The group ring of $SL_2(2^f)$ over 2-adic integers.

Gabriele Nebe

Dedicated to Prof. K. W. Roggenkamp in occasion of his 60th birthday

Abstract: Let $R = \mathbb{Z}_2[\zeta_{2^f-1}]$ and $G = SL_2(2^f)$. The group ring RG is calculated nearly up to Morita equivalence. In particular the irreducible RG-lattices can be described purely combinatorically in terms of subsets of $\{1, \ldots, f\}$.

1991 Mathematics Subject Classification: 20C05, 20C11

1 Introduction

The group $G = SL_2(p^f)$ of all 2×2-matrices over the field k with p^f elements is one of the simplest examples of a nonabelian finite group of Lie type. Its representation theory in characteristic 0 was already investigated by I. Schur [13] and its modular representation theory is also well understood ([1], [2]). The next step is to describe the integral group ring RG of G when R is the ring of integers in a finite extension of the field $\mathbb{Q}_l$ of l-adic numbers, to bring together the characteristic 0 and the characteristic l information. If $l \neq p$ and $l \neq 2$ then the defect groups of the ring direct summands of RG are cyclic, so RG is described by the general theory of blocks with cyclic defect groups ([10], [12], [7]). For odd primes p the Sylow 2-subgroups of G are dihedral groups and [10], Chapter VII investigates RG for $l = 2$. So the only remaining case is $l = p$, where the Sylow p-subgroups of G are elementary abelian of rank f. If $f = 1$ one again has the cyclic defect case and for $f = 2$ the group ring $\mathbb{Z}_pG$ is described up to Morita equivalence in [8]. In the present paper the remaining cases $f \geq 3$ are treated for $p = 2$.

To find kG, one uses methods from the representation theory for groups of Lie type in defining characteristic. However these methods are not directly applicable for calculating RG, when $R = \mathbb{Z}_2[\zeta_{2^f-1}]$ is the ring of integers in the unramified extension K of degree f of $\mathbb{Q}_2$. The new idea used in this paper is to start from the explicit presentation of kG given in [6] and lift the generators of kG to generators of RG. The explicit knowledge of kG together with the decomposition numbers calculated in [4] and [5] do not seem to be sufficient to determine RG up to Morita equivalence. But they give enough information to describe the inclusion patterns of the irreducible RG-lattices (Theorem 3.15) as well as the endomorphism rings of the projective indecomposable RG-lattices (Theorem 3.12). In particular it turns out that the endomorphism ring of the projective cover of the trivial RG-module is isomorphic to the group ring of the Sylow 2-subgroup of G. From Theorem

3.15 one gets the following explicit description of the projections of RG onto the simple summands of KG. The simple kG-modules M_I are naturally indexed with the subsets I of $\{1,\dots,f\}$ such that $dim_k(M_I) = 2^{|I|}$.

Theorem. Let V be a simple KG-module of dimension n and let $M_{I_1},\dots,M_{I_r}$ be the 2-modular constituents of V of dimension $n_j := 2^{|I_j|} = dim_k(M_{I_j})$, $1 \le j \le r$. Then there is a basis of V such that the corresponding matrix representation Δ_V satisfies

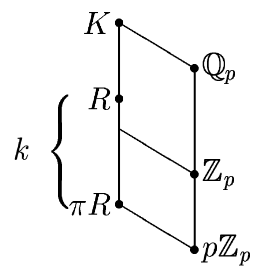
$$\Delta_V(RG) = \{(X_{ij})_{1\le i,j\le r} \in R^{n\times n} \mid X_{ij} \in 2^{|I_i - I_j|} R^{n_i \times n_j}\}.$$

This is the first time that such a detailed description of an infinite series of p-adic group rings has been found, where not only the order but also the number of generators of the Sylow p-subgroups grows. It is astonishing that, though the situation gets more and more complicated, the group rings $RSL_2(2^f)$ can be described in a uniform way for all $f \ge 3$. Similar methods can be applied for $G = SL_2(p^f)$ where p is odd, to get analogous information about the group ring as is given here for $p = 2$. There are additional technical difficulties for odd primes p that make the basic ideas less transparent, so the case $p > 2$ will be treated in a separate paper.

This paper is intended to make one part of my habilitation thesis [9] available to a wider audience. I thank Dr. Alexander Zimmermann for pointing out to me reference [6].

2 Generalities.

Throughout the paper let K be a finite extension of $\mathbb{Q}_p$, R its ring of integers with maximal ideal πR and residue class field $k := R/\pi R$.



Let A be a finite-dimensional semisimple K-algebra

$$A = \bigoplus_{t=1}^{s} A\epsilon_t \cong \bigoplus_{t=1}^{s} K_t^{n_t \times n_t}$$

where $\epsilon_1,\dots,\epsilon_s$ are the central primitive idempotents of A and K_t are K-division algebras.

This section develops a language for describing the ring theoretic structure of group rings RG of finite groups G up to Morita equivalence. Group rings are certain R-orders Λ in a semisimple K-algebra $K \otimes_R \Lambda =: A$.

It turns out that it is easier to describe the overorder

$$\Gamma := \bigoplus_{t=1}^{s} \Lambda \epsilon_t$$

of Λ, the direct sum of the projections of Λ into the simple components of A. If the decomposition numbers of RG are ≤ 1 (and R is big enough), then the order Γ is a so called graduated order (see Definition 2.1). Then one may describe Γ by purely combinatorical data, which also allows one to read off the Λ-lattices in the irreducible A-modules. A language for describing such graduated orders is developed in [10] and will be repeated briefly in section 2.1.

The main tool for computing Λ and Γ is the observation that group rings and their ring direct summands are symmetric orders (see Definition 2.4). This means that $\Lambda = \Lambda^{\#}$ is a self dual lattice with respect to some associative symmetric bilinear form on A. The knowledge of this form allows one in particular to calculate the index of Λ in a maximal overorder in A.

Let $J(\Lambda)$ denote the Jacobson radical of Λ, the smallest Λ-ideal I in Λ such that Λ/I is semisimple. Then $\Lambda/J(\Lambda)$ is a semisimple k-algebra and one can lift the central primitive idempotents of $\Lambda/J(\Lambda)$ to a system $e_1, \ldots, e_h$ of orthogonal idempotents in Λ with $1 = \sum_{i=1}^{h} e_i$ (see e.g. [11], Theorem 6.19). Then one obtains a direct sum decomposition

$$\Lambda = \bigoplus_{i,j=1}^{h} e_i \Lambda e_j .$$

Under certain conditions one can embed the summands $e_i \Lambda e_j$ simultaneously into a commutative K-algebra E (isomorphic to the center of A) such that the multiplication $e_i \Lambda e_j \times e_j \Lambda e_l \to e_i \Lambda e_l$ can be performed in E. This is described in Section 2.3.

2.1 Graduated orders.

Definition 2.1 *An R-order $\Gamma \subset A$ is called* graduated *if there are orthogonal idempotents $e_1, \ldots, e_h \in \Gamma$ satisfying $e_i e_j = \delta_{ij} e_i$ and $1 = \sum_{i=1}^{h} e_i$ such that $e_i \Gamma e_i$ is a maximal order in $e_i A e_i$.*

Let Γ be a graduated order in A. Then Γ contains the central primitive idempotents $\epsilon_1, \ldots, \epsilon_s \in \Gamma$ and each order $\Gamma \epsilon_t$ is a graduated order in the simple algebra $A \epsilon_t$.

Definition 2.2 *Let Γ be a graduated order in the simple K-algebra $A = D^{n \times n}$ and Ω the maximal R-order in the division algebra D with maximal ideal $\mathcal{P}$. Then* *there are* $h, n_1, \ldots, n_h \in \mathbb{N}$ *(*$n = n_1 + \ldots + n_h$*) and* $M = (m_{ij}) \in \mathbb{Z}_{\geq 0}^{h \times h}$ *such that* Γ *is conjugated to*

$$\Lambda(\Omega, n_1, \ldots, n_h, M) :=$$
$$\{X = (x_{ij})_{i,j=1,\ldots,h} \in D^{n \times n} \mid x_{ij} \in (\mathcal{P}^{m_{ij}})^{n_i \times n_j} \text{ for all } 1 \leq i, j \leq h\}.$$

If $\Gamma/J(\Gamma) \cong \oplus_{i=1}^{h} (\Omega/\mathcal{P})^{n_i \times n_i}$ *then* $m_{ii} = 0$, $m_{ij} + m_{ji} > 0$ *and* $m_{ij} + m_{jl} \geq m_{il}$ *for all* $1 \leq l, i \neq j \leq h$. *In this case* M *is called an* exponent matrix *of* Γ.

The Γ-lattices in the simple A-module can be easily described by means of its exponent matrix M, see [10], Remark (II.4). One can always conjugate Γ such that $m_{1j} = 0$ for all $1 \leq j \leq h$.

From [10], Proposition (IV.1) one finds

Lemma 2.3 *Let* $M \in \mathbb{Z}^{h \times h}$ *be an exponent matrix of a graduated* R*-order* Γ *in the simple* K*-algebra* A. *Assume that there is an involution* $^\circ : \Gamma \to \Gamma$ *(i.e. an* R*-order antiautomorphism of order* ≤ 2*) fixing the central primitive idempotents of* $\Gamma/J(\Gamma)$. *Then*

$$m_{ij} + m_{jl} + m_{li} = m_{ji} + m_{il} + m_{lj} \text{ for all } 1 \leq i, j, l \leq h.$$

If M *is normalized such that the first row of* M *consists of* 0 *only then*

$$m_{ij} + m_{j1} = m_{ji} + m_{i1} \text{ for all } 1 \leq i, j \leq h.$$

This lemma will be applied to epimorphic images of group rings RG. The natural involution $^\circ : RG \to RG$ is the R-linear map defined by $g \mapsto g^{-1}$ for all $g \in G$. If ϵ is a central primitive idempotent of KG with $\epsilon^\circ = \epsilon$ such that $\Gamma := RG\epsilon$ is a graduated order and all p-modular constituents of the character belonging to ϵ are self dual, then Γ satisfies the conditions of Lemma 2.3.

2.2 Symmetric orders.

Definition 2.4 *An* R*-order* Λ *in* A *is called* symmetric *if there is a nondegenerate symmetric associative* K*-bilinear form* $\Phi : A \times A \to K$ *such that* Λ *is self dual with respect to* Φ, *i.e.* $\Lambda = \Lambda^{\#} = \{a \in A \mid \Phi(\Lambda, a) \subset R\}$.

One easily shows that the nondegenerate symmetric associative K-bilinear form on A are precisely the forms

$$Tr_u : A \times A \to K, (a, b) \mapsto \sum_{t=1}^{s} tr_{red}(au\epsilon_t b)$$

where $u \in Z(A)^*$ and tr_{red} denotes the reduced trace of $A\epsilon_t$ to K.

Example. Let G be a finite group. Then RG is a symmetric order in $A = KG$ with respect to $|G|^{-1}$ times the regular trace bilinear form. If $\chi_t(1)$ denotes the dimension of an absolutely irreducible constituent of the simple $KG\epsilon_t$-module, then this associative symmetric bilinear form equals Tr_u, where $u = |G|^{-1}\sum_{t=1}^{s}\chi_t(1)\epsilon_t$.

Lemma 2.5 *([14], Proposition (1.6.2)) If Λ is a symmetric R-order with respect to Φ and e, f are idempotents in Λ then $\Phi_{|(e\Lambda f)\times(f\Lambda e)}$ is a nondegenerate R-bilinear pairing. In particular $e\Lambda e$ is a symmetric order.*

2.3 A language for describing certain basic orders.

Let Δ be an R-order in A. In this section it is assumed that $k = R/\pi R$ is a splitting field for $k \otimes_R \Delta$ and that the division algebras K_t are commutative. Let $P_1, \ldots, P_h$ represent the isomorphism classes of projective indecomposable Δ right modules.

Then Δ is Morita equivalent to

$$\Lambda := \mathrm{End}_\Delta(P_1 \oplus \ldots \oplus P_h) = \bigoplus_{i,j=1}^{h} \mathrm{Hom}_\Delta(P_i, P_j)$$

and Λ is a basic order in the sense that the simple Λ-modules are one dimensional vector spaces over k.

Since there is an idempotent $e \in \Delta$ such that $\Lambda \cong e\Delta e$, Lemma 2.5 shows that Λ is symmetric if Δ is symmetric. Note that the module categories of Δ and Λ are equivalent. In particular the decomposition numbers of Δ and Λ are equal. We assume that for $1 \le i \le h$ the endomorphism rings $\mathrm{End}_\Delta(P_i)$ are commutative which is equivalent to say that the decomposition numbers of Δ are ≤ 1.

The main new idea for describing the order Λ is to embed the R-lattices $\mathrm{Hom}_\Delta(P_i, P_j)$ simultaneously for all $1 \le i, j \le h$ into a commutative finite-dimensional K-algebra E such that the multiplication $\mathrm{Hom}_\Delta(P_i, P_j) \times \mathrm{Hom}_\Delta(P_j, P_l) \to \mathrm{Hom}_\Delta(P_i, P_l)$ can be performed in E.

To this purpose let

$$V := \bigoplus_{t=1}^{s} V_t$$

be the sum over a system of representatives of the isomorphism classes of simple A-modules and

$$E := \mathrm{End}_A(V) \cong \bigoplus_{t=1}^{s} K_t \cong Z(A).$$

Let $1 \le j \le h$. Since $\mathrm{End}_\Delta(P_j)$ is commutative, the A-module V has a unique A-submodule isomorphic to $K \otimes_R P_j$ and up to isomorphism a unique Δ-sublattice isomorphic to P_j. For all $1 \leq j \leq h$ choose an embedding

$$\varphi_j : P_j \hookrightarrow V.$$

Let Q_j be the unique A-invariant complement of $K \otimes_R \varphi_j(P_j)$ in V,

$$V = (K \otimes_R \varphi_j(P_j)) \oplus Q_j.$$

Then the Δ-homomorphisms $\varphi \in \mathrm{Hom}_\Delta(P_j, P_i)$ for $1 \leq i, j \leq h$ are considered as elements of E by letting

$$\varphi_{|Q_j} = 0.$$

Definition 2.6 *For $i = 1, \ldots, h$ let $\varphi_i^{-1} : V \to K \otimes_R P_i$ be the right inverse of φ_i with $\varphi_i^{-1}(Q_i) = 0$. Then for $1 \leq i, j \leq h$ there are embeddings*

$$\mathrm{Hom}_\Delta(P_i, P_j) \hookrightarrow E, \ \varphi \mapsto \varphi_i^{-1}\varphi\varphi_j.$$

Via these embeddings $\mathrm{Hom}_\Delta(P_i, P_j)$ is viewed as a subset

$$\Lambda_{ij} := (\varphi_i^{-1})\mathrm{Hom}_\Delta(P_i, P_j)\varphi_j \subset E.$$

Remark 2.7 *For $1 \leq i \neq j \leq h$ the endomorphism ring $\mathrm{End}_\Delta(P_j)$ is canonically (i.e. independent of the choice of φ_j) embedded into E, whereas the embedding $\mathrm{Hom}_\Delta(P_i, P_j) \hookrightarrow E$ depends on the choice of φ_i and φ_j.*

For simplicity we now assume that K is a splitting field for A. Then $K_t = K$ for all $1 \leq t \leq s$ and the central primitive idempotents $\epsilon_1, \ldots, \epsilon_s$ form a canonical K-basis of E.

Definition 2.8 *Let $\varphi = \sum_{t=1}^{s} a_t\epsilon_t \in E$ with $a_t \in K$. The fractional R-ideal $\sum_{t=1}^{s} a_t R$ is called the* norm *of φ,*

$$n(\varphi) := \sum_{i=t}^{s} a_t R \subseteq K.$$

The norm has a certain multiplicative property.

Remark 2.9 *If $\varphi, \psi \in E - \{0\}$ then*

$$n(\varphi)n(\psi) \text{ divides } n(\varphi\psi)$$

and for $i \in \mathbb{N}$

$$n(\varphi^i) = n(\varphi)^i.$$

One may characterize the unit groups of the local rings Λ_{ii} (cf. Definition 2.6) with help of the norm.

Lemma 2.10 *For $1 \leq i \leq h$ the unit group Λ_{ii}^* of the local ring Λ_{ii} is*

$$\Lambda_{ii}^* = \{\varphi \in \Lambda_{ii} \mid n(\varphi) = R\}.$$

Proof. Let $x \in \Lambda_{ii}$ with $n(x) = R$. Then $n(x^j) = R$ and hence $x^j \notin \pi\Lambda_{ii}$ for all $j \in \mathbb{N}$. Therefore x does not lie in the unique maximal ideal of Λ_{ii} and is a unit. The other inclusion is trivial since $n(id_{|P_i}) = R$. □

Since for $i \neq j$ the modules P_i and P_j are not isomorphic one gets the following remark from Lemma 2.10.

Remark 2.11 *Let $1 \leq i \neq l \leq h$, $0 \neq \varphi \in \Lambda_{il} \subset E$, and $0 \neq \psi \in \Lambda_{li} \subset E$. Then $\varphi\psi = \psi\varphi \in \Lambda_{ii} \cap \Lambda_{ll}$ with*

$$\pi R \supseteq n(\varphi\psi).$$

Assume now that Δ (and hence Λ) is a symmetric order with respect to the associative bilinear form Tr_u, $u = \sum_{t=1}^s u_t\epsilon_t \in E$, $u_t \in K$.

Some additional notation is needed: If $L \subset M$ are two R-lattices with $M/L \cong \oplus_{i=1}^t R/\pi^{x_t}R$ the index of L in M is the ideal $[M : L] := \pi^{x_1+\ldots+x_t}R$.

For $1 \leq i \leq h$ let

$$c_i := \{1 \leq t \leq s \mid \epsilon_t P_i \neq 0\}$$

denote the constituents of the KG-module $K \otimes_R P_i$.

Lemma 2.12 *If $(\psi_1, \ldots, \psi_l)$ is an R-basis of Λ_{jj}, then*

$$(\prod_{i=1}^l n(\psi_i))^2 \text{ divides } \prod_{t \in c_j} u_t^{-1}R.$$

Proof. Let $M := \oplus_{t \in c_j} R\epsilon_t$ be the maximal R-order in $K \otimes_R \Lambda_{jj}$. Then the dual of M with respect to Tr_u is $M^\# = \oplus_{t \in c_j} u_t^{-1}R\epsilon_t$. Since $M^\# \subseteq \Lambda_{jj} = \Lambda_{jj}^\# \subseteq M$ with $[\Lambda_{jj} : M^\#] = [M : \Lambda_{jj}]$ one has

$$[M : \Lambda_{jj}]^2 = [M : M^\#] = \prod_{t \in c_j} u_t^{-1}R.$$

The Lemma follows, because $\prod_{i=1}^l n(\psi_i)$ divides $[M : \Lambda_{jj}]$. □

3 The group ring $\mathbb{Z}_2[\zeta_{2^f-1}]SL_2(2^f)$.

Let G be a finite group and R and k be as in Section 2. This section presents a method for obtaining the ring theoretic structure of the integral group ring RG from the group algebra kG. Assume that k is a splitting field for kG. Then one usually describes the finite-dimensional k-algebra kG by giving a presentation of the Morita equivalent basic algebra $\overline{\Lambda} := \mathrm{End}_{kG}(\overline{P_1} \oplus \ldots \oplus \overline{P_h})$, where $\overline{P_1}, \ldots, \overline{P_h}$ are the projective indecomposable kG-modules. $\overline{\Lambda}$ is generated by $id_{\overline{P_i}} \in \mathrm{End}_{kG}(\overline{P_i})$ $(1 \le i \le h)$ and preimages in $\mathrm{Hom}_{kG}(\overline{P_j}, \overline{P_i})$ of a k-basis of $\mathrm{Hom}_{kG}(\overline{P_j}, J(kG)\overline{P_i})/\mathrm{Hom}_{kG}(\overline{P_j}, J(kG)^2\overline{P_i})$ $(1 \le i, j \le h)$ (see [3], Proposition 4.1.7) usually encoded as vertices and arrows in the Ext-quiver. This generating set can be lifted to obtain a generating set of $\Lambda := \mathrm{End}_{RG}(P_1 \oplus \ldots \oplus P_h)$, where P_i is the projective RG-module with $P_i/\pi P_i = \overline{P_i}$ $(i = 1, \ldots, h)$ and the lifts of the generators in $\mathrm{Hom}_{kG}(\overline{P_i}, \overline{P_j})$ lie in $\mathrm{Hom}_{RG}(P_i, P_j)$ $(1 \le i, j \le h)$. Now Remark 2.11 gives upper bounds on the norm of the basis elements of $\mathrm{End}_{RG}(P_i)$ obtained as product of the generators. The fact that $\mathrm{End}_{RG}(P_i)$ is a symmetric order yields lower bounds on these norms.

In the particular situation of this section upper and lower bounds coincide.

So let $3 \le f \in \mathbb{N}$, R be the ring of integers in the unramified extension K of degree f of $\mathbb{Q}_2$ and $k := R/2R \cong \mathbb{F}_{2^f}$ the residue class field. Let $G := SL_2(2^f)$ denote the group of 2×2-matrices over k of determinant 1. Then (K, R, k) is a 2-modular splitting system for G. Since the decomposition numbers of RG are ≤ 1 (cf. [5], Corollary 2.8), the order $\oplus_{i=1}^{s} \epsilon_i RG$, where $\epsilon_1, \ldots, \epsilon_s$ are the central primitive idempotents of KG, is a graduated order in KG, the graduated hull of RG. Therefore the methods of the previous section can be applied to describe RG. In particular the graduated hull of RG has a very nice description given in Theorem 3.15.

Since an explicit presentation of kG is used to obtain information on the group ring RG, the description of kG given in [6] is repeated in the first paragraph.

3.1 The group algebra in characteristic 2

Steinberg's tensor product theorem establishes a bijection between the simple kG-modules and the subsets of $N := \{1, \ldots, f\}$: let M_1 be the natural kG-module k^2 and let F be the Frobenius automorphism $F : k \to k; x \mapsto x^2$ of k. For $i = 0, \ldots, f-1$ one defines M_{i+1} to be the set M_1 with scalar multiplication $am := F^i(a)m$ for $a \in k$. Then the simple kG-modules are the tensor products

$$M_I := \otimes_{i \in I} M_i$$

where I runs through the subsets of N. Note that $dim_k(M_I) = 2^{|I|}$. In particular $M_\emptyset$ is the trivial kG-module and M_N is the projective simple kG-module, and hence lies in a block of defect zero.

The projective kG-modules are described in [1]. The projective cover of the simple kG-module M_I is denoted by $\overline{P_I}$ $(I \subseteq N)$. Then by Theorem 1 in [1]

$$\overline{P_I} = M_N \otimes M_{N-I}, \text{ if } \emptyset \ne I \subseteq N$$

and

$$\overline{P_\emptyset} \oplus M_N = M_N \otimes M_N.$$

Alperin also calculates the Ext-groups between the simple kG-modules. Koshita [6] extends this result to give a presentation of the basic algebra that belongs to kG by describing the homomorphism spaces between the projective indecomposable kG-modules explicitly.

If $I, I' \subset N$ then $I + I' := I \cup I' - I \cap I'$ denotes the symmetric difference and for elements $i, j \in N$ let $i + j \in N$ (resp. $i - j \in N$) be the element of N, that is congruent to $i + j \in \mathbb{Z}$ (bzw. $i - j \in \mathbb{Z}$) modulo f. Then one has the following theorem.

Theorem 3.1 *([6]) Let $f \geq 3$ and*

$$\overline{\Lambda} := \mathrm{End}_{kG}(\oplus_{N \neq I \subset N} \overline{P_I})$$

be the basic algebra belonging to the principal block of kG. Let Q be the quiver with vertices corresponding to the proper subsets of N and arrows

$$\alpha_{i,I} : I + \{i\} \to I \text{ for all } I \subseteq N,\ i \in N,\ i - 1 \notin I.$$

Let kQ be the path algebra of Q. Then the paths from I to $J = I + \{i_1\} + \ldots + \{i_a\}$ are written as

$$(I|i_1, \ldots, i_a|J) := \alpha_{i_1, I+\{i_1\}} \alpha_{i_2, I+\{i_1\}+\{i_2\}} \cdots \alpha_{i_a, J}.$$

$(I||I)$ is the idempotent in kQ corresponding to the vertex I. With this notation let X be the ideal of kQ generated by

$$(I + \{i\} + \{j\}|i, j|I) - (I + \{i\} + \{j\}|j, i|I)\ (i - 1, j - 1 \notin I,\ j \neq i - 1, i, i + 1)$$

$$(I|i, i|I)\ (i - 1 \notin I, i \in I)$$

$$(I + \{i + 1\}|i + 1, i, i|I) - (I + \{i + 1\}|i, i, i + 1|I)\ (i - 1, i \notin I)$$

$$(I + \{i + 1\}|i, i + 1, i|I)\ (i - 1 \notin I, i \in I).$$

Then there is an epimorphism

$$\Psi : kQ \to \overline{\Lambda}$$

with kernel X i.e. $\overline{\Lambda} \cong kQ/X$.

Proposition 3 in [6] determines a k-basis for $\mathrm{End}_{kG}(\overline{P_I})$.

Definition 3.2 *For $i \notin I \subseteq N$ let*

$$\omega_{I,i} := \Psi((I|j, j + 1, \ldots, i - 1, i, i, i - 1, \ldots, j + 1, j|I))$$

where $j := j(I, i)$ is the unique element of N such that $j - 1 \notin I$ and $J := J(I, i) := \{j, j + 1, \ldots, i - 1\} \subseteq I$. If $i - 1 \notin I$, then $j := i$, $J = \emptyset$ and

$$\omega_{I,i} := \Psi((I|i, i|I)).$$

The length *of $\omega_{I,i}$ is the length of the corresponding path in Q,*

$$l(I, i) := 2(|J| + 1).$$

The elements $\omega_{I,i}$ are endomorphisms of $\overline{P_I}$. Since the decomposition numbers of RG are 0 or 1 ([5], Corollary 2.8), the endomorphism rings of the projective indecomposable kG-modules are commutative. Therefore

$$\omega_{I,T} := \prod_{i \in T} \omega_{I,i}$$

for subsets $T \subseteq N - I$ is well defined.

Proposition 3.3 *([6], Proposition 3) Let $I \subset N$ be a proper subset of N. The elements $\omega_{I,T}$ where T runs through the subsets of $N-I$ form a k-basis of $\mathrm{End}_{kG}(\overline{P_I})$.*

To describe the vector spaces $\mathrm{Hom}_{kG}(\overline{P_H}, \overline{P_I})$ for $I, H \subset N$ one needs further elements of kQ.

Definition 3.4 *Let $H \subset I \subset N$, such that there is a path in Q from H to I of length $|I - H|$. Then let $\omega_{H \subset I}$ be the image of such a path under Ψ and $\omega_{I \supset H}$ be the image of the corresponding path from I to H of the same length.*

The next lemma follows from [6], Proposition 3.

Lemma 3.5 *Let $H, I \subset N$ with $\mathrm{Hom}_{kG}(\overline{P_H}, \overline{P_I}) \neq 0$. Then*

$$\mathrm{Hom}_{kG}(\overline{P_H}, \overline{P_I}) = \omega_{H \supset H \cap I} \mathrm{End}_{kG}(\overline{P_{H \cap I}}) \omega_{H \cap I \subset I}.$$

3.2 The integral group ring RG.

Now this characteristic 2 information is lifted to the characteristic 0 situation to obtain the R-order RG nearly up to Morita equivalence. So let

$$\Lambda := \mathrm{End}_{RG}(\oplus_{N \neq I \subset N} P_I),$$

where P_I is the projective indecomposable RG-module with head M_I ($I \subset N$), be the basic order that is Morita equivalent to the principal block of RG.

As in Section 2.3 let V be the sum of all irreducible KG-modules in the principal block and $E := \mathrm{End}_{KG}(V)$. Let $\epsilon_1, \ldots, \epsilon_s$ be the central primitive idempotents of KG that belong to the principal block of RG. These idempotents are identified with the primitive idempotents of E. If $I \subset N$ then

$$c_I := \{1 \leq t \leq s \mid \epsilon_t P_I \neq 0\}$$

denotes the indices of the irreducibles KG-modules that occur in $K \otimes_R P_I$. The sets c_I are explicitly described in [5]. In particular $c_\emptyset = \{1, \ldots, s\}$ and hence $V \cong K \otimes_R P_\emptyset$.

Using the fact that Λ is a symmetric order, one gets:

Lemma 3.6 *Let $I \subset N$ with $|N - I| =: n$. Then $|c_I| = 2^n = dim_R(\mathrm{End}_{RG}(P_I))$ and $\mathrm{End}_{RG}(P_I)$ is a sublattice of $\oplus_{t\in c_I} R\epsilon_t$ of index $2^{2^{n-1}f}R$.*

Proof. Let $M := \oplus_{t\in c_I} R\epsilon_t$ be the maximal R-order in $K \otimes_R \mathrm{End}_{RG}(P_I)$. Now $\mathrm{End}_{RG}(P_I)$ is a symmetric order with respect to the form Tr_u where

$$u := |G|^{-1} \sum_{t\in c_I} \chi_t(1)\epsilon_t,$$

and $\chi_t(1)$ is the degree of the irreducible character of G belonging to ϵ_t. Since $\chi_t(1) \in R^*$ is odd, the dual of M with respect to Tr_u is of index $(2^f)^{(2^n)}R$ in M. Hence $[M : \mathrm{End}_{RG}(P_I)] = \sqrt{2^{f2^n}}R = 2^{2^{n-1}f}R$. □

Now suitable lifts $\beta'_{I,T} \in \Lambda$ of the elements $\omega_{I,T}$ from Definition 3.2 are constructed.

Definition 3.7 *(i) For $i-1 \notin I \subset N$ let $\varphi_{I,i} \in \mathrm{Hom}_{RG}(P_{I+\{i\}}, P_I)$ be a preimage of $\Psi(\alpha_{i,I})$.*

(ii) For $i \notin I \subseteq N$ let $\beta'_{I,i} \in \mathrm{End}_{RG}(P_I)$ be defined similarly as $\omega_{I,i}$ using the $\varphi_{I,i}$ instead of $\Psi(\alpha_{i,I})$: If $i-1 \in I$, then let $j := j(I,i)$ and $J := J(I,i)$. Then

$$\beta'_{I,i} := \varphi_{I+\{j\},j}\varphi_{I-\{j,j+1\},j+1}\cdots\varphi_{I-J+\{i\},i}\varphi_{I-J,i}\varphi_{I-J+\{i-1\},i-1}\cdots\varphi_{I-\{j\},j+1}\varphi_{I,j}.$$

If $i-1 \notin I$ then

$$\beta'_{I,i} := \varphi_{I+\{i\},i}\varphi_{I,i}.$$

For any subset $T \subseteq N - I$ define

$$\beta'_{I,T} := \prod_{i\in T} \beta'_{I,i} \in \mathrm{End}_{RG}(P_I).$$

Since $\mathrm{End}_{RG}(P_I)$ is commutative, the definition does not depend on the ordering of the factors.

(iii) If $H \subset I \subset N$, such that there is a path $\omega = \alpha_{i_1,I_1}\dots\alpha_{i_l,I_l} \in Q$ from H to I and a path $\omega' = \alpha_{j_1,J_1}\dots\alpha_{j_l,J_l} \in Q$ from I to H of length $l := |I - H|$. Then let $\beta'_{H\subset I} := \prod_{m=1}^{l} \varphi_{I_m,i_m}$ and $\beta'_{I\supset H} := \prod_{m=1}^{l} \varphi_{J_m,j_m}$.

From Proposition 3.3 one now gets immediately

Corollary 3.8 *$(\beta'_{I,T}, (T \subseteq N - I))$ is an R-basis of the R-lattice $\mathrm{End}_{RG}(P_I)$.*

The following lemma is the crucial point in the investigation of Λ.

Lemma 3.9 *For $I \subset N$ and $T \subset N - I$*

$$n(\beta'_{I,T}) = 2^{l(I,T)}$$

where $l(I,T) := \sum_{i \in T} l(I,i)/2$.

<u>Proof.</u> Let $i \in N - I$ and $l := l(I,i)/2$. Then

$$\beta'_{I,i} = f_1 \dots f_l g_l \dots g_1$$

is a product of $f_j \in \mathrm{Hom}_{RG}(P_{I_j}, P_{I_{j+1}})$ and $g_j \in \mathrm{Hom}_{RG}(P_{I_{j+1}}, P_{I_j})$ for certain pairwise distinct subsets $I_1, \dots, I_{l+1}$ of N. In the commutative ring E this product can be evaluated as

$$\beta'_{I,i} = (f_1 g_1)(f_2 g_2) \dots (f_l g_l).$$

According to Remark 2.11 the norm $n(f_j g_j)$ is divisible by 2. Then Remark 2.9 says that 2^l divides $n(\beta'_{I,i})$ and therefore $2^{l(I,T)}$ divides $n(\beta'_{I,T})$.

On the other hand let $n := |N - I|$. Then

$$\sum_{T \subseteq N-I} l(I,T) = \sum_{T \subseteq N-I} \sum_{i \in T} l(I,i)/2 = 1/2 \sum_{i \in N-I} l(I,i) 2^{n-1} = f 2^{n-1}.$$

Hence $n(\beta'_{I,T})$ divides $2^{l(I,T)}$ by Lemma 3.6 and Lemma 2.12. □

In particular if $T = \{i\}$ and $i, i-1 \notin I \subset N$ this crucial lemma yields $n(\beta'_{I,i}) = 2$. But

$$\beta'_{I,i} = \varphi_{I+\{i\},i} \varphi_{I,i} = \varphi_{I,i} \varphi_{I+\{i\},i} \in 2\mathrm{End}_{RG}(P_{I+\{i\}}),$$

by Theorem 3.1 since $(I + \{i\} | i, i | I + \{i\}) \in X$. So Lemma 2.10 implies that $\beta'_{I,i}/2 \in \mathrm{End}_{RG}(P_{I+\{i\}})^*$ is a unit. Hence one gets the following lemma.

Lemma 3.10 *If $i-1, i \notin I$, then $\varphi_{I,i}$ is injective and $\beta'_{I,\{i\}} \in 2(\mathrm{End}_{RG}(P_{I+\{i\}})^*)$. Therefore there is a unit $u_{I,i} \in \mathrm{End}_{RG}(P_{I+\{i\}})^*$, such that*

$$u_{I,i} \beta'_{I,\{i\}} = 2id_{P_{I+\{i\}}} \in \mathrm{End}_{RG}(P_I).$$

Definition 3.11 *For $I \subset N$ let $\mathrm{pr}_I := \sum_{j \in c_I} \epsilon_j \in E$ be the identity on P_I. Let $i \notin I \subset N$. If $i - 1 \notin I$, define*

$$\beta_{I,i} = 2\mathrm{pr}_{I+\{i\}}.$$

Otherwise let $j := j(I,i)$ and $J := J(I,i)$. Then

$$\beta_{I,i} := 2^{|J|+1} \mathrm{pr}_{I-J+\{i\}} \mathrm{pr}_I.$$

For $T \subset N - I$ let

$$\beta_{I,T} := \prod_{i \in T} \beta_{I,i}$$

where the empty product

$$\beta_{I,\emptyset} := \mathrm{pr}_I$$

is the unit element in $\mathrm{End}_{RG}(P_I)$.

Theorem 3.12 *Let $H, I \subset N$.*

(a) The $\beta_{I,T}$ with $T \subset N - I$ form an R-basis of the lattice $\mathrm{End}_{RG}(P_I)$.

(b) If $\mathrm{Hom}_{RG}(P_H, P_I) \neq \{0\}$ then

$$\mathrm{Hom}_{RG}(P_H, P_I) \cong (\mathrm{pr}_H(\mathrm{End}_{RG}(P_{H\cap I}))\mathrm{pr}_I)$$

as $\mathrm{End}_{RG}(P_H) - \mathrm{End}_{RG}(P_I)$-bimodule.

Proof. (a) Let $I \subset N$ and $i \in N - I$. If $i - 1 \notin I$, then $\beta_{I,i} = \beta'_{I,i} u_{I,i} \in \mathrm{End}_{RG}(P_I)$ by Lemma 3.10. If $i - 1 \in I$, then let $j := j(I, i)$ and $J := J(I, i)$ be as in Definition 3.2. For $l = j, \dots, i - 1$ define $I_l := I - \{j, \dots, l\}$ and let $u_l := u_{I_l, l+1}$ be the unit of Lemma 3.10. It easily follows from [5] that

$$c_I \subset c_{I-\{j\}} \subset \dots \subset c_{I-J}.$$

Therefore

$$\beta'_{I,i} \prod_{l=j}^{i-1} u_l = (\varphi_{I-\{j\},j}\varphi_{I,j}u_j)(\varphi_{I-\{j,j+1\},j+1}\varphi_{I-\{j\},j+1}u_{j+1}) \dots$$

$$\dots (\varphi_{I-J,i-1}\varphi_{I-J+\{i-1\},i-1}u_{i-1})(\varphi_{I-J+\{i\},i}\varphi_{I-J,i}u_{I-J,i}) =$$

$$(2\mathrm{pr}_I)(2\mathrm{pr}_{I-\{j\}}) \dots (2\mathrm{pr}_{I-J})(2\mathrm{pr}_{I-J+\{i\}}) = 2^{|J|+1}\mathrm{pr}_I \mathrm{pr}_{I-J+\{i\}}.$$

Hence the elements $\beta_{I,T}$ with $T \subset N - I$ lie in the ring $\mathrm{End}_{RG}(P_I)$.

For $T \subset N - I$ let $a(I,T)'_j, a(I,T)_j \in R$ $(j = 1, \dots, s)$ be such that $\beta'_{I,T} = \sum_{j=1}^{s} a(I,T)'_j \epsilon_j$ and $\beta_{I,T} = \sum_{j=1}^{s} a(I,T)_j \epsilon_j$. Since $\beta_{I,T}$ is obtained from $\beta'_{I,T}$ by multiplication with units in local rings, there is $k_{I,T} \in R^*$ with

$$k_{I,T}a(I,T)_j \equiv a(I,T)'_j \pmod{2n(\beta'_{I,T})}$$

for all $1 \leq j \leq s$. Replacing $\beta_{I,T}$ by $k_{I,T}\beta_{I,T}$ we assume that $k_{I,T} = 1$. Lemma 3.9 yields that $n(\beta_{I,T}) = n(\beta'_{I,T}) = 2^{l(I,T)}$ and the product of the norms is

$$\prod_{T \subset N-I} n(\beta_{I,T}) = 2^{2^{n-1}f}$$

the index of $\mathrm{End}_{RG}(P_I)$ in $\oplus_{j\in c_I} R\epsilon_j$. Here $n := |N - I|$. Let $B' := (a(I,T)'_j)_{T,j}$, $B := (a(I,T)_j)_{T,j}$ and $D := diag(n(\beta'_{I,T}) \mid T \subseteq N - I)$. Then $B' = DU$ for some $U \in GL_{2^n}(R)$ and $B = DV$ with $V \equiv U \pmod{2R}$. Therefore the determinant of V is also a unit in R and $(\beta_{I,T} \mid T \subseteq N - I)$ is an R-basis of $\mathrm{End}_{RG}(P_I)$.

(b) By Lemma 3.5

$$\mathrm{Hom}_{RG}(P_H, P_I) = \beta'_{H\supset H\cap I}\mathrm{End}_{RG}(P_{H\cap I})\beta'_{H\cap I\subset I}.$$

Multiplication with $\beta'_{H\supset H\cap I}\beta'_{H\cap I\subset I} \in E$ induces the desired bimodule isomorphism. □

Remark 3.13 *This theorem shows that the endomorphism rings of the projective indecomposable $RSL_2(2^f)$-modules have a rational structure: Let $I \subset N$ and $c_I = \{t_1, \ldots, t_n\}$. Then there is a (symmetric) $\mathbb{Z}_2$-order*

$$O_I = \bigoplus_{T \subset N - I} \mathbb{Z}_2 \beta_{I,T} \subset \oplus_{i=1}^n \mathbb{Z}_2 \epsilon_{t_i}$$

with $R \otimes_{\mathbb{Z}_2} O_I = \mathrm{End}_{RG}(P_I)$.

In particular the order $O_\emptyset$ is isomorphic to the group ring $\mathbb{Z}_2(C_2^f)$ of the Sylow 2-subgroup of G:

Proposition 3.14 *Let $O_\emptyset = \oplus_{T \subset N} \mathbb{Z}_2 \beta_{\emptyset,T}$ be as in the remark above. Then*

$$O_\emptyset \cong \mathbb{Z}_2(C_2^f).$$

In particular the endomorphism ring of $P_\emptyset$

$$\mathrm{End}_{RG}(P_\emptyset) \cong R(C_2^f)$$

is isomorphic to the group ring over R of the Sylow 2-subgroup of G.

Proof. The R-order $\mathrm{End}_{RG}(P_\emptyset) \subset E$ is generated by $\beta_{\emptyset,\emptyset} = id_{P_\emptyset} = 1 \in E$ and $x_i := \beta_{\emptyset,i} = 2\sum_{t \in c_{\{i\}}} \epsilon_t$, $i = 1, \ldots, f$. The Frobenius automorphism F acts on $\mathrm{End}_{RG}(P_\emptyset)$ mapping x_i to x_{i+1} ($i = 1, \ldots, f$) where as usual the indices are taken modulo f. With the notation of [5], the ordinary irreducible characters in the principal block of RG are $1, \eta_j, \delta_i$ where $j = 1, \ldots, 2^{f-1} - 1$ and $i = 1, \ldots, 2^{f-1}$. The Frobenius automorphism F acts on the irreducible characters η_j and δ_i by multiplying the indices with 2, where the indices of η are taken modulo $2^f - 1$ and the ones of δ modulo $2^f + 1$ and in both cases identified with the negative index. In the rest of the proof these characters are used to index the primitive idempotents of E. Then by [5]

$$x_f = 2\left(\sum_{j=1, j \text{ odd}}^{2^{f-1}-1} \epsilon_{\eta_j} + \epsilon_{\delta_j}\right).$$

Choose a generating set $(b_0, \ldots, b_{f-1})$ of C_2^f and let $0 \leq i = \sum_{j=0}^{f-1} z_j 2^j < 2^f$ with $z_j \in \{0, 1\}$. Then define the linear character χ_i of C_2^f via $\chi_i(b_j) = (-1)^{z_j}$. Let $h(i) := \sum_{j=0}^{f-2} z_j 2^j$ and define a bijection between the set of characters $\{\chi_0, \ldots, \chi_{2^f-1}\}$ and the set of characters in the principal block of G via

$$\chi_i \mapsto \begin{cases} 1 & \text{if } i = 0 \\ \eta_{h(i)} & \text{if } i > 0 \text{ and } z_{f-1} = 0 \\ \delta_{h(i)} & \text{if } z_{f-1} = 1. \end{cases}$$

This bijection induces a bijection of the primitive idempotents of E and KC_2^f and hence an isomorphism $\varphi : E \to KC_2^f$. Clearly $\chi_i(b_0) = 1$ if and only if $z_0 = 0$. Therefore one finds $\varphi(x_f) = 1 - b_0 \in \mathbb{Z}_2 C_2^f$.

The action of F on KC_2^f induced via φ is given by $b_i \mapsto b_{i+1}$ if $i = 0, \ldots, f-3$, $b_{f-2} \mapsto \sum_{i=0}^{f-2} b_i$ and $b_{f-1} \mapsto b_{f-1}$. One has $\varphi(x_1) = 1 - b_1, \ldots, \varphi(x_{f-3}) = 1 - b_{f-2}, \varphi(x_{f-2}) = 1 - \sum_{i=0}^{f-2} b_i, \varphi(x_{f-1}) = 1 - b_{f-1} \in \mathbb{Z}_2 C_2^f$. Together with $1 = \varphi(1)$ these elements span $\mathbb{Z}_2 C_2^f$, therefore $\varphi_{|O_\emptyset} : O_\emptyset \to \mathbb{Z}_2 C_2^f$ is an isomorphism. □

Note that this proposition also shows that $\mathrm{End}_{RG}(P_\emptyset)$ is also symmetric with respect to Tr_v where $v := 2^{-f} \sum_{t=1}^{s} \epsilon_t$.

Since the decomposition numbers of RG are ≤ 1, the projections $\Lambda\epsilon_t$ of Λ onto the simple components of $K \otimes_R \Lambda$ are graduated orders. From Theorem 3.12 one gets a simple description of the graduated hull $\oplus_{t=1}^{s} \epsilon_t \Lambda$ of Λ, which also yields the theorem stated in the introduction.

Theorem 3.15 *For $1 \leq t \leq s$ there is an exponent matrix $M^{(t)} = (m_{H,I}^{(t)})$ where $H, I \subset N,\ t \in c_H \cap c_I$ for $\Lambda\epsilon_t$ such that*

$$m_{H,I}^{(t)} = |H - I| \quad (\textit{ for all } H, I \textit{ such that } t \in c_H \cap c_I).$$

<u>Proof.</u> Let $M^{(t)}$ be an exponent matrix of $\Lambda\epsilon_t$ such that the row corresponding to $M_\emptyset$ consists of 0 only

$$m_{\emptyset,H}^{(t)} = 0 \text{ for all } H \subset N, t \in c_H.$$

From Lemma 3.9 it follows that

$$n(\beta'_{H \supset H\cap I} \beta'_{H\cap I \subset H}) = 2^{|H-I|}$$

and

$$n(\beta'_{I \supset H\cap I} \beta'_{H\cap I \subset I}) = 2^{|I-H|}.$$

Then Theorem 3.12 (b) implies that for $I, H \subset N$ such that $t \in c_H \cap c_I$

$$m_{H,I}^{(t)} + m_{I,H}^{(t)} = |H - I| + |I - H|.$$

In particular

$$m_{H,\emptyset}^{(t)} = |H| \text{ for all } H \subset N, t \in c_H.$$

Since the simple kG-modules are all self dual, one gets from Lemma 2.3

$$m_{H,I}^{(t)} = m_{I,H}^{(t)} - m_{I,\emptyset}^{(t)} + m_{H,\emptyset}^{(t)} = m_{I,H}^{(t)} - |I| + |H|.$$

Therefore the Theorem follows. □

Theorem 3.15 and Theorem 3.12 do not describe Λ up to Morita equivalence, because they do not give a system of simultaneous embeddings $\varphi_I : P_I \hookrightarrow P_\emptyset$

$(I \subset N)$ that determines the multiplication in Λ. If the isomorphism type of Λ is uniquely determined by that of $\Lambda/2\Lambda$, then one can show that Λ is as given in the following conjecture.

Conjecture: There are embeddings $\varphi_I : P_I \hookrightarrow P_\emptyset$, $I \subset N$, such that for all $I, H \subset N$

$$\mathrm{Hom}_{RG}(\varphi_H(P_H), \varphi_I(P_I)) = 2^{|I-(H\cap I)|}(\mathrm{pr}_H(\mathrm{End}_{RG}(\varphi_{H\cap I}(P_{H\cap I})))\mathrm{pr}_I) \subset E.$$

One easily shows using the combinatorical description of the sets c_I in [5] that the R-order $\Lambda = \mathrm{End}_{RG}(\oplus_{I\subset N} P_I)$ in the conjecture satisfies $\Lambda/2\Lambda \cong kQ/X$ as in Theorem 3.1.

Proposition 3.16 *The conjecture is true for $f \leq 6$.*

Proof. For all proper subsets $\emptyset \neq I \subset N$ choose $i \in I$ with $i-1 \notin I$. Let T be the set of such pairs (I,i). Via the monomorphism $\varphi_{I-\{i\},i} : P_I \to P_{I-\{i\}}$ in Lemma 3.10 one embeds P_I into $P_{I-\{i\}}$ for all $(I,i) \in T$, such that recursively all projective indecomposable RG-modules are embedded into $P_\emptyset$. For $I \subset N$ let $\varphi_I : P_I \hookrightarrow P_\emptyset$ denote this embedding. Then for all $(I,i) \in T$ it holds that

$$\mathrm{Hom}_{RG}(\varphi_I(P_I), \varphi_{I-\{i\}}(P_{I-\{i\}})) = \mathrm{pr}_I(\mathrm{End}_{RG}(\varphi_{I-\{i\}}(P_{I-\{i\}}))).$$

One possibility for T in the case $f=5$ is given in figure 1, which shows the Ext-quiver Q for the principal block of $\mathbb{F}_{2^5}SL_2(2^5)$. The vertices of the quiver are indexed by the projective indecomposable modules P_I, where only the elements of I are given and 0 stands for the empty set. The arrows $P_I \to P_{I+\{i\}}$ and $P_{I+\{i\}} \to P_I$ in Q are represented by one straight line. The mappings φ_I are constructed along the bold edges.

So to show the Proposition for the case $f=5$, it remains to show that the homomorphism pr_I lies in $\mathrm{Hom}_{RG}(\varphi_I(P_I), \varphi_{I-\{i\}}(P_{I-\{i\}}))$ for all thin edges $(P_I, P_{I-\{i\}})$ with $i \in I \subset N$, $i-1 \notin I$ and $(I,i) \notin T$.

We prove this for the example $I = \{2,4,5\}$ and $i=4$. Let

$$h \in \mathrm{Hom}_{RG}(\varphi_{\{2,4,5\}}(P_{\{2,4,5\}}), \varphi_{\{2,5\}}(P_{\{2,5\}}))$$

be a lift of $\Psi(\alpha_{4,\{2,5\}})$. Theorem 3.1 says that there is an $x \in \mathrm{End}_{RG}(\varphi_{\{5\}}(P_{\{5\}}))$ with

$$h = h\mathrm{pr}_{\{2,5\}} = \mathrm{pr}_{\{2,4,5\}}\mathrm{pr}_{\{4,5\}}(1+2x) = \mathrm{pr}_{\{2,4,5\}}(1+2x).$$

Now

$$2\mathrm{End}_{RG}(\varphi_{\{5\}}(P_{\{5\}})) \subset \mathrm{End}_{RG}(\varphi_{\{2,5\}}(P_{\{2,5\}})),$$

so $1+2x$ is a unit in $\mathrm{End}_{RG}(\varphi_{\{2,5\}}(P_{\{2,5\}}))$. Therefore

$$\mathrm{pr}_{\{2,4,5\}} \in \mathrm{Hom}_{RG}(\varphi_{\{2,4,5\}}(P_{\{2,4,5\}}), \varphi_{\{2,5\}}(P_{\{2,5\}})).$$

The other cases are completely analogous. If $f=6$, one additionally needs the action of the Galois group $Gal(K/\mathbb{Q}_2) \cong C_f$ on the quiver Q. □

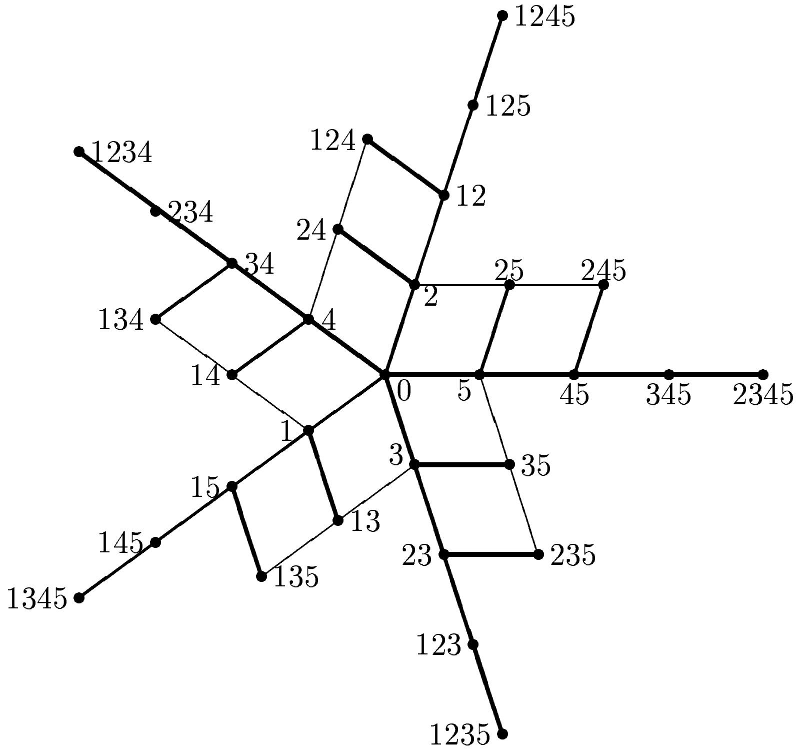


Figure 1: The Ext-quiver for the principal block of $\mathbb{F}_{2^5} SL_2(2^5)$

Remark 3.17 *If the conjecture is true, then one does not need irrationalities to describe RG. More precisely if $KG \cong \bigoplus_{t=1}^{s} K^{n_t \times n_t}$ then there is a $\mathbb{Q}_2$-algebra $A \cong \bigoplus_{t=1}^{s} \mathbb{Q}_2^{n_t \times n_t}$ and a (symmetric) $\mathbb{Z}_2$-order $\Lambda_0 \subset A$ such that $R \otimes_{\mathbb{Z}_2} \Lambda_0 = RG$.*

References

[1] J.L. Alperin, *Projective modules for $SL(2, 2^n)$*. J. Pure Appl. Algebra 15 (1979), 219-234.

[2] H.H. Andersen, J. Jørgensen, P. Landrock, *The projective indecomposable modules of $SL_2(K)$*, Proc. Lond. Math. Soc., III. Ser. 46, (1983) 38-52.

[3] D. J. Benson, *Representations and cohomology I.* Cambridge studies in advanced math. 30 (1991).

[4] R. Burkhardt, *Die Zerlegungsmatrizen der Gruppen $PSL(2, p^f)$*. J. Algebra **40**, (1976) 75-96.

[5] P.W.A.M. van Ham, T.A. Springer, M. van der Wel, *On the Cartan invariants of $SL_2(\mathbb{F}_q)$*. Comm. Alg., 10(14), (1982) 1565-1588.

[6] H. Koshita, *Quiver and Relations for $SL(2, 2^n)$ in characteristic 2*, J. Pure Appl. Algebra, 97 (1994) 313-324.

[7] M. Linckelmann, *The isomorphism problem for cyclic blocks and their source algebras.* Invent. math. 125, 265-283 (1996).

[8] G. Nebe, *The group ring of $SL_2(p^2)$ over the p-adic integers.* J. Alg. **210**, (1998) 593-613.

[9] G. Nebe, *Orthogonale Darstellungen endlicher Gruppen und Gruppenringe.* Habilitationsschrift, Aachener Beiträge zur Mathematik, Verlag Mainz Aachen, 1999

[10] W. Plesken, *Group rings of finite groups over the p-adic integers.* Springer LNM 1026 (1983).

[11] I. Reiner, *Maximal Orders.* Academic Press, 1975.

[12] K. W. Roggenkamp, *Blocks of cyclic defect and Green orders.* Comm. Alg. **20**, No. 6 (1992) 1715-1734.

[13] I. Schur, *Über die Darstellung der endlichen Gruppen durch gebrochene lineare Substitutionen.* p. 198-250 in I. Schur: *Gesammelte Abhandlungen I.* Springer Verlag 1973, resp. J. reine u. angew. Math. 132, 85-137 (1907).

[14] J. Thévenaz, *G-Algebras and Modular Representation Theory.* Oxford Science Publications (1995).

Author's address: Lehrstuhl B für Mathematik, RWTH Aachen, Templergraben 64, 52062 Aachen, Germany
e-mail: gabi@math.rwth-aachen.de