STRUCTURE AND ISOMORPHISM OF SOME CLASSES FINITE DIMENSIONAL COMMUTATIVE SEMI-SIMPLE ALGEBRAS

YORDAN Y. EPITROPOV, TODOR ZH. MOLLOV, NAKO A. NACHEV

ABSTRACT: *Let p be a prime and F be a field of characteristic, different from p. In the present paper we define the concept p-cyclotomic algebra over the field F of characteristic, different from p. We examine, up to isomorphism, the structure of the finite-dimensional commutative semi-simple p-cyclotomic algebras over F. We discover necessary and sufficient conditions for an algebra over F to be isomorphic as an F-algebra of a finite-dimensional commutative p-cyclotomic algebra over F. We give a criterion when an algebra over a field F of characteristic, different from p, can be represented as a group algebra of a finite abelian p-group over F.*

KEYWORDS: *Commutative semi-simple algebra, Commutative group algebra, Finite abelian p-group*

Mathematics Subject Classification 2000: *16S34, 20C05*

1. Structure and isomorphism of finite-dimensional commutative semi-simple p-cyclotomic algebras

Let p be a prime, F be field of characteristic, different from p and let ε_j be a primitive p^j-th root of the unit in algebraic closure of F, where j is a non-negative integer. With $F(\varepsilon_i)$ we denote the extension of the field F with ε_i. Then the condition $F \subseteq F(\varepsilon_1) \subseteq ... \subseteq F(\varepsilon_n) \subseteq ...$ is satisfied.

Following S. Berman [1], we call the field F a *field of the second kind with respect to the prime p*, if the degree of the extension

$F(\varepsilon_1, \varepsilon_2, ...)$ of F is finite, i.e. if $(F(\varepsilon_1, \varepsilon_2, ...) : F) < \infty$. Otherwise we will call F a *field of the first kind with respect to* p. G. Karpilovsky shows [3], that if F is a field of the second kind with respect to p and (i) p is odd, then $F(\varepsilon_j) = F(\varepsilon_1)$ for every natural number j; (ii) if $p = 2$, then $F(\varepsilon_j) = F(\varepsilon_2)$ for every natural number $j \geq 2$.

If F is a field of the first kind with respect to p, then there exists a natural m, which is called a *constant of the field* F *with respect to* p [1], such that $F(\varepsilon_q) = F(\varepsilon_{q+1}) = ... = F(\varepsilon_m) \subset F(\varepsilon_{m+1}) \subset ...$ is fulfilled, where $q = 1$ for $p \neq 2$ and $q = 2$ for $p = 2$. If F is a field of the first kind with respect to p with constant m, then $F(\varepsilon_i)$ is a field of the first kind with respect to p with constant i for $i \geq m$ and with constant m for $i < m$ with respect to p.

For fields of the second kind with respect to p we put the constant $m = \infty$.

If F is a field of characteristic, different from the prime p, then Mollov [5] introduces the concept spectrum of the field F with respect to p and he gives the following definition: if F is a field and p is a prime, then the set

$$s_p(F) = \{ i \in \mathbb{N}_0 \,|\, F(\varepsilon_i) \neq F(\varepsilon_{i+1}) \}$$

is called a *spectrum of the field* F *with respect to* p.

When F is a field of the first kind with respect to p with constant f then, for the spectrum of F the following holds [5]: 1) if $p \neq 2$ and $F \neq F(\varepsilon_1)$, then $s_p(F) = \{0, m, m+1, ...\}$; 2) if $p \neq 2$

and $F = F(\varepsilon_1)$ or if $p = 2$ and $F = F(\varepsilon_2)$, then $s_p(F) = \{m, m+1, ...\}$; 3) if $p = 2$ and $F \neq F(\varepsilon_2)$, then $s_p(F) = \{1, m, m+1, ...\}$.

When F is a field of the second kind with respect to p, then we have $F \subseteq F(\varepsilon_1) = F(\varepsilon_2) = ...$ for $p \neq 2$ and $F = F(\varepsilon_1) \subseteq F(\varepsilon_2) = F(\varepsilon_3) = ...$ for $p = 2$. Then the spectrum of the field F of the second kind is: 1) $s_p(F) = \varnothing$ for 1.1) $p \neq 2$ and $F = F(\varepsilon_1)$ or 1.2) for $p = 2$ and $F = F(\varepsilon_2)$; 2) $s_p(F) = \{ 0 \}$ for $p \neq 2$ and $F \neq F(\varepsilon_1)$; 3) $s_p(F) = \{ 1 \}$ for $p = 2$ and $F \neq F(\varepsilon_2)$.

Definition 1.1 . Let p be a prime, F be a field of characteristic, different from p and let L be an extension of F. The field L is called p*-cyclotomic extension of the field* F, if it is obtained from F by joining only of p^i-th roots of the unit ($i \in \mathbb{N}$).

Definition 1.2 . Let p be a prime, F be a field of characteristic, different from p and let A be an algebra over F. The algebra A is called a p*-cyclotomic algebra over the field* F, if every field, which is contained in A, is p-cyclotomic extension of the field F.

We will show some elementary examples of p-cyclotomic algebras. Namely, let the field L be a p-cyclotomic extension of F (in particular $L = F$). Then:

1) the field L is a p-cyclotomic F-algebra;

2) the group algebra LG of an abelian p-group G over L is a p-cyclotomic F-algebra and a p-cyclotomic L-algebra;

3) the ring $L[x_1, x_2, ..., x_n, ...]$ of the polynomials of $x_1, x_2, ..., x_n, ...$ over L is a p-cyclotomic F-algebra and a p-cyclotomic L-algebra;

4) the direct sum of p-cyclotomic F-algebras is a p-cyclotomic F-algebra.

Theorem 1.1 (Structure). *Let p be a prime, F be a field of characteristic, different from p, and let F be a field of the second kind with respect to the prime p. Let A be finite-dimensional commutative semi-simple p-cyclotomic algebra over the field F. Then*

(1.1) $$A \cong F \oplus ... \oplus F \oplus F(\varepsilon_2) \oplus ... \oplus F(\varepsilon_2),$$

holds where ε_2 is a primitive p^2-th root of 1.

Proof. Let $\dim_F A = n$ ($n \in \mathbb{N}$). According to the structural theorem of Wedderburn [6], applied to the finite-dimensional semi-simple algebra A over the field F, we obtain

$$A \cong M_{n_1}(D_1) \oplus M_{n_2}(D_2) \oplus ... \oplus M_{n_s}(D_s),$$

where $\sum_{i=1}^{s} \dim_F D_i = \sum_{i=1}^{s} n_i^2 = n$ and D_i are algebras with division over the field F for $i = 1,2,...,s$. Since A is a commutative algebra, then $M_{n_i}(D_i)$ are commutative algebras. Therefore $n_i = 1$ for every $i = 1,2,...,s$. Besides, the algebras D_i have to be commutative for every $i = 1,2,...,s$. Therefore they are fields. Since A is a p-cyclotomic algebra over the field F, then the fields D_i are p-cyclotomic extensions of F. Since F is a field of the second kind with respect to the prime p, then the possible p-cyclotomic extensions of the field F are either of the kind F, or of the kind $F(\varepsilon_2)$. #

Definition 1.3. Let p be a prime, F be a field of characteristic, different from p, and let F be a field of the second kind with respect to the prime p. Let A be finite-dimensional commutative semi-simple p-cyclotomic algebra over the field F. The number r_A of the direct summands F in the decomposition (1.1) we will call *real cardinality of* A.

Further the direct sum of n fields F ($n \in \mathbb{N}$) is denoted by nF.

If F is a field of the second kind with respect to the prime p and A is a finite-dimensional commutative semi-simple p-cyclotomic algebra over F, then we can change (1.1) the following way.

1) if 1.1) $p \neq 2$ and $F = F(\varepsilon_1)$ or if 1.2) $p = 2$ and $F = F(\varepsilon_2)$, then $A \cong \lambda_0 F$, $\lambda_0 \in \mathbb{N}_0$.

2) if $p \neq 2$ and $F \neq F(\varepsilon_1)$, then $A \cong \lambda_0 F \oplus \lambda_1 F(\varepsilon_1)$, $\lambda_i \in \mathbb{N}_0$.

3) if $p = 2$ and $F \neq F(\varepsilon_2)$, then $A \cong \lambda_0 F \oplus \lambda_2 F(\varepsilon_2)$, $\lambda_i \in \mathbb{N}_0$.

This commentary gives us the possibility to give the following definition.

Definition 1.4. Let A be a finite-dimensional commutative semi-simple p-cyclotomic algebra over the field F of the second kind with respect to the prime p. A *characteristic system of* A we will call the systems $\{\lambda_0\}$ in case 1); $\{\lambda_0, \lambda_1\}$ in case 2); $\{\lambda_0, \lambda_2\}$ in case 3).

Proposition 1.2 (Isomorphism). *If A is a finite-dimensional commutative semi-simple p-cyclotomic algebra over the field F of characteristic, different from the prime p and F is of the second kind with respect to p and B is an arbitrary F-algebra, then $B \cong A$ as F-algebras if and only if B is a finite-dimensional commutative semi-simple p-cyclotomic algebra over F and the characteristic systems of A and B coincide.*

Proof. Obviously $B \cong A$ as F-algebras if and only if B is an finite-dimensional commutative semi-simple p-cyclotomic algebra over F. Further, the proof follows from Definition 1.4 and the three cases of the commentary of Definition 1.3. #

Proposition 1.2. can be expressed in the following equivalent form:

Proposition 1.3 (Isomorphism). *If A is a finite-dimensional commutative semi-simple p-cyclotomic algebra over the field F of the second kind with respect to the prime p and B is an arbitrary F-algebra, then $B \cong A$ as F-algebras if and only if all of the following conditions are fulfilled:*

(i) *B is a finite-dimensional commutative semi-simple p-cyclotomic algebra over F;*

(ii) $\dim_F B = \dim_F A$;

(iii) $r_B = r_A$.

Proof. When F is a field of the second kind with respect to p, then the characteristic system of A determines uniquely the invariants $\dim_F A$ and r_A and vice versa. #

Theorem 1.4 (Structure). *Let F be a field of characteristic,* *different from the prime p, and let F be of the first kind with respect to p and let A be a finite-dimensional commutative semi-simple p-cyclotomic algebra over F. Then the following direct decomposition holds*

$$A \cong \dot{\sum_{i \in s_p(F)}} \lambda_i F(\varepsilon_i),\ \lambda_i \in \mathbb{N}_0, \tag{1.2}$$

where only a finite number of numbers λ_i are different from 0.

The proof is analogous to the proof of Theorem 1.1.

Definition 1.5. Let A be a finite-dimensional commutative semi-simple p-cyclotomic algebra over the field F of the first kind with respect to the prime p. The system $\{\lambda_i | i \in s_p(F)\}$, where λ_i are the numbers from (1.2) we call *characteristic system of* A.

Proposition 1.5 (Isomorphism). *If A is a finite-dimensional commutative semi-simple p-cyclotomic algebra over the field F of characteristic, different from the prime p, F is a field of the first kind with respect to p and B is an arbitrary F-algebra, then $B \cong A$ as F-algebras if and only if B is a finite-dimensional commutative semi-simple p-cyclotomic algebra over F and the characteristic systems of A and B coincide.*

Proof. Obviously $B \cong A$ as F-algebras if and only if B is a finite-dimensional commutative semi-simple p-cyclotomic algebra over the field F. Further, the proof follows from Definition 1.5 and Theorem 1.4. #

Since the field F of characteristic, different from the prime p, is either of the first kind or of the second kind with respect to p, then Theorems 1.2 and 1.5 give the following general result:

Theorem 1.6 (Isomorphism). *If A is a finite-dimensional commutative semi-simple p-cyclotomic algebra over the field F with characteristic, different from the prime p, and B is an arbitrary F-algebra, then $B \cong A$ as F-algebras if and only if B is a finite-dimensional commutative semi-simple p-cyclotomic algebra over F and the characteristic systems of A and B coincide.*

If G is a finite abelian p-group, F is a field of characteristic, different from p, then FG is a finite-dimensional commutative semi-simple algebra and, according to Example 2, is a p-cyclotomic F-algebra. We will denote by r_{FG} the real cardinality of the F-algebra FG. Furthermore, if G is a finite abelian p-group, we will denote $G[p^i] = \left\{ g \in G \;\middle|\; g^{p^i} = 1 \right\}$, $i \in \mathbb{N}_0$.

Lemma 1 of Mollov [4] is in fact a structural theorem for a group algebra of a finite abelian p-group and can be formulated the following way:

Theorem 1.7 (Structure). *If G is a finite abelian p-group and F is a field of the first kind with respect to p, then*

$$FG \cong \dot{\sum_{i \in s_p(F)}} \lambda_i F(\varepsilon_i),$$

where

$$\lambda_i = \begin{cases} \dfrac{\left|G[p^i]\right| - \left|G[p^j]\right|}{\left(F(\varepsilon_i) : F\right)} & \text{if } \; i \neq i_0, \\ \left|G[p^{i_0}]\right| & \text{if } \; i = i_0, \end{cases} \qquad (1.3)$$

i_0 is the smallest number of $s_p(F)$ and j is the maximal number of $s_p(F)$, which is less than i.

2. Some group-theoretic results

In this Section we shall prove some results for finite abelian p-groups, where p is a prime. If G is abelian p-group, then the sets $G^{p^i} = \{g^{p^i} | g \in G\}$ and $G[p^i] = \{g \in G | g^{p^i} = 1\}$ are subgroups of the group G for every $i \in \mathbb{N}_0$, where N_0 is the set of non-negative integer. For those subgroups we have

(2.1) $$G^{p^{i+1}} \le G^{p^i} \quad \texttt{and} \quad G[p^i] \le G[p^{i+1}].$$

If G is finite then there exists a natural number k, such that $G^{p^k} = 1$. Let k be the smallest number with this property. Then we shall call the number p^k *exponent of the group* G and we shall denote it with $\exp G$. The inclusions in (2.1) are strong if and only if $p^i < \exp G$.

Consider the factor-groups $G^{p^{i-1}}[p]/G^{p^i}[p]$ for each $i \in N$. These factor-groups are elementary abelian p-groups and therefore they are linear spaces over the Galois field $GF(p)$. Put

$$\alpha_i = \dim_{GF(p)}\left(G^{p^{i-1}}[p]/G^{p^i}[p]\right),\ i \in N.$$

The number α_i is called *i-th Ulm-Kaplansky invariant of the group* G and is denoted by $f_i(G)$. Let $r(G)$ be the rank of the abelian p-group G [2]. Then it holds $f_i(G) = r\left(G^{p^{i-1}}[p]/G^{p^i}[p]\right)$, $i \in N$. Therefore, $f_i(G)$ is the number of direct factors of order p^i in the direct decomposition of G of cyclic p-subgroups. For the finite abelian p-group G the Ulm-Kaplansky invariants form a complete system of invariants and therefore they define the group G up to isomorphism. For infinite abelian p-groups the Ulm-Kaplansky invariants are determined the same way, namely i are ordinal numbers. The largest class of abelian p-groups, for which the Ulm-Kaplansky invariants form a complete system of invariants, are the totally-projective groups. For groups outside of this class this is not the case.

For the finite abelian p-groups the Ulm-Kaplansky invariants not only do form a complete system of invariants, but they are also independent of each other. That means that if we chose $\alpha_1, \alpha_2, ..., \alpha_n$ to be arbitrary non-negative integers then there shall exists a finite abelian p-group G, for which the chosen numbers shall be the Ulm-Kaplansky invariants of G. This group is unique up to isomorphism and for $\alpha_n \neq 0$ we have $\exp G = p^n$. For infinite abelian p-groups the case is different.

Put

(2.2) $$\left|G\left[p^i\right]\right| = p^{\beta_i} .$$

Lemma 2.1. *As per (2.2) if* $p^i \leq \exp G$*, then* $\beta_i \geq i$*. An equality is achieved if and only if* G *is a cyclic group.*

The proof follows from (2.2) and from the second inequalities of (2.1). #

In the next lemma we shall denote with p^n the exponent of the finite abelian p-group G.

Lemma 2.2. *The numbers* β_i *from (2.2) are determined from the Ulm-Kaplansky invariants by*

(2.3) $$\beta_i = \sum_{j=1}^{i} j\alpha_j + i\sum_{j=i+1}^{n}\alpha_j = \alpha_1 + 2\alpha_2 + \ldots + i\alpha_i + i\alpha_{i+1} + \ldots + i\alpha_n$$

for each $i = 1,2,\ldots,n$ *where* $n = \log_p(\exp G)$.

Proof. Decompose G in a direct product of cyclic p-groups. This decomposition implies a respective decomposition of $G[p^i]$. It contains all cyclic direct factors of G, whose orders do not exceed p^i. When $i < n$ each of the rest of the factors contain exactly one subgroup of order p^i. The number of these factors is equal to $\alpha_{i+1} + \alpha_{i+2} + \ldots + \alpha_n$ and the order of their direct product is p^{is}, where $s = \alpha_{i+1} + \alpha_{i+2} + \ldots + \alpha_n$. The order of the direct product of the cyclic factors of G, whose orders do not exceed p^i is p^t, where $t = \alpha_1 + 2\alpha_2 + \ldots + i\alpha_i$. Then the order of $G[p^i]$ is p^{t+is}, from where (2.3) follows. #

Lemma 2.2 gives an expression of the numbers β_i by α_i. Now we shall find α_i, expressed by β_i.

Lemma 2.3. *For the numbers* α_i *from (2.3) we have*

(2.4) $$\alpha_1 = 2\beta_1 - \beta_2,\ \alpha_i = 2\beta_i - \beta_{i-1} - \beta_{i+1} \text{ for } i = 2,3,\ldots,n-1,$$
$$\alpha_n = \beta_n - \beta_{n-1},\ \alpha_{n+k} = 0 \text{ for } k \in N.$$

The proof of this Lemma has a purely technical character.

We know that in order to exist an abelian p-group with invariants

$\alpha_1, \alpha_2, ..., \alpha_n$, these numbers can be arbitrary non-negative integers. We see from Lemma 2.3 that the numbers $\beta_1, \beta_2, ..., \beta_n$ can not be arbitrary non-negative because some of α_i could obtain negative values. Now we shall establish the conditions which the numbers β_i must satisfy so that there exists a finite abelian p-group G, for which $|G[p^i]| = p^{\beta_i}$, $i = 1, 2, ..., n = \log_p |G|$.

Lemma 2.4. *There exists a finite abelian* p*-group* G *with* $\exp G = p^n$ *and* $|G[p^i]| = p^{\beta_i}$ *if and only if the numbers* $\beta_1, \beta_2, ..., \beta_n$ *satisfy the inequalities*

(2.5) $$\beta_1 \geq \beta_2 - \beta_1 \geq \beta_3 - \beta_2 \geq ... \geq \beta_n - \beta_{n-1} > 0$$

Proof. Let there exists such a group G so that the Ulm-Kaplansky invariants of G are $\alpha_1, \alpha_2, ..., \alpha_n$. Then they shall be determined by the formulas (2.4) of Lemma 2.3. Since the invariants α_i are non-negative integers then (2.4) implies the inequalities (2.5).

Conversely if the inequalities (2.5) are satisfied, then (2.4) determine α_i and we have $\alpha_i \geq 0$ for each $i = 1, 2, ..., n-1$ and $\alpha_n > 0$. Then for the group G, determined by these Ulm-Kaplansky invariants, we have $\exp G = p^n$ and $|G[p^i]| = p^{\beta_i}$, $i = 1, 2, ..., n$. #

For the numbers β_i there is one more inequality, which we will need later.

Lemma 2.5. *If* $1 \leq i < j \leq n$ *and the numbers* β_i, β_j *are from (2.2), then* $i\beta_j \leq j\beta_i$.

The proof of this Lemma has a purely technical character.

Now we shall deduce a criterion that would ensure the existence of a finite abelian p-group G, if only some of the values of $\left|G\left[p^i\right]\right|$ are given. To this aim we shall give the following definitions.

Definition 2.1. Let $m < n$ are natural numbers and let $\beta_m, \beta_{m+1}, ..., \beta_n$ be a system of natural numbers. We shall call this system *normal of the first type* if it satisfies the following inequalities

(2.6) $$\frac{1}{m}\beta_m \geq \beta_{m+1} - \beta_m \geq \beta_{m+2} - \beta_{m+1} \geq ... \geq \beta_n - \beta_{n-1} > 0 .$$

Definition 2.2. Let $m < n$ are natural numbers and let $\beta_1, \beta_m, \beta_{m+1}, ..., \beta_n$ be a system of natural numbers. We shall call this system *normal of the second type* if it satisfies the following inequalities

(2.7) $$\beta_1 \geq \frac{1}{m}\beta_m \geq \beta_{m+1} - \beta_m \geq \beta_{m+2} - \beta_{m+1} \geq ... \geq \beta_n - \beta_{n-1} > 0 .$$

Theorem 2.5. *Let $m < n$ be natural numbers and let a normal system of the first or the second type be given. Then there exists a finite abelian p-group G, such that $\left|G\left[p^i\right]\right| = p^{\beta_i}$, where β_i are the numbers of the given normal system.*

Proof. 1). Let the given normal system be of the first type. From the first inequality in (2.6) we get $(m+1)\beta_m - m\beta_{m+1} \geq 0$. Consequently there exists an abelian p-group A, for which $|A| = p^{(m+1)\beta_m - m\beta_{m+1}}$. Choose A such that $\exp A \leq p^m$. This is possible because the limit of $\exp A$ above does not affect on the choice of A. Let now us make an abelian group B, for which

$\alpha_1 = \alpha_2 = ... = \alpha_m = 0$, $\alpha_i = 2\beta_i - \beta_{i-1} - \beta_{i+1}$ for $i = m+1, m+2, ..., n-1$ when $m+1 < n$, $\alpha_n = \beta_n - \beta_{n-1}$. If $m+1 = n$, then we put $\alpha_i = 0$ for $i \le n-1$. In view of (2.6) these settings are possible. Now let us put $G = A \times B$. It can be immediately verified that the group G satisfies the conditions of the theorem.

2) Now let the normal system be of the second type. From the first two inequalities of (2.7) follows $\beta_1 + \beta_m - \beta_{m+1} \ge 0$. Then there exists an abelian p-group A, for which $|A[p]| = p^{\beta_1 + \beta_m - \beta_{m+1}}$ and $\exp A \le p^m$. The maximum order of such group is p^s, where $s = m(\beta_1 + \beta_m - \beta_{m+1})$. We put $t = (m+1)\beta_m - m\beta_{m+1}$. From the first inequality of (2.7) we have $s \ge t$ and from the second we have $t \ge 0$. Then A can be chosen such that $|A| = p^t$. Further we choose an abelian group B as in case 1). This is possible, because all the inequalities in (2.6) participate in (2.7). Then the group $G = A \times B$ satisfies the required conditions. #

Note. The group G, defined in the proof of Theorem 2.5 is not unique, because A is not determined uniquely. In case 1) A will be unique if and only if in the first inequality of (2.6) we have equality and then we obtain $A = 1$. In case 2) A is unique if and only if in the first two inequalities of (2.7) we have equality and then we obtain $A = 1$.

3. Algebras of the first and the second kind with respect to a prime number

Definition 3.1. Finite-dimensional commutative semi-simple p-cyclotomic F-algebra A is called *algebra of the first kind with respect to* p, if the field F is of the first kind with respect to p and in the direct decomposition of F-algebra A in direct sum of fields

$F(\varepsilon_i)$ participates at least one field $F(\varepsilon_n)$, for which $\lambda_n \neq 0$ and $n > m$, where m is the constant of the field F with respect to p. Otherwise the F-algebra A is called *algebra of the second kind with respect to* p. If A is an algebra of the first kind with respect to p, then the largest number n with the above indicated properties is called the *exponent of* A.

We note that if A is an algebra of the second kind with respect to p over the field F, then F can be either of the first kind or of the second kind with respect to p. Moreover if $p \neq 2$, then in the direct decomposition of this algebra A only fields of the form F and $F(\varepsilon_1)$ will participate. For $p = 2$ these fields will be of the form F and $F(\varepsilon_2)$.

Later we shall use the dimensions of $F(\varepsilon_i)$ over F and we shall determine them now. When $p \neq 2$ we set $d = (F(\varepsilon_1):F)$. Let $d = (F(\varepsilon_2):F)$ for $p = 2$. When $p \neq 2$ we have $d/(p-1)$ and for $p = 2$ we have $d/2$. If $p \neq 2$, then $d = 1$ if and only if $F = F(\varepsilon_1)$. If $p = 2$, then $d = 1$ if and only if $F = F(\varepsilon_2)$ and $d = 2$ if and only if $F \neq F(\varepsilon_2)$. If F is of the first kind with respect to p and $i \geq m$, then $(F(\varepsilon_i):F) = dp^{i-m}$.

Now we can give special direct decompositions of the algebra A, which we will call *canonical*, namely:

1) If the algebra A is of the first kind with respect to p, with exponent n, then the decomposition of A is

(3.1) $$A \cong \lambda_0 F \oplus \lambda_m F(\varepsilon_m) \oplus \ldots \oplus \lambda_n F(\varepsilon_n).$$

2) If A is of the second kind with respect to p, then

(3.2)
$$A \cong \lambda_0 F ,$$

if $d = 1$,

(3.3)
$$A \cong \lambda_0 F \oplus \lambda_1 F(\varepsilon_1),$$

if $p \neq 2$ and $d > 1$,

(3.4)
$$A \cong \lambda_0 F \oplus \lambda_2 F(\varepsilon_2),$$

if $p = d = 2$.

The numbers λ_i, determined respectively in (3.1), (3.2), (3.3) or (3.4), are called *characteristic numbers of* A and we shall say that they form a *characteristic system of* A. These numbers form a complete invariant system of A and determine it up to F-isomorphism.

For an algebra of the first kind with respect to p when $\lambda_m \neq 0$ we shall introduce one more system of numeric invariants. Let us denote

(3.5)
$$\beta_i = \log_p\left(\lambda_0 + d\lambda_m + pd\lambda_{m+1} + \ldots + p^{i-m} d\lambda_i\right),$$
$$i = m, m+1, \ldots, n.$$

For $p = d = 2$ and $\lambda_0 \neq 0$ we set

(3.6)
$$\beta_1 = \log_2 \lambda_0 .$$

Since the numbers $\lambda_0, \lambda_m, \lambda_{m+1}, \ldots, \lambda_n$ are non-negative and $\lambda_m \neq 0$, then the logarithms in (3.5) make sense. This holds also for the logarithm in (3.6).

When $p \neq 2$ or $p = 2 = d + 1$ we say that the numbers (3.5) form a *special characteristic system of* A. When $p = d = 2$ a *special characteristic system of* A form the numbers (3.5) and (3.6).

With the help of the formulas (3.5) and (3.6) the numbers β_i are determined by $\lambda_0, \lambda_m, \lambda_{m+1}, \dots, \lambda_n$.

The numbers λ_i can be determined by the numbers β_i, namely

(3.7)
$$\lambda_m = \frac{p^{\beta_m} - \lambda_0}{d},$$

(3.8)
$$\lambda_i = \frac{p^{\beta_i} - p^{\beta_{i-1}}}{dp^{i-m}} \text{ for } i = m, m+1, \dots, n,$$

and for $p = d = 2$ we have $\lambda_0 = 2^{\beta_1}$. This shows that the special characteristic system, combined with the number λ_0, form a complete invariant system of the algebra A.

For an algebra of the second kind with respect to p we do not determine a special characteristic system.

4. Representation of a F-algebra as a group algebra

Now we shall clarify on when an algebra over a field F of characteristic different from the prime p can be represented as a group algebra of a finite abelian p-group over F. The answer to that question is in the following main result:

Theorem 4.1. *An algebra* A *over a field* F *of characteristic,* *different from the prime* p, *is isomorphic to group algebra* FG *of some finite abelian* p*-group* G *if and only if the following conditions are fulfilled:*

1) A *is a finite-dimensional, commutative, semi-simple and* p*-cyclotomic algebra over* F *;*

2) if A *is of the first kind with respect to* p *with an exponent* n *and the constant of the field* F *with respect to* p *is* m, *then for* $p \neq 2$ *or* $p = 2 = d + 1$ *we have* $\lambda_m \neq 0$, *the special characteristic system of* A *consists of positive integer and is normal of first type and*

$$\lambda_0 = \begin{cases} 0, \text{ if } d = 1, \\ 1, \text{ if } p \neq 2, d > 1 \end{cases}. \tag{4.1}$$

For $p = d = 2$ *we have* $\lambda_0 \neq 0$, *the special characteristic system of* A *consists of positive integers and it is normal of the second type;*

3) If A *is of the second kind with respect to* p, *then*

$$\lambda_0 = p^s,\ s \geq 0 \text{ is integer, if } d = 1; \tag{4.2}$$

$$\lambda_0 = 1,\ \lambda_1 = \frac{p^s - 1}{d},\ s \geq 0 \text{ is integer, if } p \neq 2 \text{ and } d > 1; \tag{4.3}$$

$$\lambda_0 = 2^t,\ \lambda_2 = 2^{s-1} - 2^{t-1}, \text{ if } p = d = 2 \text{ and if } F \text{ is of the first kind, then } 0 \leq t \leq s \leq mt \text{ and if } F \text{ is of the second kind with respect to 2, then } 0 < t \leq s \text{ or } s = t = 0. \tag{4.4}$$

Proof. *Necessity*. Let $A \cong FG$ as F-algebras for some finite abelian p-group G. Then $\dim_F A = |G| < \infty$ and therefore A is finite-dimensional algebra over F. The commutativity of G implies that A is also commutative. Since $charF \neq p$ and G is p-group, then the algebra A is semi-simple. Besides, FG decomposes in a direct sum of fields of the form $F(\varepsilon_i)$. Therefore the algebra A is p-cyclotomic. Thus the conditions in point 1) of the theorem are satisfied.

Let A be of the first kind with respect to p with exponent n and m is a constant of the field F. Based on the isomorphism $A \cong FG$ it follows that A and FG have the same canonical decompositions in direct sum of fields. From the decomposition

(4.5) $$FG \cong \lambda_0 F \oplus \lambda_m F(\varepsilon_m) \oplus \ldots \oplus \lambda_n F(\varepsilon_n),$$

and Theorem 1.7 we have

(4.6) $$\lambda_0 = \begin{cases} 0, \text{ if } d = 1, \\ 1, \text{ if } p \neq 2, d > 1, \\ |G[2]|, \text{ if } p = d = 2, \end{cases} .$$

(4.7) $$\lambda_m = \frac{|G[p^m]| - \lambda_0}{d}, .$$

(4.8) $$\lambda_i = \frac{|G[p^i]| - |G[p^{i-1}]|}{dp^{i-m}} \text{ for } i = m, m+1, \ldots, n.$$

Let $p \neq 2$ or $p = 2 = d + 1$. Since A has exponent n, then the exponent of G is p^n and $m < n$ implies $|G[p^n]| \geq p^m$. Then from (4.7) and the first two cases of (4.6) follows $\lambda_m \geq p^m - 1 > 0$, i.e.

$\lambda_m \neq 0$. The equalities (4.7) and (3.7) imply $|G[p^m]| = p^{\beta_m}$. The equalities (4.8) and (3.8) imply $|G[p^i]| = p^{\beta_i}$ for $i = m, m+1, ..., n$. Since the orders of the groups $G[p^i]$ for $i = m, m+1, ..., n$ are non-trivial degrees of p, then the numbers β_i for $i = m, m+1, ..., n$ are natural. These numbers form the special characteristic system of A. Therefore this system consists entirely of positive integer. From Lemma 2.4 (the proof of necessity) it follows that the numbers β_i satisfy the inequalities of (2.6), except the first one. The first inequality of (2.6) follows from Lemma 2.5 for $i = m$, $j = m+1$. Therefore the special characteristic system of A is normal of the first type. The formula (4.1) follows from the first two cases of (4.6).

Let $p = d = 2$. The third case in formula (4.6) and formula (3.6) implies $|G[2]| = 2^{\beta_1}$. Since $2 \leq m < n$, then the order of $G[2]$ is a nontrivial power of the number 2. Therefore β_1 is a positive integer. Analogically the numbers $\beta_m, \beta_{m+1}, ..., \beta_n$ are non-negative integer and they satisfy the inequalities (2.6), which are the same as the inequalities (2.7), except the first. The first inequality in (2.7) follows from Lemma 2.5 for $i = 1$ and $j = m$. Therefore the system $\beta_1, \beta_m, \beta_{m+1}, ..., \beta_n$ consists of positive integer and is normal system of the second type. This system is also the special characteristic system of A. In this way the requirements in point 2) are proved.

3) Let A is of the second kind with respect to p. Then if F is of the first kind with respect to p and the exponent of G is p^n, then $n \leq m$ and when F is of the second kind then the exponent of G is an arbitrary power of p. Therefore when $p \neq 2$ in the canonical decomposition of FG will participate only the fields F and $F(\varepsilon_1)$ and for $p = 2$ only the fields F and $F(\varepsilon_2)$. For $d = 1$ the

decomposition of FG contains only the field F with coefficient $\lambda_0 = |G| = p^s$, where $s \geq 0$ is an integer. Thus we get formula (4.2).

If $p \neq 2$ and $d > 1$, then the decomposition of FG is $FG \cong F \oplus \frac{|G|-1}{d} F(\varepsilon_1)$ so we have $\lambda_0 = 1$, $\lambda_1 = \frac{p^s - 1}{d}$, where $|G| = p^s$, $s \geq 0$ is integer. Thus we get formula (4.3). For $s = 0$ formula (4.3) is the same as (4.4). This is a trivial case in which $G = 1$.

Let $p = d = 2$. Then the decomposition of FG is

(4.9) $$FG \cong \lambda_0 F \oplus \lambda_2 F(\varepsilon_2),$$

where $\lambda_0 = |G[2]|$ and $\lambda_2 = \frac{|G| - |G[2]|}{2}$. We set $|G[2]| = 2^t$, $|G| = 2^s$. From (4.9) we get (4.4), where for t and s we have to find limiting inequalities. The group G is decomposed in a direct product of t cyclic groups because $|G[2]| = 2^t$. Each of these cyclic groups has an order, not larger from 2^m, since otherwise the algebra A would be of the first kind. Therefore the maximal order of G is 2^{mt}. From here $s \leq mt$ follows. The inequalities $0 \leq t \leq s$ follow from the fact that $G[2]$ is a subgroup of G. If F is of the second kind with respect to p, then we also have $0 \leq t \leq s$, but in this case there is no upper limit for s. However the case $t = 0$ and $s > 0$ leads to a contradiction, because $G[2] = 1$ implies $G = 1$, so this leaves only $0 < t \leq s$ or $s = t = 0$ (a trivial case). In this way we proved point 3) of the necessary conditions.

Sufficiency. Let the conditions 1), 2) and 3) are satisfied. From 1) it follows that A is decomposed in a direct sum of finite number of fields $F(\varepsilon_i)$. We will prove that there exists finite abelian p-group G, such that the canonical decomposition of FG is the same as the decomposition of A.

Let A be of the first kind with respect to p with exponent n and a constant m of the field F. Then 2) implies that the special characteristic system of A exists and consists of positive integer and it is a normal system of the first or the second type. From Theorem 2.5 it follows that there exists a finite abelian p-group G, such that $\left|G[p^i]\right| = p^{\beta_i}$, where β_i are the numbers of the special characteristic system of A. Thus (3.7) and (3.8) imply (4.7) and (4.8) and (3.6) for $p = d = 2$ implies the third case of (4.6). Moreover from (4.1) the first two cases of (4.6) follow. Therefore the algebras A and FG have the same canonical decomposition from which follows the F-isomorphism $A \cong FG$.

Let A be of the second kind with respect to p. If $d = 1$, then for G we can choose an arbitrary finite abelian group of order p^s and so from formula (4.1) we have $A \cong FG$. If $p \neq 2$ and $d > 1$, then for G we choose again an abelian group of order p^s and from (4.3) $A \cong FG$ follows. For $p = d = 2$ we choose an abelian group of order 2^s and $\left|G[2]\right| = 2^t$. If F is of the first kind with respect to p, then we choose the exponent of G to be not greater than p^m. If F is of the second kind with respect to p, then for the exponent of G there are no restrictions. The inequalities (4.4) ensure the existence of such group. Then (4.4) implies $A \cong FG$. Thus the theorem is proven. #

REFERENCES

[1] BERMAN, S., Group algebras of countable abelian p-groups (In Russian), *Publ Math – Debrecen*, **14**, (1967),

365-405. (Zbl 0080.02102)
[2] FUCHS, L., *Infinite abelian groups*, Vol. I and II, Academic Press, (1970 and 1973).
[3] KARPILOVSKY, G., *Unit groups of group rings*, Longman Scientific and Technical, (1989).
[4] MOLLOV, T., Multiplicative groups of semi-simple group algebras (In Russian), *Pliska Stud. Math. Bulgar.*, **8**, (1986), 54-64. (Zbl 0655.16004)
[5] MOLLOV, T., Sylow p-subgroups of the group of the normalized units of semi-simple group algebras of uncountable abelian p-groups (In Russian), *Pliska Stud. Math. Bulgar.*, **8**, (1986), 34-46.
[6] PIERCE, R., *Associative algebras*, Springer, (2012).