, Mat. Zametki **11** (1972), 191–200.

[37] H. Kupisch, *Symmetrische Algebren mit endlich vielen unzerlegbaren Darstellungen. I.*, J. Reine Angew. Math. **219** (1965), 1–25.

[38] P. Landrock and G. O. Michler, *Block structure of the smallest janko group*, Math. Ann. **232** (1978), no. 3, 205–238.

[39] A. Mann and A. Shalev, *The nilpotency class of the unit group of a modular group algebra, II.*, Israel J. Math. **70** (1990), no. 3, 267–277.

[40] L. Paris, *Some examples of group algebras without filtered multiplicative basis*, Enseign. Math. **33** (1987), no. 3–4, 307–314.

[41] D. S. Passman, *Algebraic structure of group rings*, Interscience, New-York, 1977.

[42] R. Sandling, *The isomorphism problem for group rings: a survey*, Lecture Notes in Math. **1142** (1985), 258–288.

[43] A. Shalev, *The nilpotency class of the unit group of a modular group algebra I.*, Israel. J. Math. **70** (1990), no. 3, 257–266.

List of papers of the author

1. Zs. Balogh, *On existing of filtered multiplicative bases in group algebras*, Acta Acad. Paed. Nyíregyháziensis **20** (2004), 11 – 30.

2. Zs. Balogh and A. Bovdi, *On units of group algebras of 2-groups of maximal class*, Comm. Algebra **32** (2004), no. 8, 3227 – 3245.

3. Zs. Balogh and A. Bovdi, *Group algebras with unit group of class p*, Publ. Math. Debrecen **65** (2004), no. 3 – 4, 261 – 268.

List of conference talks of the author

1. Balogh Zs., *Csoportalgebrák normalizált egységcsoportjának izomorfia problémája*, Magyar Tudományos Akadémia Szegedi Központja, 1998.

2. Balogh, Zs., *Isomorphism problem of the normalized group of units of group algebras*, Konstanca (România), 2000.

3. Balogh Zs., *Csoportalgebrák multiplikatív filtrációs bázisa*, Gödöllő, 2001.

4. Balogh Zs., *Csoportalgebrák normalizált egységcsoportja*, Nyíregyháza, 2003.

5. Balogh Zs., *Csoportalgebrák egységcsoportjának szerkezete* Rényi Alfréd Matematika Kutatóintézet, 2004.

Filtered multiplicative basis and group of units of group algebra

Értekezés a doktori (PhD) fokozat megszerzése érdekében
a Matematika tudományágban

Írta: Balogh Zsolt Ádám okleveles matematikus

Készült a Debreceni Egyetem Matematika és számítástudományok
doktori iskolája
(Csoportalgebrák és alkalmazásai) keretében

Témavezető: Dr. Bódi Béla

A doktori szigorlati bizottság:

elnök:	Dr. ....
tagok:	Dr. ....
	Dr. ....

A doktori szigorlat időpontja: 200 .. ..

Az értekezés bírálói:

Dr. ....
Dr. ....
Dr. ....

A bírálóbizottság:

elnök:	Dr. ....
tagok:	Dr. ....
	Dr. ....
	Dr. ....
	Dr. ....

Az értekezés védésének időpontja: 200 .. ..