The Loewy Structure of Certain Fixpoint Algebras, Part I

T. Breuer, L. Héthelyi, E. Horváth and B. Külshammer

April 1, 2019

Abstract

We investigate the Loewy structure of the fixpoint algebra of the group algebra of the additive group of a finite field F under the action of a subgroup of the multiplicative group of F.

1 Introduction

In [13], B. Külshammer and B. Sambale investigated the Loewy lengths of centers of group algebras of finite groups. In Corollary 5 of [13], they proved:

Proposition 1.1. *Let F be an algebraically closed field of characteristic $p > 0$, let G be a finite group, and let B be a block of the group algebra FG with abelian defect group D. Moreover, suppose that the inertial quotient I of B (a p'-subgroup of $\mathrm{Aut}(D)$) acts semiregularly on $[D, I] \setminus \{1\}$. Then*

$$\mathrm{LL}(\mathrm{Z}(B)) = \mathrm{LL}(\mathrm{Z}(F[D \rtimes I])) = \mathrm{LL}((FD)^I).$$

Here $\mathrm{LL}(A)$ denotes the Loewy length of a finite-dimensional F-algebra A, i.e. the minimal nonnegative integer t such that $\mathrm{J}(A)^t = 0$ where $\mathrm{J}(A)$ is the (Jacobson) radical of A, the largest nilpotent ideal of A. Also, $\mathrm{Z}(A)$ denotes the center of A, $D \rtimes I$ denotes the semidirect product of D and I, and $(FD)^I$ denotes the fixpoint algebra

$$(FD)^I = \{x \in FD : \alpha(x) = x \text{ for all } \alpha \in I\}.$$

Moreover, the proof of Corollary 5 in [13] shows that

$$(FD)^I = F\mathrm{C}_D(I) \otimes_F (F[D, I])^I$$

where $\mathrm{C}_D(I) = \{x \in D : \alpha(x) = x \text{ for all } \alpha \in I\}$ is the fixpoint subgroup, so that

$$\mathrm{LL}((FD)^I) = \mathrm{LL}(F\mathrm{C}_D(I)) + \mathrm{LL}((F[D, I])^I) - 1.$$

The Loewy structure of the group algebra of a finite p-group is well-known by the work of Jennings ([10], see also [9] or [15]). The results above motivate the investigation of the fixpoint algebra $(FP)^H$ where P is a finite abelian p-group and H is a finite p'-group acting on P. Some special cases have been dealt with in [13] and [5]. In this note we generalize several results in these two papers. A related paper is [14].

In Section 2, we will show that the fixpoint algebra $(FP)^H$ is always symmetric, and we are going to construct useful bases of FP and of $(FP)^H$. In Section 3 we will generalize our setup by replacing the prime number p by an arbitrary positive integer $q > 1$. Then the fixpoint algebra $(FP)^H$ is replaced by an algebra $A = A(q, n, e)$ where n, e are positive integers satisfying $e \mid q^n - 1$. The F-algebra A has an F-basis $b_0, \ldots, b_z$ where $z = (q^n - 1)/e$; the corresponding structure constants are either 0 or 1. Similar algebras have been investigated in [6], for example. In Proposition 3.2, we present an inductive method to compute the Loewy structure and, in particular, the Loewy length of $A(q, n, e)$.

In Section 4, we construct an automorphism of $A(q, n, e)$ which is useful in the computation of the Loewy structure of $A(q, n, e)$. In Section 5, we investigate certain isomorphisms between our algebras, for different triples (q, n, e). We also characterize for which parameters the algebra $A(q, n, e)$ is uniserial. In Section 7, we prove upper and lower bounds for the Loewy length of $A(q, n, e)$, as functions of the parameters q, n and e. Here a number-theoretic function $(q, e) \longmapsto m(q, e)$ will become important which we investigate in Section 6. In part II of this paper, we are going to study this function in more detail. We will then see that very often the Loewy length of $A(q, n, e)$ is equal to the upper bound of Theorem 7.1, but we will also construct examples whose Loewy length differs from this upper bound. Throughout, we illustrate our concepts and results by examples.

Algebras with actions of a finite group G, the so-called G-algebras, and the corresponding fixpoint algebras are important in representation theory (see [16], for example). Of course, they also appear in the work of M. Broué (such as [3] and [4]).

2 Fixpoint algebras

In the following, let F be an algebraically closed field of characteristic $p > 0$. We can and will view every finite field of characteristic p as a subfield of F.

Let P be an elementary abelian p-group of order p^n, and let H be a finite p'-group acting on P. We are interested in the Loewy structure of the fixpoint algebra $(FP)^H$. Since $\mathrm{J}(FP)$ and $\mathrm{J}(FP)^2$ are invariant under the action of H, Maschke's Theorem implies that

$$\mathrm{J}(FP) = V \oplus \mathrm{J}(FP)^2$$

where V is an FH-submodule of $\mathrm{J}(FP)$. Moreover, we have isomorphisms

$$V \simeq_{FH} \mathrm{J}(FP)/\mathrm{J}(FP)^2 \simeq_{FH} F \otimes_{\mathbb{F}_p} P$$

where P is considered as an $\mathbb{F}_p H$-module in the usual way. Let $x_1, \ldots, x_n$ be an F-basis of V. Then $x_i^p = 0$ for $i = 1, \ldots, n$, and the monomials

$$x_1^{i_1} \ldots x_n^{i_n} \qquad (0 \leq i_t < p \text{ for } t = 1, \ldots, n)$$

constitute an F-basis of FP, as is well-known and easy to see (cf. Proposition 5.2 in [12], for example).

Proposition 2.1. *With notation as above, the fixpoint algebra $(FP)^H$ is symmetric (and commutative).*

Proof. Obviously, the group algebra FP and its subalgebra $A := (FP)^H$ are commutative. Moreover, it is well-known that the group algebra FP is symmetric with respect to the linear form $\sigma : FP \longrightarrow F$ such that $\sigma(1) = 1$ and $\sigma(y) = 0$ for $1 \neq y \in P$. Note that $\sigma({}^h x) = \sigma(x)$ for $h \in H$, $x \in FP$. The restriction σ' of σ turns A into a symmetric F-algebra; in fact, let $a \in A$ such that $\sigma'(aA) = 0$. Then, for $x \in FP$, we have $x' := \sum_{h \in H} {}^h x \in A$ and

$$0 = \sigma'(ax') = \sum_{h \in H} \sigma(a \cdot {}^h x) = \sum_{h \in H} \sigma({}^h(ax)) = \sum_{h \in H} \sigma(ax) = |H| \sigma(ax).$$

Thus $\sigma(aFP) = 0$ which implies that $a = 0$. The result follows. □

Examples show that Proposition 2.1 does not hold, in general, when we omit the hypothesis $p \nmid |H|$ (see [1], for example).

Now we specialize further and fix a divisor e of $p^n - 1$. Then

$$G := G(p, n, e) := \left\{ \begin{pmatrix} \alpha & 0 \\ \beta & 1 \end{pmatrix} : \alpha, \beta \in \mathbb{F}_{p^n}, \alpha^e = 1 \right\}$$

is a subgroup of $\mathrm{GL}_2(p^n)$ and a semidirect product $G = P \rtimes H$ where P is an elementary abelian p-group of order p^n, and H is a cyclic group of order e acting on P. By Proposition 2.1, the fixpoint algebra

$$A := A(p, n, e) := (FP)^H$$

is symmetric (and commutative). It is well-known that we can choose the basis $x_1, \ldots, x_n$ of V above in such a way that the action of a generator h of H is given by a diagonal matrix with diagonal entries $\zeta, \zeta^p, \zeta^{p^2}, \ldots, \zeta^{p^{n-1}}$ where ζ is a primitive e-th root of unity in F (see Satz II.7.3 in [8], for example). Thus the action of h on the F-basis of FP given by monomials satisfies

$$h \cdot x_1^{i_1} x_2^{i_2} \ldots x_n^{i_n} = \zeta^{i_1 + p i_2 + \ldots + p^{n-1} i_n} x_1^{i_1} x_2^{i_2} \ldots x_n^{i_n}$$

($0 \leq i_t < p$ for $t = 1, \ldots, n$). Hence the monomials $x_1^{i_1} \ldots x_n^{i_n}$ with $0 \leq i_t < p$ for $t = 1, \ldots, n$ and

$$i_1 + pi_2 + \ldots + p^{n-1} i_n \equiv 0 \pmod{e} \qquad (*)$$

constitute an F-basis of $(FP)^H = A$.

It turns out that many properties of A can be proved in somewhat greater generality. We introduce this slightly more general setup in the following section.

3 A more general setup

Let F be an arbitrary field. We fix positive integers q, n, e such that $q > 1$ and $e \mid q^n - 1$. Then we consider the ideal $I := (X_1^q, \ldots, X_n^q)$ of the polynomial algebra $F[X_1, \ldots, X_n]$ and set $x_i := X_i + I \in F[X_1, \ldots, X_n]/I$, so that $x_i^q = 0$ for $i = 1, \ldots, n$. Finally, we define $A := A(q, n, e)$ as the subalgebra of $F[X_1, \ldots, X_n]/I = F[x_1, \ldots, x_n]$ generated by all monomials $x_1^{i_1} x_2^{i_2} \ldots x_n^{i_n}$ such that

$$i_1 + qi_2 + \ldots + q^{n-1} i_n \equiv 0 \pmod{e}. \qquad (*)$$

(When F is algebraically closed of characteristic $p > 0$ and $q = p$ then we get back the algebra at the end of Section 2.) Of course, the monomials $x_1^{i_1} x_2^{i_2} \ldots x_n^{i_n}$ satisfying $(*)$ and $0 \leq i_t < q$ for $t = 1, \ldots, n$ are in bijection with the n-tuples $(i_1, i_2, \ldots, i_n) \in \{0, 1, \ldots, q-1\}^n$ satisfying $(*)$, via their exponent vectors. And these n-tuples are in bijection with the integers in $\{0, 1, \ldots, q^n - 1\}$ which are divisible by e, via the coefficient vectors in their q-adic expansions. These integers are precisely the $1 + z$ numbers $0, e, 2e, \ldots, ze = q^n - 1$ where

$$z := (q^n - 1)/e;$$

in particular, we have $\dim A = 1 + z \geq 2$. For $k = 0, 1, \ldots, z$, we abbreviate the monomial $x_1^{i_1} x_2^{i_2} \ldots x_n^{i_n}$ by b_k where $ke = i_1 + qi_2 + \ldots + q^{n-1} i_n$ is the q-adic expansion of ke. Then $b_0, b_1, \ldots, b_z$ constitute an F-basis of A, and $b_1, \ldots, b_z$ constitute an F-basis of $J := \mathrm{J}(A)$. There is a nice multiplication rule for these basis elements.

Proposition 3.1. *Let $k, l \in \{0, 1, \ldots, z\}$, and suppose that ke and le have q-adic expansions $ke = i_1 + qi_2 + \ldots + q^{n-1} i_n$ and $le = j_1 + qj_2 + \ldots + q^{n-1} j_n$. Then*

$$b_k b_l = \begin{cases} b_{k+l}, & \text{if } i_t + j_t < q \text{ for } t = 1, \ldots, n \\ 0, & \text{otherwise.} \end{cases}$$

In particular, we have $b_0 = 1$, and $\mathrm{S}(A)$, the socle of A, equals Fb_z. Moreover, A is a symmetric F-algebra.

Proof. Since $b_k = x_1^{i_1} \ldots x_n^{i_n}$ and $b_l = x_1^{j_1} \ldots x_n^{j_n}$ we have $b_k b_l = x_1^{i_1 + j_1} \ldots x_n^{i_n + j_n}$. Thus $b_k b_l = 0$ whenever $i_t + j_t \geq q$ for some $t \in \{1, \ldots, n\}$. And, if $i_t + j_t < q$ for $t = 1, \ldots, n$ then

$$(i_1 + j_1) + q(i_2 + j_2) + \ldots + q^{n-1}(i_n + j_n) = ke + le = (k + l)e$$

is the q-adic expansion of $(k+l)e$. Thus $b_k b_l = b_{k+l}$ in this case.

Our multiplication rule implies that $b_0 b_k = b_k$ for $k = 0, 1, \ldots, z$. Thus $b_0 = 1$. Also, we have $b_z b_k = 0$ for $k = 1, \ldots, z$ since $ze = q^n - 1$ has q-adic expansion

$$ze = (q-1) + q(q-1) + \ldots + q^{n-1}(q-1).$$

Thus $b_z \in \mathrm{S}(A)$.

Let $\sigma : A \longrightarrow F$ be the linear map defined by $\sigma(b_z) = 1$ and $\sigma(b_k) = 0$ for $k = 0, 1, \ldots, z-1$. Our multiplication rule implies that $b_k b_{z-k} = b_z$ for $k = 0, 1, \ldots, z$. Thus the elements $b_z, \ldots, b_0$ form an F-basis of A which is dual to the F-basis $b_0, \ldots, b_z$ (with respect to σ). Hence σ is a symmetrizing linear form on A.

Since A is symmetric, we have $\dim \mathrm{S}(A) = \dim A/J = 1$. Thus we conclude that $\mathrm{S}(A) = Fb_z$. □

We note that $b_k b_l = 0$ if there is a carry when we add the q-adic expansions of ke and le, and that $b_k b_l = b_{k+l}$ if there is no such carry.

Example 3.1. Let $(q, n, e) = (11, 2, 15)$, so that $z = (11^2 - 1)/15 = 8$. Since $2e = 30 = 8 + 11 \cdot 2$ and $3e = 45 = 1 + 11 \cdot 4$ we have $b_2 b_2 = 0$ (carry!), but $b_2 b_3 = b_5$ (no carry!).

Proposition 3.1 implies that, for any positive integer $d > 1$, the F-algebras $A(q, n, e)$, where (q, n, e) ranges over the triples of positive integers with $q > 1$, $e \mid q^n - 1$ and $\dim A(q, n, e) = d$, fall into finitely many isomorphism classes. We will have more to say about this in part II of this paper.

Proposition 3.1 gives a straightforward method to compute an F-basis of J^2; it consists of the nonzero products $b_k b_l$ (repetitions removed) with $k, l \in \{1, \ldots, z\}$. The resulting F-basis of J^2 is, of course, a subset of $\{b_1, \ldots, b_z\}$. From this subset, one gets an F-basis of $J^2 \cdot J = J^3$ by taking nonzero products of basis elements again. Continuing in this fashion, we obtain F-bases for the powers of J. This then also provides F-bases of the various Loewy layers J^{i-1}/J^i $(i = 1, \ldots, \mathrm{LL}(A))$.

Example 3.2. Let $(q, n, e) = (3, 4, 5)$, so that $z = 16$. Then we can work out and depict the Loewy structure of A as follows:

b_0	$(0,0,0,0)$
$b_1, b_2, b_3, b_6, b_9, b_{11}$	$(0,0,2,1), (0,1,0,1), (0,2,1,0), (1,0,0,2), (1,0,1,0), (2,1,0,0)$
$b_4, b_5, b_7, b_8, b_{12}, b_{13}, b_{15}$	$(0,1,2,2), (0,2,0,2), (1,1,1,1), (1,2,2,0), (2,0,1,2), (2,0,2,0), (2,2,0,1)$
b_{10}, b_{14}	$(1,2,1,2), (2,1,2,1)$
b_{16}	$(2,2,2,2)$

Thus $\dim A = 17$, $\mathrm{LL}(A) = 5$, and the dimensions of the Loewy layers are recorded by the $\mathrm{LL}(A)$-tuple $[1, 6, 7, 2, 1]$ which we call the *Loewy vector* of A.

Our next result gives a slightly easier way to determine the Loewy structure of A.

Proposition 3.2. *For $k = 0, 1, \ldots, z$, we define $\lambda(k) \in \mathbb{N}_0$ inductively by $\lambda(0) := 0$ and*

$$\lambda(k) := 1 + \max\{\lambda(l) : l \in L_k\} \quad \text{for} \quad k > 0$$

where L_k is the set of integers $l \in \{0, 1, \ldots, k-1\}$ such that the digits in the q-adic expansions $ke = i_1 + qi_2 + \ldots + q^{n-1}i_n$ and $le = j_1 + qj_2 + \ldots + q^{n-1}j_n$ satisfy $i_t \geq j_t$ for $t = 1, \ldots, n$. Then

$$b_k \in J^{\lambda(k)} \setminus J^{\lambda(k)+1} \quad \text{for} \quad k = 0, 1, \ldots, z.$$

More precisely, for $s \in \mathbb{N}$, the elements $b_k + J^s$ with $\lambda(k) = s - 1$ form an F-basis of J^{s-1}/J^s; in particular, we have $\lambda(1) = 1$ and $\mathrm{LL}(A) = \lambda(z) + 1$.

Proof. First we show by induction that $b_k \in J^{\lambda(k)}$ for $k = 0, 1, \ldots, z$. Certainly, we have $b_0 = 1 \in A = J^0 = J^{\lambda(0)}$. Thus let $k > 0$ and suppose that $b_l \in J^{\lambda(l)}$ for all $l < k$. Choose $l \in L_k$ with $\lambda(l)$ maximal, i.e. $\lambda(k) = 1 + \lambda(l)$. Consider the q-adic expansions $ke = i_1 + qi_2 + \ldots + q^{n-1}i_n$ and $le = j_1 + qj_2 + \ldots + q^{n-1}j_n$. Then $i_t \geq j_t$, i.e. $0 \leq i_t - j_t \leq i_t < q$ for $t = 1, \ldots, n$. Thus $(k-l)e = ke - le$ has the q-adic expansion

$$(k-l)e = (i_1 - j_1) + q(i_2 - j_2) + \ldots + q^{n-1}(i_n - j_n).$$

Since $l < k$ our induction hypothesis implies: $b_k = b_l b_{k-l} \in J^{\lambda(l)} J = J^{\lambda(l)+1} = J^{\lambda(k)}$.

Next we show inductively that $b_k \notin J^{\lambda(k)+1}$ for $k = 0, 1, \ldots, z$. Certainly, we have $b_0 = 1 \notin J = J^{\lambda(0)+1}$. Thus let $k > 0$ and assume that $b_k \in J^r$ for some $r > \lambda(k)$; we choose r maximal with this property. Then $b_k = b_{i_1} \ldots b_{i_r}$ for suitable $i_1, \ldots, i_r \in \{1, \ldots, z\}$. Thus $k = i_1 + \ldots + i_r$ and $b_{i_1}, \ldots, b_{i_r} \notin J^2$. Since $b_{i_1} \ldots b_{i_{r-1}} \neq 0$ we have $b_{i_1} \ldots b_{i_{r-1}} = b_l$ where $l = i_1 + \ldots + i_{r-1} < k$. By induction, we may assume that $b_l \in J^{\lambda(l)} \setminus J^{\lambda(l)+1}$. On the other hand, we have $b_l \in J^{r-1} \setminus J^r$. Thus $\lambda(l) = r - 1$. Consider the q-adic expansions

$$le = j_1 + qj_2 + \ldots + q^{n-1}j_n \quad \text{and} \quad (k-l)e = j_1' + qj_2' + \ldots + q^{n-1}j_n'.$$

Since $b_l b_{k-l} = b_l b_{i_r} = b_k$ we must have $j_t + j_t' < q$ for $t = 1, \ldots, n$. Then ke has the q-adic expansion $ke = (j_1 + j_1') + q(j_2 + j_2') + \ldots + q^{n-1}(j_n + j_n')$. Since $j_t \leq j_t + j_t'$ for $t = 1, \ldots, n$ we have $l \in L_k$ and therefore $r > \lambda(k) \geq 1 + \lambda(l) = r$, which is a contradiction. □

Example 3.3. Let $(q, n, e) = (13, 2, 8)$, so that $z = 21$. The following table gives the values of λ:

k	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
$\lambda(k)$	0	1	1	2	2	1	3	2	4	3	2	4	3	1	4	3	5	4	2	5	4	6

Thus $\dim A = 22$, $\mathrm{LL}(A) = 7$, and the Loewy vector of A is $[1, 4, 5, 4, 5, 2, 1]$. More precisely,

the Loewy layers of A are given as follows:

$$\begin{array}{cc} b_0 & (0,0) \\ b_1, b_2, b_5, b_{13} & (0,8)(1,3)(3,1)(8,0) \\ b_3, b_4, b_7, b_{10}, b_{18} & (1,11)(2,6)(4,4)(6,2)(11,1) \\ b_6, b_9, b_{12}, b_{15} & (3,9)(5,7)(7,5)(9,3) \\ b_8, b_{11}, b_{14}, b_{17}, b_{20} & (4,12)(6,10)(8,8)(10,6)(12,4) \\ b_{16}, b_{19} & (9,11)(11,9) \\ b_{21} & (12,12) \end{array}$$

In the following, we denote by $s_q(x)$ the q-adic digit sum of an integer $x \in \mathbb{N}_0$, i.e.

$$s_q(x) = x_1 + x_2 + x_3 + \dots$$

where $x = x_1 + qx_2 + q^2x_3 + \dots$ is the q-adic expansion of x. Our next result computes the values of λ for a class of examples.

Corollary 3.1. *If $e \mid q-1$ then $\lambda(k) = s_q(ke)/e$ for $k = 0, \dots, z$. Thus*

$$\mathrm{LL}(A) = \lambda(z) + 1 = n\frac{q-1}{e} + 1.$$

Proof. We argue by induction on k. Certainly, we have $\lambda(0) = 0 = s_q(0e)/e$. Suppose therefore that $k > 0$ and that $\lambda(l) = s_q(le)/e$ for every $l < k$. Consider the q-adic expansion $ke = i_1 + qi_2 + \dots + q^{n-1}i_n$. Then

$$0 \equiv ke \equiv i_1 + i_2 + \dots + i_n = s_q(ke) \pmod{e}.$$

Let $l \in L_k$, and consider the q-adic expansion $le = j_1 + qj_2 + \dots + q^{n-1}j_n$. Then $l < k$ and $j_t \leq i_t$ for $t = 1, \dots, n$. Moreover, we have $s_q(le) \equiv 0 \pmod{e}$ and

$$s_q(le) = j_1 + \dots + j_n < i_1 + \dots + i_n = s_q(ke).$$

Thus $s_q(le) \leq s_q(ke) - e$ and $\lambda(l) = s_q(le)/e \leq s_q(ke)/e - 1$.

On the other hand, there is certainly some $l < k$ such that the q-adic expansion $le = j_1 + qj_2 + \dots + q^{n-1}j_n$ satisfies $0 \leq j_t \leq i_t$ for $t = 1, \dots, n$ and

$$s_q(le) = j_1 + \dots + j_n = i_1 + \dots + i_n - e = s_q(ke) - e.$$

Then $l \in L_k$ and $\lambda(l) = s_q(le)/e = s_q(ke)/e - 1$. Hence, by definition, we have $\lambda(k) = 1 + \lambda(l) = s_q(ke)/e$.

The final assertion follows since $ez = q^n - 1$ has q-adic expansion

$$q^n - 1 = (q-1) + q(q-1) + \dots + q^{n-1}(q-1),$$

so that $s_q(q^n - 1) = n(q-1)$ and $\lambda(z) = n\frac{q-1}{e}$. □

Let us compute the Loewy length in another class of examples.

Proposition 3.3. *If $2 < e \mid q+1$ then n is even, and $\mathrm{LL}(A) = n\frac{q-1}{2} + 1$.*

Proof. Suppose that $2 < e \mid q+1$. Then $0 \equiv q^n - 1 \equiv (-1)^n - 1 \pmod{e}$, so that n is even. An F-basis of $A = A(q,n,e)$ is given by the monomials $x_1^{i_1}x_2^{i_2}\dots x_n^{i_n}$ such that

$$0 \equiv i_1 + qi_2 + \ldots + q^{n-1}i_n \equiv i_1 + i_3 + \ldots + i_{n-1} - i_2 - i_4 - \ldots - i_n \pmod{e}$$

and $0 \le i_t < q$ for $t = 1, \dots, n$. Clearly, $x_i x_{i+1}$ is such a monomial, for $i = 1, \dots, n-1$. Moreover, $(x_1x_2)^{q-1}\dots(x_{n-1}x_n)^{q-1}$ is a nonzero product of $\frac{n}{2}(q-1)$ such monomials. Thus $\mathrm{LL}(A) \ge n\frac{q-1}{2} + 1$.

On the other hand, each of our basis monomials of J has degree at least 2. Thus a product of $n\frac{q-1}{2} + 1$ such monomials has degree at least $n(q-1)+2$. Hence at least one variable x_t occurs in this product with an exponent bigger than $q-1$, so the product is zero. This shows that $\mathrm{LL}(A) = n\frac{q-1}{2} + 1$. □

4 An automorphism

We keep the setup of Section 3. In our next result, we construct a certain useful F-algebra automorphism of $A = A(q,n,e)$.

Proposition 4.1. *For $k \in \{1, \dots, z\}$, let $k' \in \{1, \dots, z\}$ such that $k' \equiv qk \pmod{z}$. Then the F-linear map $\pi : A \longrightarrow A$ such that $\pi(b_0) = b_0$ and $\pi(b_k) = b_{k'}$ for $k = 1, \dots, z$ is an F-algebra automorphism. In particular, we have $\lambda(k) = \lambda(k')$ for $k = 1, \dots, z$.*

Proof. Let $k \in \{1, \dots, z\}$, and consider the q-adic expansion $ke = i_1 + qi_2 + \ldots + q^{n-1}i_n$. Then $qke = qi_1 + q^2i_2 + \ldots + q^n i_n$ is the q-adic expansion of qke, and

$$(qk - zi_n)e = qke - (q^n - 1)i_n = i_n + qi_1 + q^2i_2 + \ldots + q^{n-1}i_{n-1}$$

is the q-adic expansion of $(qk - zi_n)e$; in particular, $(qk - zi_n)e \in \{1, \dots, q^n - 1\}$. Since

$$(qk - zi_n)e = qke - (q^n - 1)i_n \equiv qke \equiv k'e \pmod{q^n - 1}$$

and $k'e \in \{1, \dots, q^n - 1\}$ we obtain $k'e = (qk - zi_n)e = i_n + qi_1 + q^2i_2 + \ldots + q^{n-1}i_{n-1}$. Now let also $l \in \{1, \dots, z\}$, and consider the q-adic expansion $le = j_1 + qj_2 + \ldots + q^{n-1}j_n$. Then $l'e = j_n + qj_1 + q^2j_2 + \ldots + q^{n-1}j_{n-1}$ is the q-adic expansion of $l'e$. Thus Proposition 3.1 implies that $b_k b_l \neq 0$ if and only if $b_{k'}b_{l'} \neq 0$.

Suppose that $b_k b_l \neq 0$, i.e. $b_k b_l = b_{k+l}$; in particular, $k + l \in \{1, \dots, z\}$. Then also $b_{k'}b_{l'} \neq 0$, i.e. $b_{k'}b_{l'} = b_{k'+l'}$ and $k' + l' \in \{1, \dots, z\}$. Since

$$k' + l' \equiv qk + ql \equiv q(k+l) \equiv (k+l)' \pmod{z}$$

we conclude that $k'+l' = (k+l)'$. This shows that π is an F-algebra endomorphism. Since $k \longmapsto k'$ is clearly a permutation of $\{1, \ldots, z\}$, π is even an F-algebra automorphism. In particular, we have $\pi(J^s) = J^s$ for $s \in \mathbb{N}_0$. Thus Proposition 3.2 implies that $\lambda(k) = \lambda(k')$ for $k = 1, \ldots, z$. □

By Proposition 4.1, the map λ is constant on each orbit of the permutation $k \longmapsto k'$ of $\{1, \ldots, z\}$. This often simplifies the computation of the values of λ.

Note that the order of the permutation $k \longmapsto k'$ is the order of q modulo z, i.e. the smallest positive integer s such that $q^s \equiv 1 \pmod{z}$. We denote this order by $\mathrm{ord}_z(q)$. Then $\mathrm{ord}_z(q)$ divides both n and $\varphi(z)$ where φ denotes Euler's totient function.

Example 4.1. In Example 3.2 above ($(q, n, e, z) = (3, 4, 5, 16)$) the permutation $k \longmapsto k'$ is

$$(1, 3, 9, 11)(2, 6)(4, 12)(5, 15, 13, 7)(8)(10, 14)(16).$$

This explains part of the Loewy structure of A. Here we have $\mathrm{ord}_z(q) = 4$. The table containing the values of λ can now be written in a more compact form:

k	0	1	2	4	5	8	10	16
$\lambda(k)$	0	1	1	2	2	2	3	4

.

Remark 4.1. (i) Since $\lambda(1) = 1$, Proposition 4.1 implies that always $\dim J/J^2 \geq \mathrm{ord}_z(q)$.

(ii) If t denotes the number of orbits of the permutation $k \longmapsto k'$ on $\{1, \ldots, z\}$ then clearly $\mathrm{LL}(A) \leq t + 1$.

(iii) Recall that the socle series of A is the chain of ideals

$$0 = \mathrm{S}_0(A) \subseteq \mathrm{S}_1(A) \subseteq \mathrm{S}_2(A) \subseteq \ldots$$

of A such that $\mathrm{S}_i(A)/\mathrm{S}_{i-1}(A)$ is the socle of $A/\mathrm{S}_{i-1}(A)$ for $i \in \mathbb{N}$. Since A is symmetric we have

$$\mathrm{S}_i(A) = \big\{a \in A : aJ^i = 0\big\} = (J^i)^\perp$$

for $i \in \mathbb{N}_0$ where $U^\perp = \{x \in A : \sigma(xA) = 0\}$ for every subspace U of A, and σ denotes a symmetrizing linear form on A. It is easy to compute an F-basis of $\mathrm{S}_i(A)$ for $i \in \mathbb{N}_0$. In fact, since an F-basis of J^i is provided by the elements b_k with $\lambda(k) \geq i$, a basis of $\mathrm{S}_i(A) = (J^i)^\perp$ is given by the elements b_{z-l} with $\lambda(l) < i$.

Example 4.2. In Example 3.2 above ($(q, n, e, z) = (3, 4, 5, 16)$) the socle series of A is as follows:

$$b_0$$
$$b_2, b_6$$
$$b_1, b_3, b_4, b_8, b_9, b_{11}, b_{12}$$
$$b_5, b_7, b_{10}, b_{13}, b_{14}, b_{15}$$
$$b_{16}$$

Note that the socle series of A does not coincide with the Loewy series of A (in contrast to the situation for group algebras of finite p-groups where p is a prime).

5 Isomorphisms

We keep the notation introduced above. Thus F is an arbitrary field, and q, n, e are positive integers such that $q > 1$ and $e \mid q^n - 1$. We consider the F-algebra $A = A(q, n, e)$ and its radical J. Since all structure constants of A are either 0 or 1 the structure of A is essentially independent of F.

Theorem 5.1. *Let n' be a divisor of n, and suppose that $e = e' \frac{q^n-1}{q^{n'}-1}$ for a positive integer e'. Then the F-algebras $A(q, n, e)$ and $A(q, n', e')$ are isomorphic.*

Proof. We observe first that

$$\dim A(q, n, e) = \frac{q^n - 1}{e} + 1 = \frac{q^{n'} - 1}{e'} + 1 = \dim A(q, n', e').$$

Let us denote the standard bases of $A := A(q, n, e)$ and $A' := A(q, n', e')$ by $b_0, \ldots, b_z$ and $b'_0, \ldots, b'_z$ where $z = (q^n - 1)/e = (q^{n'} - 1)/e'$. We claim that the F-linear map $f : A \longrightarrow A'$ with $f(b_k) = b'_k$ for $k = 0, \ldots, z$ is an F-algebra isomorphism. In order to see this, let $k, l \in \{0, \ldots, z\}$, and consider the q-adic expansions $ke' = \sum_{t=1}^{n'} q^{t-1} i_t$ and $le' = \sum_{t=1}^{n'} q^{t-1} j_t$. Then

$$\begin{aligned} ke &= ke' \tfrac{q^n-1}{q^{n'}-1} = (\textstyle\sum_{t=1}^{n'} q^{t-1} i_t)(1 + q^{n'} + q^{2n'} + \ldots + q^{n-n'}) \\ &= \textstyle\sum_{t=1}^{n'} q^{t-1} i_t + \sum_{t=1}^{n'} q^{n'+t-1} i_t + \ldots + \sum_{t=1}^{n'} q^{n-n'+t-1} i_t \end{aligned}$$

is the q-adic expansion of ke. Similarly, the q-adic expansion of le is

$$le = \sum_{t=1}^{n'} q^{t-1} j_t + \sum_{t=1}^{n'} q^{n'+t-1} j_t + \ldots + \sum_{t=1}^{n'} q^{n-n'+t-1} j_t.$$

Thus Proposition 3.1 implies that $b_k b_l \neq 0$ if and only if $i_t + j_t < q$ for $t = 1, \ldots, n$ if and only if $b'_k b'_l \neq 0$, and in this case we have $b_k b_l = b_{k+l}$ and $b'_k b'_l = b'_{k+l}$. The result follows. □

We note that, as shown in the proof above, the condition $e = e' \frac{q^n-1}{q^{n'}-1}$ means that the q-adic expansion of e is periodic with period n'.

Example 5.1. Let $q = 5$, $n = 4$, $e = 78$ and $n' = 2$, $e' = 3$. (Note that $78 = 3 \cdot (5^2 + 1)$.) Theorem 5.1 implies that $A(5, 4, 78) \cong A(5, 2, 3) =: A$. It is easy to verify that $\dim A = 9$ and $\mathrm{LL}(A) = 5$. The Loewy vector is $[1, 3, 3, 1, 1]$, and the Loewy structure is as follows:

b_0	$(0,0,0,0)$
b_1, b_2, b_5	$(0,3,0,3), (1,1,1,1), (3,0,3,0)$
b_3, b_4, b_7	$(1,4,1,4), (2,2,2,2), (4,1,4,1)$
b_6	$(3,3,3,3)$
b_8	$(4,4,4,4)$

Corollary 5.1. *(i) Suppose that* $e = e'\frac{q^n-1}{q-1}$ *for some* $e' \in \mathbb{N}$. *Then*

$$A(q,n,e) \cong A(q,1,e') \cong F[X]/(X^{1+z})$$

where $z = (q-1)/e'$*; in particular,* $A(q,n,e)$ *is a uniserial algebra.*
(ii) Conversely, if $A(q,n,e)$ *is a uniserial* F*-algebra then* $\frac{q^n-1}{q-1}$ *divides* e.
(iii) If $e = \frac{q^n-1}{q^{n'}-1}$ *for a divisor* n' *of* n *then*

$$A(q,n,e) \cong A(q,n',1) \cong F[X_1,\ldots,X_{n'}]/(X_1^q,\ldots,X_{n'}^q).$$

Proof. (i) The isomorphism $A(q,n,e) \cong A(q,1,e')$ is the special case $n'=1$ of Theorem 5.1. Both algebras have dimension $1+z$ where $z = \frac{q-1}{e'}$, and $\mathrm{LL}(A(q,1,e')) = 1\frac{q-1}{e'} + 1 = \dim A(q,1,e')$ by Corollary 3.1. Thus they are isomorphic to the truncated polynomial algebra $F[X]/(X^{1+z})$.

(ii) Suppose that $A = A(q,n,e)$ is uniserial; in particular, $\dim J/J^2 = 1$. Thus $\mathrm{ord}_z(q) = 1$ by Remark 4.1, i.e. $q \equiv 1 \pmod z$. Hence $\frac{q^n-1}{e} = z \mid q-1$, and $\frac{q^n-1}{q-1} \mid e$.

(iii) The isomorphism $A(q,n,e) \cong A(q,n',1)$ is the special case $e'=1$ of Theorem 5.1. By definition, we have $A(q,n',1) \cong F[X_1,\ldots,X_{n'}]/(X_1^q,\ldots,X_{n'}^q)$. □

We continue with another application of Theorem 5.1.

Proposition 5.1. *Suppose that* $e = \frac{q^n-1}{k(q-1)}$ *where* k *is a proper divisor of* $q+1$*, and set* $r := \frac{q+1}{k} - 1$. *Then* $A = A(q,n,e)$ *has Loewy length* q *and Loewy vector*

$$[1,3,5,\ldots,2k-3,\underbrace{2k-1,\ldots,2k-1}_{r},\underbrace{2k-3,\ldots,2k-3}_{r},\ldots,\underbrace{1,\ldots,1}_{r}].$$

Proof. It is easy to check that

$$1+3+5+\ldots+2k-3+r(2k-1+2k-3+\ldots+1) = k(q-1)+1 = \dim A,$$

and that the candidate for the Loewy vector above has precisely q components.

If $k=1$ then $e = \frac{q^n-1}{q-1}$ and $z = q-1$, so $A(q,n,e) \cong A(q,1,1) \cong F[X]/(X^q)$ by Corollary 5.1. Thus A has Loewy length q and Loewy vector $[1,\ldots,1]$ which has the desired form, with $r=q$.

Thus we may assume that $k>1$; in particular, $q \neq 2$. Since $q \equiv -1 \pmod k$ we have

$$0 \equiv 1+q+\ldots+q^{n-1} \equiv 1+(-1)+\ldots+(-1)^{n-1} \pmod k,$$

so that n is even. Then $e = \frac{q+1}{k}\cdot\frac{q^n-1}{q^2-1}$. By Theorem 5.1, we have $A \cong A(q,2,\frac{q+1}{k})$. Thus we may assume that $n=2$, $e = \frac{q+1}{k}$, and $r = e-1$. Then $\mathrm{LL}(A) = q$ by Proposition 3.3. Let

$$V_0 \;:=\; \{(i,i) : 0 \le i < q\},$$

$$\begin{aligned} V_1 &:= \{(i, i+je) : 1 \le j < k, 0 \le i < q - je\}, \\ V_2 &:= \{(i+je, i) : 1 \le j < k, 0 \le i < q - je\}. \end{aligned}$$

Each pair in $V := V_0 \cup V_1 \cup V_2$ is a solution $(x, y) \in \{0, \ldots, q-1\}^2$ of the congruence $x + qy \equiv 0 \pmod{e}$. Moreover, it is easily checked that $|V| = k(q-1)+1 = \dim A$. Thus V is precisely the set of solutions $(x, y) \in \{0, \ldots, q-1\}^2$ of the congruence $x + qy \equiv 0 \pmod{e}$.

It is easy to see that each pair $(i, i) \in V_0$ gives rise to a basis vector in the Loewy layer J^i/J^{i+1}, that each pair $(i, i+je) \in V_1$ gives rise to a basis vector in the Loewy layer J^{i+j}/J^{i+j+1} and that, similarly, each pair $(i+je, i) \in V_2$ gives rise to a basis vector in the Loewy layer J^{i+j}/J^{i+j+1}.

Let $t \in \{0, \ldots, q-1\}$. In order to determine $\dim J^t/J^{t+1}$ we need to count the pairs $(i, i+je) \in V_1$ such that $i+j = t$. These are the pairs $(t-j, t-j+je) = (t-j, t+j(e-1))$ such that $1 \le j < k$ and $0 \le t - j \le q - 1 - je$.

Suppose first that $t \le k-1$. Then we need to count the pairs $(t-j, t+j(e-1))$ such that $1 \le j \le q - 1 - j(e-1)$. However, the condition $1 \le j \le t$ implies that

$$t + j(e-1) \le t + t(e-1) = te \le (k-1)e < q.$$

Thus we are simply counting the t pairs $(t-j, t+j(e-1))$ with $1 \le j \le t$.

Suppose now that $t \ge k$. Then we need to count the pairs $(t-j, t+j(e-1))$ such that $1 \le j < k$ and $t + j(e-1) \le q-1$. However, it is easily checked that

$$\frac{q-t-1}{e-1} \le \frac{q-k-1}{e-1} < \frac{q+1}{e} = k.$$

Thus we are simply counting the $\lfloor \frac{q-t-1}{e-1} \rfloor = \lfloor \frac{q-t-1}{r} \rfloor$ pairs $(t-j, t+j(e-1))$ with $1 \le j \le \frac{q-t-1}{e-1}$.

The count for V_2 is similar, and the count for V_0 is trivial. We conclude that

$$\dim J^t/J^{t+1} = \begin{cases} 2t+1, & \text{for } t = 0, \ldots, k-1, \\ 2\lfloor \frac{q-1-t}{r} \rfloor + 1, & \text{for } t = k, \ldots, q-1. \end{cases}$$

The result follows. □

Example 5.2. Let $(q, n, e) = (11, 2, 4)$. Then Proposition 5.1 applies with $k = 3$ and $r = 3$. In this case, A has dimension 31, Loewy length $q = 11$ and Loewy vector $[1, 3, 5, 5, 5, 3, 3, 3, 1, 1, 1]$. More precisely, bases for the various Loewy layers are given

as follows:

b_0	$(0,0)$
b_1, b_3, b_{11}	$(0,4), (1,1), (4,0)$
$b_2, b_4, b_6, b_{14}, b_{22}$	$(0,8), (1,5), (2,2), (5,1), (8,0)$
$b_5, b_7, b_9, b_{17}, b_{25}$	$(1,9), (2,6), (3,3), (6,2), (9,1)$
$b_8, b_{10}, b_{12}, b_{20}, b_{28}$	$(2,10), (3,7), (4,4), (7,3), (10,2)$
b_{13}, b_{15}, b_{23}	$(4,8), (5,5), (8,4)$
b_{16}, b_{18}, b_{26}	$(5,9), (6,6), (9,5)$
b_{19}, b_{21}, b_{29}	$(6,10), (7,7)(10,6)$
b_{24}	$(8,8)$
b_{27}	$(9,9)$
b_{30}	$(10,10)$

Many of our algebras will turn out to have Loewy length 3. In this connection, the following result may be of interest.

Proposition 5.2. *Let F be algebraically closed of characteristic $p \neq 2$, and let A be a symmetric local F-algebra with $\dim \mathrm{J}(A)^2/\mathrm{J}(A)^3 = 1$. Then A has an F-basis*

$$1, x, x^2, \ldots, x^r, y_1, \ldots, y_s$$

such that $x^{r+1} = 0 = xy_i = y_i x$ for $i = 1, \ldots, s$ and

$$y_i y_j = \begin{cases} x^r, & \text{if } i = j, \\ 0, & \text{otherwise} \end{cases} \qquad (i, j = 1, \ldots, s).$$

In particular, A is commutative, and the isomorphism type of A is uniquely determined by the dimension and the Loewy length of A.

Proof. Let $J := \mathrm{J}(A)$. Since $\dim J^2/J^3 = 1$, Lemma G in [11] implies that $J \subseteq \mathrm{Z}(A)$. Thus $A = F \cdot 1 \oplus J$ is commutative.

Assume that $a^2 \in J^3$ for all $a \in J$. Then $2ab = (a+b)^2 - a^2 - b^2 \in J^3$ for all $a, b \in J$. Since $\mathrm{char}(F) \neq 2$ this implies that $J^2 \subseteq J^3$. Thus $J^2 = 0$, a contradiction.

Hence there is $x \in J$ such that $x^2 \notin J^3$, i.e. $J^2 = Fx^2 \oplus J^3$. Now Lemma E in [11] shows that $J^i = Fx^i + J^{i+1}$ for $i \geq 2$. Let $r \in \mathbb{N}$ be minimal such that $x^{r+1} = 0$. Then $x^2, \ldots, x^r$ constitute an F-basis of J^2. We set $I := Fx + Fx^2 + \ldots + Fx^r$. Since $IJ \subseteq J^2 \subseteq I$, I is an ideal of A. Let $\sigma : A \longrightarrow F$ be a symmetrizing linear form on A. Then

$$I^\perp := \{y \in A : \sigma(yI) = 0\} = \{y \in A : Iy = 0\}$$

is an ideal of A, and $\dim I + \dim I^\perp = \dim A$. It is easy to see that $I \cap I^\perp = Fx^r$. Thus $\dim(I + I^\perp) = \dim A - 1$, i.e. $I + I^\perp = J$. Since σ is a symmetrizing linear form on A, we have $\sigma(J^r) \neq 0$, i.e. $\sigma(x^r) \neq 0$; we may assume that $\sigma(x^r) = 1$. Then $I^\perp = Fx^r \oplus Y$ where $Y := I^\perp \cap \mathrm{Ker}(\sigma)$. We claim that the bilinear form

$$\beta : Y \times Y \longrightarrow F, \quad (y, z) \longmapsto \sigma(yz),$$

is nondegenerate. Indeed, suppose that $y \in Y$ satisfies $\sigma(yz) = 0$ for all $z \in Y$. Since $J = I + I^\perp = I \oplus Y$ this implies that $\sigma(yz) = 0$ for all $z \in J$. Since also $\sigma(y \cdot 1) = \sigma(y) = 0$ we conclude that $\sigma(yA) = 0$, so that $y = 0$.

Now let $y_1, \ldots, y_s$ be an orthonormal basis of Y, and let $i, j \in \{1, \ldots, s\}$. Then $y_i y_j \in J^2 \subseteq I$ and $y_i y_j \in I^\perp$, i.e. $y_i y_j \in I \cap I^\perp = Fx^r$. Let $\alpha_{ij} \in F$ such that $y_i y_j = \alpha_{ij} x^r$. Then $\alpha_{ij} = \sigma(\alpha_{ij} x^r) = \sigma(y_i y_j) = \delta_{ij}$. Since

$$A = F \cdot 1 \oplus J = F1 \oplus I \oplus Y = F1 \oplus Fx \oplus Fx^2 \oplus \ldots \oplus Fx^r \oplus Fy_1 \oplus \ldots \oplus Fy_s$$

the result follows. □

6 The numbers $m(q, e)$

Let $q, e \in \mathbb{N}$ such that $\gcd(q, e) = 1$. We define $m(q, e)$ as the smallest positive integer t with the property that there exists a sum of t powers of q which is divisible by e. These numbers will be used in Section 7 in order to bound the Loewy length of our algebras. The following facts are easy to verify; we leave the formal proofs to the readers.

Lemma 6.1. *(i)* $m(q, e) = m(r, e)$ *for every* $r \in \mathbb{N}$ *such that* $q \equiv r \pmod{e}$.

(ii) $m(q, e) \leq m(q^k, e)$ *for every* $k \in \mathbb{N}$.

(iii) $m(q, e) \leq m(r, e)$ *whenever* $r \in \mathbb{N}$ *is such that the cyclic subgroup* $\langle r + e\mathbb{Z} \rangle$ *of* $(\mathbb{Z}/e\mathbb{Z})^\times$ *is contained in* $\langle q + e\mathbb{Z} \rangle$.

(iv) $m(q, f) \leq m(q, e)$ *for every (positive) divisor* f *of* e.

(v) $m(q, ef) \leq m(q, e)m(q, f)$ *for every* $f \in \mathbb{N}$.

Note that always $m(q, e) \leq e$, and observe that $m(q, e)$ can be worked out by computing in the finite ring $\mathbb{Z}/e\mathbb{Z}$.

Example 6.1. (i) $m(q, e) = e$ if and only if $q \equiv 1 \pmod{e}$.

(ii) $m(q, e) = 1$ if and only if $e = 1$.

Example 6.2. One can check that the first values of the function $\mathbb{N}_0 \longrightarrow \mathbb{N}_0$ sending x to $m(2, 2x + 1)$, are given as follows:

$$1,\ 2,\ 2,\ 3,\ 2,\ 2,\ 2,\ 4,\ 2,\ 2,\ 3,\ 3,\ 2,\ 2,\ 2,\ 5,\ 2,\ 3, \ldots$$

Recall that we denote by $\mathrm{ord}_e(q)$ the order of q modulo e, i.e. the order of $q + e\mathbb{Z}$ in $(\mathbb{Z}/e\mathbb{Z})^\times$. Thus $\mathrm{ord}_e(q)$ divides $\varphi(e)$ where φ denotes Euler's totient function. Moreover, for $n \in \mathbb{N}$, we have:

$$q^n \equiv 1 \pmod{e} \Longleftrightarrow \mathrm{ord}_e(q) \mid n.$$

The following result gives some further properties of the numbers $m(q, e)$.

Lemma 6.2. *Let $e_1 := \gcd(e, q-1)$, and let $n := \mathrm{ord}_e(q)$.*
(i) If e divides a sum of t powers of q then e_1 divides t. In particular, e_1 divides $m(q,e)$.
(ii) $m(q,e) \le e_1 m(q, \frac{e}{e_1})$.
(iii) $m(q,e) \le \frac{ne_1}{l} \le ne_1$ where $l := \gcd(n, e_1, \frac{q^n-1}{e})$.
(iv) $m(q,e) \le n$ if e divides $1 + q + \cdots + q^{n-1}$.

Proof. (i) Let $a_1, \ldots, a_t \in \mathbb{N}_0$ such that $q^{a_1} + \ldots + q^{a_t} \equiv 0 \pmod{e}$. Then

$$0 \equiv q^{a_1} + \ldots + q^{a_t} \equiv 1^{a_1} + \ldots + 1^{a_t} \equiv t \pmod{e_1}.$$

(ii) Lemma 6.1 (v) implies that $m(q,e) \le m(q,e_1)m(q, \frac{e}{e_1})$, and $m(q,e_1) = e_1$ by Example 6.1.

(iii) Since $l \mid e_1 \mid q-1$ we have $q \equiv 1 \pmod{l}$. Thus $1 + q + \ldots + q^{n-1} \equiv n \equiv 0 \pmod{l}$. Since $el \mid q^n - 1 = (q-1)(1 + q + \ldots + q^{n-1})$ we have $\frac{e}{e_1} \mid \frac{q-1}{e_1} \cdot \frac{1+q+\ldots+q^{n-1}}{l}$. Hence $\frac{e}{e_1} \mid \frac{1+q+\ldots+q^{n-1}}{l}$ and $e \mid \frac{e_1}{l}(1 + q + \ldots + q^{n-1})$, so that $m(q,e) \le \frac{ne_1}{l}$.

(iv) If e divides $1 + q + \ldots + q^{n-1}$ then $m(q,e) \le n$ by definition. □

We now present another useful description of the numbers $m(q,e)$.

Proposition 6.1. *Let $q > 1$, let $n \in \mathbb{N}$ such that $e \mid q^n - 1$, and let $z := \frac{q^n-1}{e}$. Then*

$$m(q,e) = \min\{s_q(ke) : k \in \mathbb{N}\} = \min\{s_q(ke) : k = 1, \ldots, z\}.$$

In particular, we always have $m(q,e) \le s_q(e) \le e$.

Proof. Let $k \in \mathbb{N}$, and consider the q-adic expansion $ke = i_1 + i_2 q + \ldots + i_r q^{r-1}$. Since $e \mid ke$, we have $m := m(q,e) \le i_1 + \ldots + i_r = s_q(ke)$, by definition. Thus

$$m \le \min\{s_q(ke) : k \in \mathbb{N}\} \le \min\{s_q(ke) : k = 1, \ldots, z\}.$$

Now let $k \in \mathbb{N}$ be minimal such that ke is a sum of m powers of q. Moreover, let $a_1, \ldots, a_m \in \mathbb{N}_0$ such that $ke = q^{a_1} + \ldots + q^{a_m}$. Then $a_t < n$ for $t = 1, \ldots, m$, and $ke = \sum_{t=0}^{n-1} i_t q^t$ where $i_t = |\{j \in \mathbb{N} : 1 \le j \le m,\ a_j = t\}|$ for $t = 0, \ldots, n-1$; in particular, $m = i_0 + \ldots + i_{n-1}$. Moreover, we have $i_t < q$ for $t = 0, \ldots, n-1$, by the definition of m. Thus $ke \le q^n - 1$, i.e. $k \le z$, and $s_q(ke) = i_0 + \ldots + i_{n-1} = m$. □

If ke has q-adic expansion $ke = i_1 + q i_2 + \ldots + q^{n-1} i_n$ (where $k \in \{0, \ldots, z\}$) then $(z-k)e$ has q-adic expansion

$$(z-k)e = (q - 1 - i_1) + q(q - 1 - i_2) + \ldots + q^{n-1}(q - 1 - i_n).$$

Thus $s_q((z-k)e) = n(q-1) - s_q(ke)$; this is useful in the computation of $m(q,e)$.

We have observed above that $m(q,e) = 1$ if and only if $e = 1$. The following result characterizes the condition $m(q,e) = 2$. (It seems to be difficult to characterize the case $m(q,e) = 3$ in a similar way.)

Lemma 6.3. *Let $q > 1$. Then $m(q,e) = 2$ if and only if $e = 2$, or $n := \mathrm{ord}_e(q)$ is even with $q^{n/2} \equiv -1 \pmod{e}$. Moreover, if $m(q,e) = 2$ and e is odd, then $m(q,e^k) = 2$ for $k \in \mathbb{N}$.*

Proof. If $e = 2$ then q is odd, and certainly $m(q,e) = 2$.

If $n := \mathrm{ord}_e(q)$ is even and $q^{n/2} \equiv -1 \pmod{e}$ then $q^{n/2} + 1 \equiv 0 \pmod{e}$ and $m(q,e) = 2$.

Suppose conversely that $m(q,e) = 2 \neq e$, i.e. $e > 2$. Then $e \mid q^i + q^j$ for suitable integers i, j with $0 \leq i < j < n := \mathrm{ord}_e(q)$. Since $\gcd(q,e) = 1$ this implies $e \mid 1 + q^{j-i}$. Thus we may assume that $i = 0$ and that j is minimal. Then $q^j \equiv -1 \pmod{e}$ implies that $q^{2j} \equiv 1 \pmod{e}$, so that $n \mid 2j$. Since $n > j$ this implies that $n = 2j$; in particular, n is even, and $q^{n/2} = q^j \equiv -1 \pmod{e}$.

Now let e be odd and $m(q,e) = 2$. Then e divides $Q+1$ for some power Q of q. Suppose that e^n divides $Q^{e^{n-1}} + 1$ for some $n \in \mathbb{N}$. Then $Q^{e^{n-1}} = e^n f - 1$ for some $f \in \mathbb{N}$. Thus

$$\begin{aligned} Q^{e^n} &= (e^n f - 1)^e = \sum_{i=0}^{e} \binom{e}{i} (e^n f)^i (-1)^{e-i} \\ &\equiv (-1)^e + e e^n f (-1)^{e-1} \equiv -1 \pmod{e^{n+1}}. \end{aligned}$$

i.e. $e^{n+1} \mid Q^{e^n} + 1$. By induction, we obtain $e^k \mid Q^{e^{k-1}} + 1$ for $k \in \mathbb{N}$, and the result follows. □

Remark 6.1. (i) Suppose that $(\mathbb{Z}/e\mathbb{Z})^\times$ is a nontrivial cyclic group. (Recall that this is the case if and only if e is 4, an odd prime power or the double of an odd prime power.) If $n := \mathrm{ord}_e(q)$ is even then $m(q,e) = 2$; in fact, $q^{n/2} + e\mathbb{Z}$ has order 2, and $-1 + e\mathbb{Z}$ is the only element of order 2 in $(\mathbb{Z}/e\mathbb{Z})^\times$. Thus $q^{n/2} + e\mathbb{Z} = -1 + e\mathbb{Z}$.

(ii) Suppose that e is a Fermat prime (e.g. $e \in \{3, 5, 17\}$). Then $|(\mathbb{Z}/e\mathbb{Z})^\times| = e - 1$ is a power of 2. Thus $\mathrm{ord}_e(q)$ is even whenever $q \not\equiv 1 \pmod{e}$. Hence $m(q,e) = 2$ for all such q.

As in Example 6.2, we frequently have $m(q,e) = 2$. The following result can also be used in certain situations to show that $m(q,e)$ is small.

Lemma 6.4. *Let $q > 1$, and let p be a prime divisor of $n := \mathrm{ord}_e(q)$ such that $\gcd(e, q^{\frac{n}{p}} - 1) = 1$. Then $m(q,e) \leq p$.*

Proof. Writing $n = pk$ where $k \in \mathbb{N}$ we have $e \mid q^{kp} - 1 = (q^k - 1)(q^{k(p-1)} + \ldots + q^k + 1)$. Since $\gcd(e, q^k - 1) = 1$ this implies that $e \mid q^{k(p-1)} + \ldots + q^k + 1$. Thus $m(q,e) \leq p$. □

Remark 6.2. When e is itself a prime the condition $\gcd(e, q^{\frac{n}{p}} - 1) = 1$ is always satisfied and can therefore be omitted. In this case we have $m(q,e) \leq p$ where p is the smallest prime divisor of $n = \mathrm{ord}_e(q)$. In particular, we have $m(q,e) \leq P$ where P is the largest prime divisor of $e - 1$.

We will present many more properties of the numbers $m(q,e)$ in part II of this paper.

7 Loewy length

Let F be a field, and let $q, n, e \in \mathbb{N}$ such that $q > 1$ and $e \mid q^n - 1$; in particular, $\gcd(q, e) = 1$. As before, we set $z := (q^n - 1)/e$, $e_1 := \gcd(e, q-1)$ and $m := m(q, e)$. We have already a recursive method in order to compute the Loewy length of the F-algebra $A = A(q, n, e)$, in terms of the map λ (see Proposition 3.2). In this section we are interested in more direct ways in order to compute or bound $\mathrm{LL}(A)$ in terms of the parameters q, n, e. As above, we set $J := \mathrm{J}(A)$. A connection with the Loewy length is given by the following result.

Theorem 7.1. *With notation as above, we have:*
(i) $n\lfloor \frac{q-1}{m} \rfloor + 1 \leq \mathrm{LL}(A) \leq \lfloor n\frac{q-1}{m} \rfloor + 1$.
(ii) If $m \nmid q-1$ *then* $n\lfloor \frac{q-1}{m} \rfloor + 2 \leq \mathrm{LL}(A)$.
(iii) If $m \mid q-1$ *or* $m = \frac{ne_1}{l}$ *where* $l := \gcd(n, e_1, \frac{q^n-1}{e})$ *then* $\mathrm{LL}(A) = n\frac{q-1}{m} + 1$.

Proof. (i) Consider a product $b_{k_1} \ldots b_{k_t}$ where $k_1, \ldots, k_t \in \{1, \ldots, z\}$ and $t := \lfloor n\frac{q-1}{m} \rfloor + 1 > n\frac{q-1}{m}$. For $j = 1, \ldots, t$, let $k_j e = i_{j1} + qi_{j2} + \ldots + q^{n-1}i_{jn}$ be the q-adic expansion of $k_j e$. Then $s_j := s_q(k_j e) \geq m$ for $j = 1, \ldots, t$, by Proposition 6.1. Thus $s_1 + \ldots + s_t \geq tm > n(q-1)$. On the other hand, we have

$$s_1 + \ldots + s_t = \sum_{j=1}^{t} \sum_{l=1}^{n} i_{jl} = \sum_{l=1}^{n} \sum_{j=1}^{t} i_{jl}.$$

Hence $\sum_{j=1}^{t} i_{jl} > q-1$ for some $l \in \{1, \ldots, n\}$. However, Proposition 3.1 implies that then $b_{k_1} \ldots b_{k_t} = 0$. This shows that $J^t = 0$, i.e. $\mathrm{LL}(A) \leq t$.

In order to prove the other inequality we may assume that $m < q$; for otherwise the result is trivial. By Proposition 6.1, there is $k \in \{1, \ldots, z\}$ such that $m = s_q(ke)$. Consider the q-adic expansion $ke = i_1 + qi_2 + \ldots + q^{n-1}i_n$. We have observed in Proposition 4.1 that $i_n + qi_1 + \ldots + q^{n-1}i_{n-1} = k'e$ for some $k' \in \{1, \ldots, z\}$. In this way we can cyclically permute the digits and obtain integers $k, k', k'', \ldots \in \{1, \ldots, z\}$. The sum of the n numbers $ke, k'e, k''e, \ldots$ is

$$m + qm + \ldots + q^{n-1}m = \frac{q^n - 1}{q-1}m.$$

We denote this sum by Ke where $K \in \mathbb{N}$. Setting $t := \lfloor \frac{q-1}{m} \rfloor \geq 1$ we have $tm \leq q-1$. Thus $tKe = tm + qtm + \ldots + q^{n-1}tm$ is the q-adic expansion of tKe. Hence Proposition 3.1 implies that $b_K^t = b_{tK} \neq 0$. Since b_K is a product of n elements in J this implies $\mathrm{LL}(A) > tn$, i.e. $\mathrm{LL}(A) \geq nt + 1$.

(ii) Now suppose that $m \nmid q-1$. Since $\dim A = 1 + z \geq 2$ and $\dim A/J = 1$ we have $\mathrm{LL}(A) \geq 2$. Thus we may assume $m < q-1$. We write $q - 1 = tm + r$ where $t = \lfloor \frac{q-1}{m} \rfloor$ and $r \in \{1, \ldots, m-1\}$. Then, with K as above,

$$\begin{aligned} r(1 + q + \ldots + q^{n-1}) &= (q-1)(1 + q + \ldots + q^{n-1}) - tm(1 + q + \ldots + q^{n-1}) \\ &= ze - tKe = Le \end{aligned}$$

where $L = z - tK \in \mathbb{N}$. Hence Proposition 3.1 implies that $0 \neq b_z = b_{tK+L} = b_K^t b_L$ where $b_L \in J$. Thus b_z is a product of $tn+1$ elements in J, i.e. $J^{tn+1} \neq 0$ and $\mathrm{LL}(A) \geq tn+2$.

(iii) If $m \mid q-1$ then the lower bound in (i) coincides with the upper bound. Thus

$$\mathrm{LL}(A) = n\left\lfloor \frac{q-1}{m} \right\rfloor + 1 = n\frac{q-1}{m} + 1.$$

Suppose therefore that $m = \frac{ne_1}{l}$. As in the proof of Lemma 6.2, we have

$$\frac{e_1}{l}(1 + q + \ldots + q^{n-1}) = ke$$

for some $k \in \{1, \ldots, z\}$. Thus Proposition 3.1 implies that $b_k^{(q-1)/(e_1/l)} = b_z \neq 0$, so that $\mathrm{LL}(A) > \frac{q-1}{e_1/l}$. On the other hand, by (i) we have

$$\mathrm{LL}(A) \leq \left\lfloor n\frac{q-1}{m} \right\rfloor + 1 = \left\lfloor n\frac{q-1}{ne_1/l} \right\rfloor + 1 = \frac{q-1}{e_1/l} + 1.$$

Hence $\mathrm{LL}(A) = \frac{q-1}{e_1/l} + 1 = n\frac{q-1}{m} + 1$. □

We obtain the following consequence.

Corollary 7.1. *If $n \leq 3$ then* $\mathrm{LL}(A) = \left\lfloor n\frac{q-1}{m} \right\rfloor + 1$.

Proof. If $n = 1$ then $m = e_1$ by Lemma 6.2; in particular, $m \mid q-1$, so $\mathrm{LL}(A) = \frac{q-1}{m} + 1 = \lfloor \frac{q-1}{m} \rfloor + 1$ by Theorem 7.1 (iii).

If $n = 2$ then $m \in \{e_1, 2e_1\}$ by Lemma 6.2; in particular, $m \mid q-1$ or $m = ne_1$, so that $\mathrm{LL}(A) = 2\frac{q-1}{m} + 1 = \lfloor 2\frac{q-1}{m} \rfloor + 1$ by Theorem 7.1 (iii).

If $n = 3$ then $m \in \{e_1, 2e_1, 3e_1\}$ by Lemma 6.2. If $m \in \{e_1, 3e_1\}$ then we can argue as before. Thus let $m = 2e_1$. By Theorem 7.1 (iii), we may also assume that $m \nmid q-1$. Then Theorem 7.1 (ii) implies that

$$\begin{aligned} \mathrm{LL}(A) &\geq 3\left\lfloor \frac{q-1}{2e_1} \right\rfloor + 2 = 3\left(\frac{(q-1)/e_1}{2} - \frac{1}{2}\right) + 2 = 3\frac{q-1}{2e_1} + \frac{1}{2} \\ &= \left(\frac{3(q-1)/e_1}{2} - \frac{1}{2}\right) + 1 = \left\lfloor 3\frac{q-1}{2e_1} \right\rfloor + 1 \geq \mathrm{LL}(A). \end{aligned}$$

Thus $\mathrm{LL}(A) = \lfloor 3\frac{q-1}{m} \rfloor + 1$. □

Remark 7.1. (i) In part II of the paper, we will see that often the upper bound in Theorem 7.1 is attained, but we will eventually also construct examples where $\mathrm{LL}(A) < \lfloor n\frac{q-1}{m} \rfloor + 1$.

(ii) In order to prove $\mathrm{LL}(A) = \lfloor n\frac{q-1}{m} \rfloor + 1$ in a specific case it suffices, of course, to show that $\mathrm{LL}(A) > \lfloor n\frac{q-1}{m} \rfloor =: t$, and this is usually done by finding $k_1, \ldots, k_t \in \{1, \ldots, z\}$ such that $b_{k_1} \ldots b_{k_t} = b_z \ (\neq 0)$.

(iii) Calculations with a combination of GAP [7] and Julia [2] show that $\mathrm{LL}(A) = \lfloor n\frac{q-1}{m} \rfloor + 1$ in the following cases:

n	4	5	6	7	8	9
q	≤ 100	≤ 13	≤ 9	≤ 9	≤ 9	≤ 8

(iv) Arguments similar to those of Corollary 7.1 show that $\mathrm{LL}(A) \geq \lfloor n\frac{q-1}{m} \rfloor$ in case $n = 4$. We have not found an example where equality holds.

(v) In the situation of Theorem 5.1, we have $m(q, e) = \frac{n}{n'} m(q, e')$, as is easy to see from the proof of Theorem 5.1. Thus

$$\mathrm{LL}(A(q, n, e)) = \left\lfloor \frac{n(q-1)}{m(q,e)} \right\rfloor + 1 \Longleftrightarrow \mathrm{LL}(A(q, n', e')) = \left\lfloor \frac{n'(q-1)}{m(q,e')} \right\rfloor + 1.$$

(vi) If $\frac{q^n-1}{q-1} \mid e$ then $\mathrm{LL}(A(q, n, e)) = \lfloor n\frac{q-1}{m} \rfloor + 1$; in fact, Theorem 5.1 gives an isomorphism $A(q, n, e) \cong A(q, 1, e')$ for a suitable $e' \in \mathbb{N}$. Thus (v) and Corollary 7.1 imply the equality.

(vii) If $e = \frac{q^n-1}{q^{n'}-1}$ for a divisor n' of n then $\mathrm{LL}(A(q, n, e)) = \lfloor n\frac{q-1}{m} \rfloor + 1$ since Theorem 5.1 gives an isomorphism $A(q, n, e) \cong A(q, n', 1)$, and $m(q, 1) = 1 \mid q-1$, by Example 6.1. Thus Theorem 7.1 (iii) proves the assertion.

(viii) If $e \mid q-1$ then $e = e_1 \mid m \leq s_q(e) = e$, so that $m = e \mid q-1$ (see Example 6.1 (i)). Thus $\mathrm{LL}(A) = n\frac{q-1}{m} + 1$ by Theorem 7.1 (iii) again. (This observation is [5, Theorem 1.2]; cf. also Corollary 3.1.)

(ix) If $e = \frac{q^n-1}{k(q-1)}$ for a proper divisor k of $q+1$ then $\mathrm{LL}(A) = \lfloor n\frac{q-1}{m} \rfloor + 1$; this follows from Proposition 5.1 and its proof.

The following observation is elementary.

Lemma 7.1. *The F-algebra $A = A(q, n, e)$ has the following properties:*

(i) $\mathrm{LL}(A) \geq 2$*;*

(ii) $\mathrm{LL}(A) = 2$ *if and only if* $e = q^n - 1$*;*

(iii) If $m = m(q, e) > n\frac{q-1}{3}$ *then* $\mathrm{LL}(A) = \lfloor n\frac{q-1}{m} \rfloor + 1 \leq 3$.

(iv) If $m = m(q, e) \leq 2$ *then* $\mathrm{LL}(A) = \lfloor n\frac{q-1}{m} \rfloor + 1$*; in particular, this applies whenever e divides $q+1$ (cf. Proposition 3.3).*

Proof. (i) Since $\dim A = 1 + z \geq 2$ and $\dim A/J = 1$ we have $\mathrm{LL}(A) \geq 2$.

(ii) If $\mathrm{LL}(A) = 2$ then $J^2 = 0$, so $\dim J = 1$ since A is a symmetric F-algebra. Thus $2 = \dim A = 1 + z = 1 + \frac{q^n-1}{e}$, i. e., $e = q^n - 1$. The converse is obvious.

(iii) Suppose that $m > n\frac{q-1}{3}$. Then $\mathrm{LL}(A) \leq \lfloor n\frac{q-1}{m} \rfloor + 1 \leq 2 + 1 = 3$.

If $e = q^n - 1$ then $m = s_q(q^n - 1) = n(q-1)$, so that $\mathrm{LL}(A) = 2 = \lfloor n\frac{q-1}{m} \rfloor + 1$.

If $e < q^n - 1$ then $\mathrm{LL}(A) \geq 3$ by (ii), so that $\mathrm{LL}(A) = 3 = \lfloor n\frac{q-1}{m} \rfloor + 1$.

(iv) By the remarks above, we may assume that $m = 2$. If q is odd then $m = 2 \mid q-1$, and the result follows from Theorem 7.1 (iii). Thus we may assume that q is even. Then e is odd. By Lemma 6.3, $\nu := \mathrm{ord}_e(q)$ is even, and $q^{\nu/2} \equiv -1 \pmod{e}$. Moreover, we have $n = \nu r$ for some $r \in \mathbb{N}$. In this case, $\mathrm{J}(A(q,n,e))$ contains the monomials $x_i x_{\nu/2+i}$ $(i = 1, \ldots, n - \frac{\nu}{2})$. Thus $x_1 \cdots x_n$ can be written as a product of $\frac{n}{2}$ of these monomials, and the nonzero element $b_z = x_1^{q-1} \cdots x_n^{q-1} \in A$ can be written as a product of $\frac{n}{2}(q-1)$ of these monomials. Hence

$$\mathrm{LL}(A(q,n,e)) \geq \frac{n}{2}(q-1) + 1 = \left\lfloor n\frac{q-1}{m} \right\rfloor + 1 \geq \mathrm{LL}(A(q,n,e)).$$

□

It seems to be difficult to characterize precisely when $\mathrm{LL}(A) = 3$.

Example 7.1. If $e \in \{2, 3, 4, 6\}$ then $q \equiv \pm 1 \pmod{e}$ for any q that is coprime to e. Thus Remark 7.1 and Lemma 7.1 yield that we have $\mathrm{LL}(A(q,n,e)) = \lfloor n\frac{q-1}{m} \rfloor + 1$ for these values of e, and all q and n.

We also have $\mathrm{LL}(A(q,n,e)) = \lfloor n\frac{q-1}{m} \rfloor + 1$ for $e = 5$ and all q and n; in fact, if $q \equiv \pm 1 \pmod{5}$ then we can argue as before, and if $q \not\equiv \pm 1 \pmod{5}$ then $m = 2$ by Remark 6.1, and we can apply Lemma 7.1.

We will extend this example considerably in the second part of this paper.

Acknowledgements

The work on this paper was begun while the last author was visiting the Technical University of Budapest in October 2017. Part of the work was also done while the last author was in residence at the Mathematical Sciences Research Institute in Berkeley, California, during the Spring 2018 semester, supported by the National Science Foundation under Grant No. DMS-1440140. The first author gratefully acknowledges support by the German Research Foundation (DFG) within the SFB-TRR 195 *Symbolic Tools in Mathematics and their Applications*. The research in this paper was also supported by the NKFI-Grants No. 115288 and 115799.

References

[1] A. Allan, Modular centralizer algebras corresponding to p-groups, *J. Algebra* **339** (2011), 156–171.

[2] J. Bezanson, A. Edelman, S. Karpinski, and V. B. Shah, Julia: A Fresh Approach to Numerical Computing, *SIAM Review* **59** (2017), 65-98.

[3] M. Broué, L. Puig, Characters and local structure in G-algebras, *J. Algebra* **63** (1980), 306–317.

[4] M. Broué, G. R. Robinson, Bilinear forms on G-algebras, *J. Algebra* **104** (1986), 377–396.

[5] J. Brough, I. Schwabrow, On the Loewy length of the center of a block with elementary abelian defect groups, *Comm. Algebra* **46** (2018), 829–833.

[6] S. Doty, K. Erdmann, A. Henke, Endomorphism rings of permutation modules over maximal Young subgroups, *J. Algebra* **307** (2007), 377–396.

[7] The GAP Group, GAP – Groups, Algorithms, and Programming, Version 4.8.10, 2018, (`https://www.gap-system.org`)

[8] B. Huppert, Endliche Gruppen I., Springer Verlag, Berlin, Heidelberg, New York, 1967.

[9] B. Huppert, N. Blackburn, Finite Groups II., Springer Verlag, Berlin, Heidelberg, New York, 1982.

[10] 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.

[11] B. Külshammer, Symmetric local algebras and small blocks of finite groups, *J. Algebra* **88** (1984), 190-195.

[12] B. Külshammer, Lectures on block theory, Cambridge University Press, Cambridge 1991.

[13] B. Külshammer, B. Sambale, Loewy lengths of centers of blocks, *Quart. J. Math.* **69** (2018), 855–870.

[14] O. Manz, U. Stammbach, and R. Staszewski, On the Loewy series of the group algebra of groups of small p-length, *Comm. Algebra* **17** 5 (1989), 1249–1274.

[15] D. S. Passman, The algebraic structure of group rings, John Wiley & Sons, Inc., New York 1977.

[16] J. Thévenaz, G-algebras and modular representation theory, Oxford University Press, New York 1995.

T. Breuer, Lehrstuhl D für Mathematik, RWTH Aachen University, Pontdriesch 14-16, D-52062 Aachen, Germany, e-mail: `sam@math.rwth-aachen.de`

L. Héthelyi, Department of Algebra, Budapest University of Technology and Economics, H-1111 Budapest, Műegyetem rkp. 3-9, Hungary, e-mail: `fobaba@t-online.hu`

E. Horváth, Department of Algebra, Budapest University of Technology and Economics, H-1111 Budapest, Műegyetem rkp. 3-9, Hungary, e-mail: he@math.bme.hu

B. Külshammer, Institut für Mathematik, Friedrich-Schiller-Universität, D-07737 Jena, Germany, e-mail: kuelshammer@uni-jena.de