City Research Online

City, University of London Institutional Repository

This is the accepted version of the paper.

This version of the publication may differ from the final published version.

Permanent repository link: http://openaccess.city.ac.uk/13180/

Link to published version: http://dx.doi.org/10.1016/j.jpaa.2014.09.031

City Research Online: http://openaccess.city.ac.uk/   publications@city.ac.uk

Describing units of integral group rings up to commensurability [☆]

Florian Eisele, Ann Kiefer, Inneke Van Gelder

Department of Mathematics, Vrije Universiteit Brussel, Pleinlaan 2, 1050 Brussels, Belgium

Abstract

We restrict the types of 2×2-matrix rings which can occur as simple components in the Wedderburn decomposition of the rational group algebra of a finite group. This results in a description up to commensurability of the group of units of the integral group ring $\mathbb{Z}G$ for all finite groups G that do not have a non-commutative Frobenius complement as a quotient.

Keywords: Units in integral group rings, Rational group representations, Wedderburn components
2010 MSC: 16S34, 16U60, 20C05

1. Introduction

For a group G we denote by $\mathcal{U}(\mathbb{Z}G)$ the unit group of the integral group ring $\mathbb{Z}G$. Bass [1] proved that if C is a finite cyclic group, then the so-called Bass cyclic units generate a subgroup of finite index in $\mathcal{U}(\mathbb{Z}C)$. Next Bass and Milnor proved this result for finite abelian groups. This work stimulated the search for subgroups of finite index in the unit group of the integral group ring of finite non-abelian groups. For several classes of finite groups G including nilpotent groups of odd order, Ritter and Sehgal [2, 3, 4] showed that the Bass units together with the bicyclic units generate a subgroup of finite index in $\mathcal{U}(\mathbb{Z}G)$.

Later on, Jespers and Leal [5] proved that the group generated by the Bass units and the bicyclic units is of finite index in $\mathcal{U}(\mathbb{Z}G)$ for finite groups G which do not have any non-abelian homomorphic images that are Frobenius complements (equivalently, are fixed point free, see Definitions 2.4 and 2.5) and, additionally, whose rational group ring $\mathbb{Q}G$ does not have any simple components of one of the following types:

1. a 2×2-matrix ring over the rationals;

2. a 2×2-matrix ring over a quadratic imaginary extension of the rationals;

3. a 2×2-matrix ring over a non-commutative division algebra.

The reason why some simple components are excluded is that not all congruence subgroups in the corresponding special linear groups over a maximal order are generated up to finite index by elementary matrices. We will explain this in Section 2.

In this paper we give a classification of all isomorphism types of 2×2-matrix rings which actually occur as exceptional components (see Definition 2.9), and all finite groups which have such an exceptional component as a faithful Wedderburn component. This is related to the heavy classification results of Banieqbal [6] and Nebe [7], on which we opted to rely as little as possible. For the most part we use elementary techniques. Only the proof of Theorem 3.7 relies on [7], and [6] is not used at all. It should be noted that, mostly due to the use of the classification [7] instead of [6], Theorem 3.7 can serve to significantly shorten the part in the work of Caicedo and del Río ([8]) that deals with Banieqbal's classification [6].

In Theorems 3.1 and 3.5 we prove that if $\mathbb{Q}G$ has a simple component which is a 2×2-matrix ring over a quadratic imaginary extension of the rationals or a 2×2-matrix ring over a totally definite quaternion algebra over $\mathbb{Q}$, then this component is a 2×2-matrix ring over one of the following rings:

1. $\mathbb{Q}(\sqrt{-1})$, $\mathbb{Q}(\sqrt{-2})$ or $\mathbb{Q}(\sqrt{-3})$;

2. $\left(\frac{-1,-1}{\mathbb{Q}}\right)$, $\left(\frac{-1,-3}{\mathbb{Q}}\right)$ or $\left(\frac{-2,-5}{\mathbb{Q}}\right)$.

All of these fields respectively skew-fields contain a norm Euclidean maximal order (see [9, Proposition 6.4.1] and [10, Theorem 2.1]). This makes it possible to describe generators for a subgroup of finite index in $\mathrm{SL}_2(\mathcal{O})$, with $\mathcal{O}$ the maximal order in one of the algebras listed under points 1 and 2 (see Proposition 4.1). Moreover, we are able to describe an effective method to describe generators for a subgroup S of $\mathcal{U}(\mathbb{Q}G)$ which is commensurable with the group of units of $\mathbb{Z}G$ for a finite group G (i.e. $S \cap \mathcal{U}(\mathbb{Z}G)$ has finite index in both S and $\mathcal{U}(\mathbb{Z}G)$) provided that G has no epimorphism onto a non-commutative Frobenius complement. This may be seen as a generalization of the result of Jespers and Leal [5] we mentioned earlier, which gives generators for a subgroup of finite index in $\mathcal{U}(\mathbb{Z}G)$ under stronger conditions on G.

Other constructions of subgroups of finite index of $\mathcal{U}(\mathbb{Z}G)$ for some specific classes of finite groups G, using a description of the center $\mathcal{Z}(\mathcal{U}(\mathbb{Z}G))$ and a description of the matrix units in $\mathbb{Q}G$, have been given for example in [11, 12].

2. Preliminaries

We start by introducing some notations and definitions.

Definition 2.1. *Given a field K as well as two elements $a, b \in K$ we define the quaternion algebra $\left(\frac{a,b}{K}\right)$ as follows:*

$$\left(\frac{a,b}{K}\right) = \frac{K\langle i, j \rangle}{(i^2 = a, \ j^2 = b, \ ij = -ji)}.$$

2

The following classical theorem classifies quaternion algebras over number fields up to isomorphism, see [13, Chapter 3, Théorème 3.1] for a proof of this statement or the more general Hasse-Brauer-Noether-Albert Theorem in [14, Theorem 32.11].

Theorem 2.2. *Let K be a number field. If D is a quaternion algebra over K, the set $\mathrm{Ram}(D) \subset S(K)$ of places v such that D is ramified at v, i.e. such that $D \otimes_K K_v$ is not split, is a finite set with an even number of elements. Moreover, for any finite set $S \subset S(K)$ such that $|S|$ is even, there is a unique quaternion algebra with center K such that $\mathrm{Ram}(D) = S$.*

It is well known that for each finite group G there exists a splitting p-modular system in the sense of the following definition.

Definition 2.3. *If p is a prime, (E, R, F) is called a p-modular system if R is a complete discrete valuation ring of characteristic zero with maximal ideal $R\pi$ such that its residue field $F = R/R\pi$ has characteristic p and E is the field of fractions of R. It is called a p-modular splitting system for G if E and F are both splitting fields for G.*

We recall the definitions of fixed point free groups and Frobenius complements.

Definition 2.4. *A finite group F is said to be fixed point free if it has an (irreducible) complex representation ρ such that 1 is not an eigenvalue of $\rho(f)$ for all $1 \neq f \in F$.*

Definition 2.5. *A finite group G is said to be a Frobenius group if it contains a proper non-trivial subgroup H such that $H \cap H^g = \{1\}$ for all $g \in (G \setminus H)$. The group H is called a Frobenius complement in G.*

Fixed point free groups are strongly related to Frobenius complements, i.e. a finite group G is fixed point free if and only if G has an epimorphism onto a Frobenius complement [15, Theorem 18.1.v].

Definition 2.6. *Let G be a finite group.*

1. *If $H \leq G$, we set $\widehat{H} = \frac{1}{|H|}\sum_{h \in H} h$ an idempotent of $\mathbb{Q}G$. If $x \in G$ then we set $\widehat{x} = \widehat{\langle x \rangle}$.*

2. *Let g be an element of G of order n and k and m positive integers such that $k^m \equiv 1 \mod n$. Then*

$$u_{k,m}(g) = (1 + g + \cdots + g^{k-1})^m + \frac{1 - k^m}{n}(1 + g + \cdots + g^{n-1})$$

is a unit of the integral group ring $\mathbb{Z}G$ called a Bass unit.

3. *The* bicyclic units *of $\mathbb{Z}G$ are the elements of one of the following forms*

$$\beta_{g,h} = 1 + (1-g)h(1 + g + g^2 + \cdots + g^{n-1}), \ \gamma_{g,h} = 1 + (1 + g + g^2 + \cdots + g^{n-1})h(1-g),$$

where $g, h \in G$ and g has order n.

3

4. Let $\mathcal{B}_1$ denote the group generated by the Bass units of $\mathbb{Z}G$ and $\mathcal{B}_2$ the group generated by the bicyclic units of $\mathbb{Z}G$.

5. More generally, given a collection $\{e_1, ..., e_n\}$ of idempotents of $\mathbb{Q}G$, we define generalized bicyclic units

$$\beta_{i,g} = 1 + z^2(1 - e_i)ge_i, \ \gamma_{i,g} = 1 + z^2e_ig(1 - e_i),$$

where $z \in \mathbb{N}$ is chosen of minimal absolute value with respect to the property that ze_i lies in $\mathbb{Z}G$. We shall call the group generated by the various $\beta_{i,g}$ and $\gamma_{i,g}$ the group of generalized bicyclic units and also denote it by $\mathcal{B}_2$ (i.e., when we refer to $\mathcal{B}_2$, a collection of idempotents should be given at least implicitly; for the ordinary bicyclic units this system of idempotents would be formed by the elements of the form $\hat{g}$ where g ranges over all elements of G).

We recall some notions concerning the rational group algebra $\mathbb{Q}G$. Let $e_1, \ldots, e_n$ be the primitive central idempotents of $\mathbb{Q}G$, then

$$\mathbb{Q}G = \mathbb{Q}Ge_1 \oplus \cdots \oplus \mathbb{Q}Ge_n,$$

where each $\mathbb{Q}Ge_i$ is identified with the matrix ring $M_{n_i}(D_i)$ for some division algebra D_i. For every i, let $\mathcal{O}_i$ be an order in D_i. Then $M_{n_i}(\mathcal{O}_i)$ is an order in $\mathbb{Q}Ge_i$. Denote by $\mathrm{GL}_{n_i}(\mathcal{O}_i)$ the group of invertible matrices in $M_{n_i}(\mathcal{O}_i)$ and by $\mathrm{SL}_{n_i}(\mathcal{O}_i)$ its subgroup consisting of matrices of reduced norm 1.

The following proposition is a reformulation of the result of chapter 22 from [16].

Proposition 2.7. *Assume G is a finite group and let $U \leq \mathcal{U}(\mathbb{Z}G)$ be a subgroup of the unit group of the integral group ring. Let $\mathbb{Q}G = \bigoplus_{i=1}^{n} \mathbb{Q}Ge_i = \bigoplus_{i=1}^{n} M_{n_i}(D_i)$ be the Wedderburn decomposition of $\mathbb{Q}G$ and let $\mathcal{O}_i \subset D_i$ denote orders in each division ring.*
Then U is of finite index in $\mathcal{U}(\mathbb{Z}G)$ if and only if both of the following hold:

1. *The natural image of U in $K_1(\mathbb{Z}G)$ is of finite index.*

2. *For each $i \in \{1, ..., n\}$, the group U contains a subgroup of finite index in $1 \times \cdots \times 1 \times \mathrm{SL}_{n_i}(\mathcal{O}_i) \times 1 \times \cdots \times 1$, a multiplicative subgroup of $\bigoplus_{i=1}^{n} M_{n_i}(D_i)$.*

For an ideal Q_i of $\mathcal{O}_i$ we denote by $E(Q_i)$ the subgroup of $\mathrm{SL}_{n_i}(\mathcal{O}_i)$ generated by all so-called Q_i-elementary matrices, that is, $E(Q_i) = \langle I + qE_{lm} \mid q \in Q_i, \ 1 \leq l, m \leq n_i, \ l \neq m, \ E_{lm}$ the (l, m)-matrix unit$\rangle$. We summarize the following theorems [17, Theorem 21.1, Corollary 21.4], [18, Theorem 2.4, Lemma 2.6], [19, Theorem 24] and [20, Theorem].

Theorem 2.8 (Bass-Vaseršteĭn-Liehl-Venkataramana)**.** *Let Q_i be an ideal in $\mathcal{O}_i$. If $n_i \geq 3$ then $[\mathrm{SL}_{n_i}(\mathcal{O}_i) : E(Q_i)] < \infty$. If $n_i = 2$ and if D_i is different from $\mathbb{Q}$, a quadratic imaginary extension of $\mathbb{Q}$ and a totally definite quaternion algebra with center $\mathbb{Q}$, then $[\mathrm{SL}_2(\mathcal{O}_i) : E(Q_i)] < \infty$.*

Note that Kleinert [21] proved that if D_i is non-commutative then $\mathrm{SL}_1(\mathcal{O}_i)$ is finite if and only if D_i is a totally definite quaternion algebra.

Since the image of $\mathcal{B}_1$ in $K_1(\mathbb{Z}G)$ is always of finite index [1, Theorem 5], one is interested in finding additional units such that the group generated by $\mathcal{B}_1$ and these additional units satisfies condition 2 of Proposition 2.7. Often the bicyclic units can be used for this purpose, but our main focus will lie on groups G for which this is not the case.

This leads us to the definition of exceptional components. Note that this is a weaker version of the definition used in [5], since the result of Venkataramana stated in Theorem 2.8 immediately leads to a strengthening of the results of [5].

Definition 2.9. *Let G be a finite group. An exceptional component of $\mathbb{Q}G$ is a simple component of the following types:*

type 1: a non-commutative division ring other then a totally definite quaternion algebra,

type 2: a 2×2-matrix ring over the rationals, a quadratic imaginary extension of the rationals or over a totally definite quaternion algebra over $\mathbb{Q}$.

The following result is a reformulation of [5, Theorem 3.3].

Proposition 2.10. *Let G be a finite group such that $\mathbb{Q}G = \bigoplus_{i=1}^{n} M_{n_i}(D_i)$ has no exceptional components. Let $e_1, ..., e_k$ be a set of idempotents in $\mathbb{Q}G$ such that for each irreducible representation $\Delta_i : \mathbb{Q}G \to M_{n_i}(D_i)$ with $n_i > 1$ there is some index $j(i)$ such that $\Delta_i(e_{j(i)}) \notin \{0, 1\}$ (i.e. $\Delta_i(e_{j(i)})$ is a non-central idempotent in $M_{n_i}(D_i)$). Then the Bass cyclic units together with the generalized bicyclic units associated with $e_1, ..., e_k$ generate a subgroup of finite index in $\mathcal{U}(\mathbb{Z}G)$.*

We will restrict the types of exceptional components that can actually occur in group rings, and we will show that this restriction results in a more general method of constructing a subgroup of $\mathcal{U}(\mathbb{Q}G)$ which is commensurable with $\mathcal{U}(\mathbb{Z}G)$.

3. Main results

In this section we restrict the type of 2×2-matrices which can occur as simple components in the Wedderburn decomposition of $\mathbb{Q}G$ for finite groups G. We also give a classification of those finite groups which have a faithful exceptional 2×2-matrix ring component.

Theorem 3.1. *If $\mathbb{Q}G$ has a simple component which is a 2×2-matrix ring over a quadratic imaginary extension of the rationals, then this component is a 2×2-matrix ring over one of the following fields:*

1. $\mathbb{Q}(\sqrt{-1})$,

2. $\mathbb{Q}(\sqrt{-2})$ or

3. $\mathbb{Q}(\sqrt{-3})$.

Moreover, a finite subgroup G of $\mathcal{U}(M_2(K))$, where K is one of the above quadratic imaginary extension of the rationals, is solvable and $|G| = 2^a 3^b$ for $a, b \in \mathbb{N}$.

Proof. Let $K = \mathbb{Q}(\sqrt{-d})$ for a positive square-free integer d. Assume that there is a finite group G and a primitive central idempotent e of $\mathbb{Q}G$ such that the simple component $\mathbb{Q}Ge$ is isomorphic to $M_2(K)$. We can assume without loss of generality that the $\mathbb{Q}$-representation of G determined by e is faithful and hence G can be embedded into $M_2(K)$. We will identify G with its image in $M_2(K)$.

Since the characteristic polynomial of a matrix in $M_2(K)$ always has degree 2 over K and degree 4 over $\mathbb{Q}$, we conclude that the minimal polynomial of any element in G over $\mathbb{Q}$ has degree 1, 2 or 4. Moreover, for any prime p, we know that the $\mathbb{Q}$-irreducible cyclotomic polynomial $\frac{X^p-1}{X-1}$ divides the minimal polynomial of $g \in G$ over $\mathbb{Q}$ whenever g has order p. Therefore we deduce that if the order of an element of G is a prime, then this prime must be equal to either 2, 3 or 5, as these are the only primes whose associated cyclotomic polynomials have admissible degrees. Hence $|G| = 2^x 3^y 5^z$ for some integers x, y, z.

We claim that G has no elements of order 5. Indeed, suppose $g \in G$ and $o(g) = 5$. Then the minimal polynomial of g over K, which we shall denote by μ_g, divides $X^5 - 1$ and has degree at most 2. Moreover μ_g cannot be of degree 1, because then g would be a scalar matrix and a scalar matrix in $M_2(K)$ cannot have order 5. Clearly $X^5 - 1$ factorizes completely over the field $\mathbb{Q}(\zeta_5)$, where ζ_5 is a 5th root of unity. Indeed in $\mathbb{Q}(\zeta_5)$,

$$X^5 - 1 = (X - 1)\left(X - \zeta_5\right)\left(X - \zeta_5^2\right)\left(X - \zeta_5^3\right)\left(X - \zeta_5^4\right).$$

Consequently μ_g is a product of two out of these five terms and we have two possibilities:

1. The constant term of μ_g is of the form ζ_5^i for some $1 \le i \le 4$. Thus $\zeta_5^i \in K$ and hence also $\zeta_5 \in K$. This implies that $[K : \mathbb{Q}] \ge 4$, which contradicts the assumption that $[K : \mathbb{Q}] = 2$.

2. The constant term of μ_g is equal to one, and the coefficient of X is equal to $-(\zeta_5 + \zeta_5^4) \in \mathbb{R} - \mathbb{Q}$ or $-(\zeta_5^2 + \zeta_5^3) \in \mathbb{R} - \mathbb{Q}$, which would imply that K contains the totally real field $\mathbb{Q}[\zeta_5 + \zeta_5^{-1}] = \mathbb{Q}[\sqrt{5}]$, which is impossible since by assumption K is a quadratic imaginary extension of $\mathbb{Q}$.

Hence $|G| = 2^x 3^y$ for some integers x, y. By Burnside's $p^a q^b$-theorem, this implies that G is solvable. This proves our claim on the solvability and possible orders of finite subgroups of $\mathcal{U}(M_2(K))$.

Assume that $g \in G$ has order p^n with either $p = 2$ and $n > 3$ or $p = 3$ and $n > 1$. In this case the minimal polynomial of g over $\mathbb{Q}$ is divisible by $\frac{X^{p^n}-1}{X^{p^{n-1}}-1}$, which has degree bigger than 4, a contradiction.

Now let us consider the case where G has an element g of order 8. Denote by $\mu_{\mathbb{Q},g}$ and $\mu_{K,g}$ the minimal polynomials of g over $\mathbb{Q}$ and K respectively. Their degrees are 4 and 2, respectively. The field $\mathbb{Q}(\zeta_8) \cong \frac{\mathbb{Q}[X]}{(\mu_{\mathbb{Q},g})}$ is an extension of $\mathbb{Q}$ of degree 4 and the field $K(\zeta_8) \cong \frac{K[X]}{(\mu_{K,g})}$ is an extension of K of degree 2. However, since $K/\mathbb{Q}$ is also a

field extension of degree 2 and $\mathbb{Q}(\zeta_8) \subseteq K(\zeta_8)$, we have that $\mathbb{Q}(\zeta_8) = K(\zeta_8)$ and hence $K \subseteq \mathbb{Q}(\zeta_8)$. Using Galois' fundamental theorem we conclude that K is either $\mathbb{Q}(\sqrt{-1})$, $\mathbb{Q}(\zeta_8 + \zeta_8^{-1})$ or $\mathbb{Q}(\sqrt{-2})$. Since K is assumed to be totally imaginary, we can exclude $\mathbb{Q}(\zeta_8 + \zeta_8^{-1})$.

Assume from now on that G has no element of order 8. Then the exponent of G divides 12 and hence $K \subseteq \mathbb{Q}(\zeta_{12})$ ($\mathbb{Q}(\zeta_{12})$ is even a splitting field of G). Again using Galois' theorem we deduce that K is either $\mathbb{Q}(\sqrt{-1})$, $\mathbb{Q}(\sqrt{-3})$ or $\mathbb{Q}(\sqrt{3})$. We can exclude $\mathbb{Q}(\sqrt{3})$ since this is a real field extension of $\mathbb{Q}$. This finishes the proof. $\qquad\square$

Remark 3.2. Note that not only finite subgroups of $\mathcal{U}(M_2(K))$ for quadratic imaginary field extensions K but also finite subgroups of $\mathcal{U}(M_2(\mathbb{Q}))$ are solvable. This is clear since the only possible prime power orders for elements of finite order in $\mathcal{U}(M_2(\mathbb{Q}))$ are 1, 2, 3 and 4 (again by looking at the degrees of the corresponding cyclotomic polynomials, and noting that the degree of the minimal polynomial of an element is bounded by two).

The following proposition turns the classification of all finite subgroups of $\mathcal{U}(M_2(K))$ for $K \in \left\{ \mathbb{Q}, \mathbb{Q}(\sqrt{-1}), \mathbb{Q}(\sqrt{-2}), \mathbb{Q}(\sqrt{-3}) \right\}$ into a finite problem.

Proposition 3.3. *Let* $K \in \left\{ \mathbb{Q}, \mathbb{Q}(\sqrt{-1}), \mathbb{Q}(\sqrt{-2}), \mathbb{Q}(\sqrt{-3}) \right\}$, *and let* $G \le \mathcal{U}(M_2(K))$ *be a finite group. Then* G *can be embedded in the finite group* $\mathrm{GL}(2, 25)$.

Proof. The finite field $\mathbb{F}_{25}$ contains roots of -1, -2 and -3. By Hensel's lemma it follows that the given fields K can all be embedded in $\mathbb{Q}_{5^2}$, the unramified extension of $\mathbb{Q}_5$ of degree 2. Let $\mathbb{Z}_{5^2}$ be the integral closure of $\mathbb{Z}_5$ in $\mathbb{Q}_{5^2}$, and let π denote a generator of the maximal ideal of $\mathbb{Z}_{5^2}$ (so, in particular, $\mathbb{Z}_{5^2}/\pi\mathbb{Z}_{5^2} \cong \mathbb{F}_{25}$). The algebra $M_2(\mathbb{Q}_{5^2})$ contains the maximal order $M_2(\mathbb{Z}_{5^2})$, which is unique up to conjugation. Therefore we can assume without loss that $G \le \mathcal{U}(M_2(\mathbb{Z}_{5^2}))$. There is some n such that $G \cap (1 + 5^n \cdot M_2(\mathbb{Z}_{5^2})) = \{1\}$, and therefore we can again assume without loss that $G \le \mathcal{U}(M_2(\mathbb{Z}_{5^2}/5^n \cdot \mathbb{Z}_{5^2}))$. Consider the short exact sequence

$$1 \longrightarrow (1 + \pi \cdot M_2(\mathbb{Z}_{5^2}))/(1 + 5^n \cdot M_2(\mathbb{Z}_{5^2})) \longrightarrow \mathcal{U}(M_2(\mathbb{Z}_{5^2}/5^n\mathbb{Z}_{5^2})) \longrightarrow \mathrm{GL}(2, 25) \longrightarrow 1. \quad (1)$$

The leftmost term in this sequence is a 5-group, and we know by Theorem 3.1 that 2 and 3 are the only possible prime divisors of the order of G. Therefore G intersects trivially with the kernel of the epimorphism to $\mathrm{GL}(2, 25)$, which proves our claim. $\qquad\square$

We will use the following proposition in the proof of Theorem 3.5 below.

Proposition 3.4. *Let* D *be a quaternion algebra with center* $\mathbb{Q}$ *and* $M \subset D$ *a maximal* $\mathbb{Z}$-*order. If* D *is ramified at the prime* p, *then* $\mathbb{Z}_p \otimes M/\mathrm{Jac}(\mathbb{Z}_p \otimes M) \cong \mathbb{F}_{p^2}$.

Proof. This is an immediate consequence of [14, Theorem 14.3]. $\qquad\square$

Theorem 3.5. *Let* G *be a finite group. If* $\mathbb{Q}G$ *has a simple component which is a* 2×2-*matrix ring over a totally definite quaternion algebra with center* $\mathbb{Q}$, *then this component is a* 2×2-*matrix ring over one of the following algebras:*

7

1. $\left(\frac{-1,-1}{\mathbb{Q}}\right)$,

2. $\left(\frac{-1,-3}{\mathbb{Q}}\right)$ *or*

3. $\left(\frac{-2,-5}{\mathbb{Q}}\right)$.

Proof. Let $D = \left(\frac{a,b}{\mathbb{Q}}\right)$ be a totally definite quaternion algebra over $\mathbb{Q}$. Assume that there is a finite group G and a primitive central idempotent e of $\mathbb{Q}G$ such that the simple component $\mathbb{Q}Ge$ is isomorphic to $M_2(D)$. We can assume without loss of generality that the $\mathbb{Q}$-representation of G determined by e is faithful and hence G can be embedded into $M_2(D)$. We will identify G with its image in $M_2(D)$.

Since the reduced characteristic polynomial of a matrix in $M_2(D)$ always has degree 4 over $\mathbb{Q}$, we conclude that the minimal polynomial of any element in G over $\mathbb{Q}$ has degree at most 4. Moreover, when p is prime we know that the cyclotomic polynomial $\frac{X^p-1}{X-1}$ is irreducible over $\mathbb{Q}$ and it divides the minimal polynomial of $g \in G$ over $\mathbb{Q}$ whenever g has order p. Therefore we deduce that 2, 3 and 5 are the only primes that can occur as orders of elements of G. Hence $|G| = 2^x 3^y 5^z$ for some integers x, y, z.

We claim that if D is ramified at a prime p then p divides the order of G. Suppose by way of contradiction that p is a prime such that D ramifies at p but p does not divide the order of G. Let (E, R, F) denote a splitting p-modular system for G. Then by [14, Theorem (41.1)] the R-order RG is maximal. Hence RGe is a maximal order in $EGe \cong M_4(E)$, which implies $RGe \cong M_4(R)$. Let M be a maximal order in $\mathbb{Q}Ge$ containing $\mathbb{Z}Ge$. Then $M_4(R) \cong RGe \cong R \otimes \mathbb{Z}Ge \cong R \otimes M$, the last isomorphism being due to the fact that $R \otimes M$ would by construction be an R-order containing $R \otimes \mathbb{Z}Ge$, which is already known to be maximal. Since D is ramified at p the $\mathbb{Q}_p$-algebra $\mathbb{Q}_p \otimes \mathbb{Q}Ge$ is not split. This implies in particular that $\mathbb{Z}_p \otimes M$ does not contain a system of more than two non-trivial orthogonal idempotents and hence neither does $\mathbb{F}_p \otimes M$ since idempotents of $\mathbb{F}_p \otimes M$ can be lifted to $\mathbb{Z}_p \otimes M$ (see [22, Theorem 6.7]). It follows that if $\mathbb{F}_p \otimes M$ is semisimple, then it must be isomorphic to either $\mathbb{F}_{p^{16}}$, $\mathbb{F}_{p^8} \oplus \mathbb{F}_{p^8}$ or $M_2(\mathbb{F}_{p^4})$, since all other semisimple $\mathbb{F}_p$-algebras of dimension 16 have a larger system of orthogonal primitive idempotents. If $\mathbb{F}_p \otimes M$ is not semisimple, then its Jacobson radical is non-zero. This would imply that the Jacobson radical of $F \otimes M$ is non-zero as well. In any case it follows that $F \otimes M$ is not isomorphic to $M_4(F)$ and hence $R \otimes M$ is not isomorphic to $M_4(R)$, a contradiction.

Hence the only finite primes p where D can be ramified are $p = 2, 3, 5$. Theorem 2.2 now implies that the only possible sets of ramified places for D are $\{\infty, 2\}$, $\{\infty, 3\}$, $\{\infty, 5\}$ and $\{\infty, 2, 3, 5\}$. The following quaternion algebras have these respective sets as their set of ramified places: $\left(\frac{-1,-1}{\mathbb{Q}}\right)$ (places ∞, 2), $\left(\frac{-1,-3}{\mathbb{Q}}\right)$ (places ∞, 3), $\left(\frac{-2,-5}{\mathbb{Q}}\right)$ (places ∞, 5) and $\left(\frac{-3,-10}{\mathbb{Q}}\right)$ (places ∞, 2, 3, 5). By the uniqueness asserted in Theorem 2.2, it follows that D is isomorphic to one of these four quaternion algebras. It remains to prove that the case $D \cong \left(\frac{-3,-10}{\mathbb{Q}}\right)$ cannot occur.

Assume by way of contradiction that $D \cong \left(\frac{-3,-10}{\mathbb{Q}}\right)$. The algebra D is ramified at the primes 3 and 5 and hence G contains an element of order 3 and an element of order 5. We will use this to show that G must be non-solvable. To see this we first bound the 3-part and

8

the 5-part of the order of G. Note that G embeds into $\mathcal{U}(M_p/p^i M_p)$ for any prime p and sufficiently large i, where M is a maximal order in $\mathbb{Q}Ge$ containing $\mathbb{Z}Ge$ and $M_p := \mathbb{Z}_p \otimes M$ denotes the completion of M at the prime p. The finite group $\mathcal{U}(M_p/p^i M_p)$ is an extension of $\mathcal{U}(M_p/\mathrm{Jac}(M_p))$ by the p-group $1 + \mathrm{Jac}(M_p)/1 + p^i M_p$. As a consequence, every p'-subgroup of G can be embedded in $\mathcal{U}(M_p/\mathrm{Jac}(M_p))$. In particular, a Sylow 3-subgroup of G can be embedded in $\mathcal{U}(M_5/\mathrm{Jac}(M_5)) \cong \mathrm{GL}(2,25)$ (by Proposition 3.4) and a Sylow 5-subgroup of G can be embedded in $\mathcal{U}(M_3/\mathrm{Jac}(M_3)) \cong \mathrm{GL}(2,9)$. It follows that the Sylow 5-subgroup of G has order at most 5, and the Sylow 3-subgroup of G has order at most 9. But all groups of order $3 \cdot 5$ and $3^2 \cdot 5$ are abelian, and hence a Hall $\{3,5\}$-subgroup of G (if it exists) must be abelian. In particular, a Hall $\{3,5\}$-subgroup of G would contain an element of order 15. If G is solvable, then, by Hall's Theorem, all possible Hall-subgroups exist, which implies that G contains an element of order 15. But an element of order 15 in $\mathcal{U}(M_2(D))$ would have minimal polynomial over $\mathbb{Q}$ divisible by the irreducible cyclotomic polynomial $\frac{X^{15}-1}{(X^5-1)(1+X+X^2)}$. This is impossible, since an element of $M_2(D)$ has minimal polynomial of degree at most 4. We conclude that G is non-solvable.

Now we will place restrictions on the structure of the Sylow 2-subgroups of G. Let S_2 denote such a Sylow 2-subgroup. Clearly, the $\mathbb{Q}$-span of S_2 in $M_2(D)$, which we shall denote by A, is a semisimple $\mathbb{Q}$-subalgebra of $M_2(D)$. As we have already shown that any finite group spanning $M_2(D)$ must be non-solvable, it is also clear that A is properly contained in $M_2(D)$. Hence $\dim_{\mathbb{Q}}(A) < 16$. We get the following cases:

1. A is not simple: In this case $A = D_1 \oplus D_2$, and both D_1 and D_2 can be embedded in D. Note that each D_i is spanned by units of 2-power order, and the elements 1 and -1 are the only elements of 2-power order in D (since $\mathbb{Q}_5 \supset \mathbb{Q}(\sqrt{-1})$ does not split D). It follows that $D_1 = D_2 = \mathbb{Q}$, and therefore $S_2 \cong V_4$.

2. A is simple and neither a skew-field nor a field: We get $A = M_2(K)$, where K is a field contained in D. This means that either $K = \mathbb{Q}$ or K is a quadratic imaginary extension of $\mathbb{Q}$. In the latter case Theorem 3.1 tells us that $K = \mathbb{Q}(\sqrt{-d})$ for $d \in \{1,2,3\}$. Since A occurs as a simple component of $\mathbb{Q}S_2$, $Z(A) = K$ occurs as a simple component of $Z(\mathbb{Q}S_2)$, and we know that those are contained in $\mathbb{Q}(\zeta_{\exp(S_2)})$. But $\mathbb{Q}(\sqrt{-3}) = \mathbb{Q}(\zeta_3)$ cannot be embedded in $\mathbb{Q}(\zeta_{2^i})$ for any i, so $d = 3$ is impossible. Moreover, $\mathbb{Q}(\sqrt{-1}) \subset \mathbb{Q}_5$ and $\mathbb{Q}(\sqrt{-2}) \subset \mathbb{Q}_3$. If K were either one of those, then it would be a maximal subfield of D and therefore a splitting field. This would imply that either $\mathbb{Q}_3$ or $\mathbb{Q}_5$ is also a splitting field for D, but we know that this is not the case. The only possibility is hence $K = \mathbb{Q}$, and in this case $S_2 \leq \mathrm{GL}_2(\mathbb{R})$. Using some basic linear algebra (see for example [23]), one can see that finite subgroups of $\mathrm{GL}_2(\mathbb{R})$ can only be cyclic or dihedral. Hence, by Remark 3.2, we get that $S_2 \cong D_8$.

3. A is a skew-field or a field: In this case S_2 has a faithful fixed point free representation and is therefore a Frobenius complement. By [15, Theorem 18.1], the Sylow 2-subgroups of Frobenius complements are cyclic groups or generalized quaternion groups. So $S_2 \cong Q_{2^i}$ for some $i \geq 3$ or $S_2 \cong C_{2^i}$ for some $i \geq 0$. Among those possibilities the quaternion groups Q_8 and Q_{16} and the cyclic groups of order 1, 2,

4, 8 and 16 are the only ones whose group ring over $\mathbb{Q}$ has a faithful Wedderburn component of dimension strictly smaller than 16.

In particular we can conclude that the order of S_2 is at most 16.

For sufficiently large i we can embed G in $\mathcal{U}(M/2^i M)$, and we have a short exact sequence

$$1 \longrightarrow 1 + \mathrm{Jac}(M_2/2^i M_2) \longrightarrow \mathcal{U}(M_2/2^i M_2) \longrightarrow \mathcal{U}(M_2/\mathrm{Jac}(M_2)) \cong \mathrm{GL}(2,4) \longrightarrow 1 \quad (2)$$

where we again use the notation $M_2 := \mathbb{Z}_2 \otimes M$. Since the leftmost group in this sequence is a 2-group, and G is non-solvable, the rightmost arrow must map the image of G in $\mathcal{U}(M_2/2^i M_2)$ to a non-solvable subgroup of $\mathrm{GL}(2,4)$, which we shall denote by $\bar{G}$. We know that $\mathrm{SL}(2,4) \cong \mathrm{PSL}(2,4) \cong A_5$ is a normal simple subgroup of $\mathrm{GL}(2,4)$ of index 3. The group $\bar{G} \cap \mathrm{SL}(2,4)$ is a normal subgroup of $\bar{G}$, and $\bar{G}/\bar{G} \cap \mathrm{SL}(2,4) \hookrightarrow \mathrm{GL}(2,4)/\mathrm{SL}(2,4) \cong C_3$. If $\bar{G} \cap \mathrm{SL}(2,4)$ were properly contained in $\mathrm{SL}(2,4)$, then it would have to be solvable (as any group of order < 60 is solvable). Then $\bar{G}$ would be solvable, which is impossible. It follows that $\mathrm{SL}(2,4) \subseteq \bar{G}$. Since $\mathrm{SL}(2,4)$ is a maximal subgroup of $\mathrm{GL}(2,4)$ it follows that $\bar{G} \in \{\mathrm{SL}(2,4), \mathrm{GL}(2,4)\}$. We already saw that G may not contain an element of order 15, and hence neither may $\bar{G}$. Thus $\bar{G}$ cannot be equal to $\mathrm{GL}(2,4)$, and we conclude $\bar{G} = \mathrm{SL}(2,4)$.

We have bounded the order of the Sylow 2-subgroup of G by 16, and therefore we get a short exact sequence

$$1 \longrightarrow X \longrightarrow G \longrightarrow \mathrm{SL}(2,4) \longrightarrow 1 \quad (3)$$

where X is a 2-group of size ≤ 4. The automorphism groups of 2-groups of those sizes are solvable, and therefore $\mathrm{SL}(2,4)$ has no non-trivial homomorphisms into those automorphism groups. Hence (3) is a central extension. We know that the center of G is contained in $Z(M_2(D)) \cong \mathbb{Q}$, which implies that X can have order at most 2. Hence G corresponds with an element in $H^2(\mathrm{SL}(2,4), C_2)$. It is well known that this cohomology group is of order 2 and thus G is isomorphic with either $C_2 \times \mathrm{SL}(2,4)$ (corresponding to the trivial element in the cohomology group) or with $\mathrm{SL}(2,5)$. If $G \cong C_2 \times \mathrm{SL}(2,4)$, then $M_2(D)$ is a simple component of $\mathbb{Q}\mathrm{SL}(2,4)$. Hence we just have to check whether either $\mathbb{Q}\mathrm{SL}(2,4)$ or $\mathbb{Q}\mathrm{SL}(2,5)$ has $M_2(D)$ as a simple component. But the Wedderburn decompositions of $\mathbb{Q}\mathrm{SL}(2,4)$ and $\mathbb{Q}\mathrm{SL}(2,5)$ are known (alternatively, can be computed using GAP), and indeed neither $\mathbb{Q}\mathrm{SL}(2,4)$ nor $\mathbb{Q}\mathrm{SL}(2,5)$ has $M_2(D)$ as a simple component, which means that we have reached a contradiction. □

Theorems 3.1 and 3.5 and some computations done in [9, Chapter 6.4] and [10] yield the existence of norm Euclidean orders in the corresponding 2×2-matrix ring components of rational group algebras. It is easy to verify that this norm Euclidean order has to be a (and hence the unique) maximal order $\mathcal{O}$. For quaternion algebras, it can even be shown that the listed algebras are the only possible positive definite quaternion algebras over $\mathbb{Q}$ having this property [10, Theorem 2.1].

Corollary 3.6. *Let G be a finite group with the property that $\mathbb{Q}G$ has a simple component $M_2(D)$ of one of the following types:*

1. a 2×2-matrix ring over $\mathbb{Q}$;

2. a 2×2-matrix ring over an imaginary quadratic extension of $\mathbb{Q}$;

3. a 2×2-matrix ring over a totally definite quaternion algebra with center $\mathbb{Q}$.

Then a maximal order of D is norm Euclidean and therefore unique. The corresponding maximal orders are listed in Table 1 below.

Table 1: Maximal orders

Division ring	Maximal order
$\mathbb{Q}$	$\mathbb{Z}$
$\mathbb{Q}(\sqrt{-1})$	$\mathbb{Z}[\sqrt{-1}]$
$\mathbb{Q}(\sqrt{-2})$	$\mathbb{Z}[\sqrt{-2}]$
$\mathbb{Q}(\sqrt{-3})$	$\mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right]$
$\left(\frac{-1,-1}{\mathbb{Q}}\right)$	$\mathbb{Z}[1, i, j, \frac{1}{2}(1 + i + j + ij)]$
$\left(\frac{-1,-3}{\mathbb{Q}}\right)$	$\mathbb{Z}[1, i, \frac{1}{2}(1 + j), \frac{1}{2}(i + ij)]$
$\left(\frac{-2,-5}{\mathbb{Q}}\right)$	$\mathbb{Z}[1, \frac{1}{4}(2 + i - ij), \frac{1}{4}(2 + 3i + ij), \frac{1}{2}(1 + i + j)]$

Theorem 3.7. *Let G be a finite group with the property that $\mathbb{Q}G$ has a faithful simple component of one of the following types:*

1. a 2×2-matrix ring over $\mathbb{Q}$;

2. a 2×2-matrix ring over an imaginary quadratic extension of $\mathbb{Q}$;

3. a 2×2-matrix ring over a totally definite quaternion algebra with center $\mathbb{Q}$.

Then G is isomorphic to one of the 55 groups listed in Table 2 below.

Proof. The maximal finite subgroups of 2×2-matrices over totally definite quaternion algebras with center $\mathbb{Q}$ were classified in [7] by means of investigating invariant rational lattices. Among those groups, the ones acting primitively are listed in a database which forms part of the computer algebra system MAGMA. The two groups acting imprimitively are explicitly given. By Proposition 3.3, all finite subgroups of $M_2(\mathbb{Q})$ and $M_2(\mathbb{Q}(\sqrt{-d}))$ for $d \in \{1, 2, 3\}$ can be embedded in the finite group $\mathrm{GL}(2, 25)$. The rest is a computation, which was performed using GAP. $\square$

Note that the problem of determining all groups in Theorem 3.7 was even a priori (i.e. without using [7]) clearly a finite problem: If $G \leq M_2(D)$ with D a totally definite quaternion algebra over $\mathbb{Q}$, then it can be shown with techniques as in the proof op Proposition 3.3 that $G \leq \mathcal{U}(M_2(\mathcal{O}/7\mathcal{O}))$, where $\mathcal{O}$ is the maximal order of D.

Remark 3.8 (Notation in Table 2). We use the abbreviations

$$\mathbb{H}_1 = \left(\frac{-1,-1}{\mathbb{Q}}\right) \quad \mathbb{H}_3 = \left(\frac{-1,-3}{\mathbb{Q}}\right) \quad \mathbb{H}_5 = \left(\frac{-2,-5}{\mathbb{Q}}\right) \tag{4}$$

We use the standard short GAP notation for the group structure. In this description, cyclic groups are denoted by their order, e. g. "3" denotes the cyclic group C_3, and "3^2" denotes the elementary abelian group $C_3 \times C_3$. Direct products are denoted by $A \times B$ and semidirect products by $A : B$. For non-split extension of A by B, we write $A.B$.

Table 2: Groups with faithful exceptional components

SMALLGROUP ID	Structure	Faithful exceptional components
[6, 1]	S_3	$1 \times M_2(\mathbb{Q})$
[8, 3]	D_8	$1 \times M_2(\mathbb{Q})$
[12, 4]	D_{12}	$1 \times M_2(\mathbb{Q})$
[16, 6]	$8 : 2$	$1 \times M_2(\mathbb{Q}(\sqrt{-1}))$
[16, 8]	QD_{16} (also denoted by D_{16}^-)	$1 \times M_2(\mathbb{Q}(\sqrt{-2}))$
[16, 13]	$(4 \times 2) : 2$	$1 \times M_2(\mathbb{Q}(\sqrt{-1}))$
[18, 3]	$3 \times S_3$	$1 \times M_2(\mathbb{Q}(\sqrt{-3}))$
[24, 3]	$SL(2,3)$	$1 \times M_2(\mathbb{Q}(\sqrt{-3}))$
[24, 5]	$4 \times S_3$	$1 \times M_2(\mathbb{Q}(\sqrt{-1}))$
[24, 8]	$(6 \times 2) : 2$	$1 \times M_2(\mathbb{Q}(\sqrt{-3}))$
[24, 10]	$3 \times D_8$	$1 \times M_2(\mathbb{Q}(\sqrt{-3}))$
[24, 11]	$3 \times Q_8$	$1 \times M_2(\mathbb{Q}(\sqrt{-3}))$
[32, 8]	$2.((4 \times 2) : 2) = (2^2).(4 \times 2)$	$1 \times M_2(\mathbb{H}_1)$
[32, 11]	$(4 \times 4) : 2$	$2 \times M_2(\mathbb{Q}(\sqrt{-1}))$
[32, 44]	$(2 \times Q_8) : 2$	$1 \times M_2(\mathbb{H}_1)$
[32, 50]	$(2 \times Q_8) : 2$	$1 \times M_2(\mathbb{H}_1)$
[36, 6]	$3 \times (3 : 4)$	$1 \times M_2(\mathbb{Q}(\sqrt{-3}))$
[36, 12]	$6 \times S_3$	$1 \times M_2(\mathbb{Q}(\sqrt{-3}))$
[40, 3]	$5 : 8$	$1 \times M_2(\mathbb{H}_5)$
[48, 16]	$(3 : 8) : 2$	$1 \times M_2(\mathbb{H}_1)$
[48, 18]	$3 : Q_{16}$	$1 \times M_2(\mathbb{H}_3)$
[48, 28]	$2.S_4 = SL(2,3).2$	$1 \times M_2(\mathbb{H}_3)$
[48, 29]	$GL(2,3)$	$1 \times M_2(\mathbb{Q}(\sqrt{-2}))$
[48, 33]	$SL(2,3) : 2$	$1 \times M_2(\mathbb{Q}(\sqrt{-1}))$
[48, 39]	$(2 \times (3 : 4)) : 2$	$1 \times M_2(\mathbb{H}_3)$
[48, 40]	$Q_8 \times S_3$	$1 \times M_2(\mathbb{H}_1)$
[64, 37]	$2.(((4 \times 2) : 2) : 2) = (4 \times 2).(4 \times 2)$	$2 \times M_2(\mathbb{H}_1)$
[64, 137]	$((4 \times 4) : 2) : 2$	$2 \times M_2(\mathbb{H}_1)$
[72, 19]	$(3^2) : 8$	$2 \times M_2(\mathbb{H}_3)$
[72, 20]	$(3 : 4) \times S_3$	$1 \times M_2(\mathbb{H}_3)$

<div align="center">continued</div>

SmallGroup ID	Structure	Faithful exceptional components
[72, 22]	$(6 \times S_3) : 2$	$1 \times M_2(\mathbb{H}_3)$
[72, 24]	$(3^2) : Q_8$	$1 \times M_2(\mathbb{H}_3)$
[72, 25]	$3 \times \mathrm{SL}(2,3)$	$3 \times M_2(\mathbb{Q}(\sqrt{-3}))$
[72, 30]	$3 \times ((6 \times 2) : 2)$	$2 \times M_2(\mathbb{Q}(\sqrt{-3}))$
[96, 67]	$\mathrm{SL}(2,3) : 4$	$2 \times M_2(\mathbb{Q}(\sqrt{-1}))$
[96, 190]	$(2 \times \mathrm{SL}(2,3)) : 2$	$1 \times M_2(\mathbb{H}_1)$
[96, 191]	$(2.S_4 = \mathrm{SL}(2,3).2) : 2$	$1 \times M_2(\mathbb{H}_1)$
[96, 202]	$(2 \times \mathrm{SL}(2,3)) : 2$	$1 \times M_2(\mathbb{H}_1)$
[120, 5]	$\mathrm{SL}(2,5)$	$1 \times M_2(\mathbb{H}_3)$
[128, 937]	$(Q_8 \times Q_8) : 2$	$4 \times M_2(\mathbb{H}_1)$
[144, 124]	$3 : (2.S_4 = \mathrm{SL}(2,3).2)$	$3 \times M_2(\mathbb{H}_3)$
[144, 128]	$S_3 \times \mathrm{SL}(2,3)$	$1 \times M_2(\mathbb{H}_1)$
[144, 135]	$((3^2) : 8) : 2$	$4 \times M_2(\mathbb{H}_3)$
[144, 148]	$(2 \times ((3^2) : 4)) : 2$	$2 \times M_2(\mathbb{H}_3)$
[160, 199]	$((2 \times Q_8) : 2) : 5$	$1 \times M_2(\mathbb{H}_1)$
[192, 989]	$((2.S_4 = \mathrm{SL}(2,3).2) : 2) : 2$	$2 \times M_2(\mathbb{H}_1)$
[240, 89]	$2.S_5 = \mathrm{SL}(2,5).2$	$1 \times M_2(\mathbb{H}_5)$
[240, 90]	$\mathrm{SL}(2,5) : 2$	$1 \times M_2(\mathbb{H}_5)$
[288, 389]	$((3 : 4) \times (3 : 4)) : 2$	$2 \times M_2(\mathbb{H}_3)$
[320, 1581]	$2.(((2^4) : 5) : 2) = (((2 \times Q_8) : 2) : 5).2$	$2 \times M_2(\mathbb{H}_1)$
[384, 618]	$((Q_8 \times Q_8) : 3) : 2$	$1 \times M_2(\mathbb{H}_1)$
[384, 18130]	$((Q_8 \times Q_8) : 3) : 2$	$1 \times M_2(\mathbb{H}_1)$
[720, 409]	$\mathrm{SL}(2,9)$	$2 \times M_2(\mathbb{H}_3)$
[1152, 155468]	$(\mathrm{SL}(2,3) \times \mathrm{SL}(2,3)) : 2$	$1 \times M_2(\mathbb{H}_1)$
[1920, 241003]	$2.(2^4 : A_5)$	$1 \times M_2(\mathbb{H}_1)$

4. An effective method to compute $\mathcal{U}(\mathbb{Z}G)$ up to commensurability

The proof of the following proposition is based on the Euclidean algorithm and is well known.

Proposition 4.1. *Let $\mathcal{O}$ be a norm Euclidean order in either $\mathbb{Q}$, a totally definite quaternion algebra over $\mathbb{Q}$ or a quadratic imaginary extension of $\mathbb{Q}$. Let B be a $\mathbb{Z}$-basis of $\mathcal{O}$. Let*

$$X = \left\{ \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ x & 1 \end{pmatrix} : x \in B \right\}.$$

Then X generates a subgroup of finite index in $\mathrm{SL}_2(\mathcal{O})$.

Due to the restrictions we obtained on the possible exceptional components, together with Proposition 4.1, we can generalize Proposition 2.10. That is, we can allow exceptional components of type 2. Recall that $\mathcal{B}_1$ denotes the group generated by the Bass units of $\mathbb{Z}G$ and $\mathcal{B}_2$ the group generated by the bicyclic units of $\mathbb{Z}G$.

Method 4.2. *Let G be a finite group and let $\mathbb{Q}G = \bigoplus_{i=1}^n \mathbb{Q}Ge_i = \bigoplus_{i=1}^n M_{n_i}(D_i)$ be the Wedderburn decomposition of $\mathbb{Q}G$. Assume that $\mathbb{Q}G$ has no simple component which is a non-commutative division ring other than a totally definite quaternion algebra. Assume furthermore that for each $i \in \{1, ..., n\}$ with $n_i > 2$ or $n_i = 2$ and D_i different from $\mathbb{Q}$, a quadratic imaginary extension of $\mathbb{Q}$ or a totally definite quaternion algebra over $\mathbb{Q}$, there exists a $g_i \in G \setminus \{1\}$ such that $\widehat{g_i}e_i \notin \{0, e_i\}$.*

For each component $\mathbb{Q}Ge_i \cong M_2(D_i)$, with D_i one of the following rings:

1. *$\mathbb{Q}$;*

2. *$\mathbb{Q}(\sqrt{-1})$, $\mathbb{Q}(\sqrt{-2})$ or $\mathbb{Q}(\sqrt{-3})$;*

3. *$\left(\frac{-1,-1}{\mathbb{Q}}\right)$, $\left(\frac{-1,-3}{\mathbb{Q}}\right)$ or $\left(\frac{-2,-5}{\mathbb{Q}}\right)$,*

compute the isomorphism $\iota_i : M_2(D_i) \xrightarrow{\sim} \mathbb{Q}Ge_i \subset \mathbb{Q}G$. Let $\mathcal{O}_i$ be a maximal order of D_i with $\mathbb{Z}$-basis B_i and set

$$U_i := \left\{ 1 + \iota_i \begin{pmatrix} 0 & x \\ 0 & 0 \end{pmatrix}, 1 + \iota_i \begin{pmatrix} 0 & 0 \\ x & 0 \end{pmatrix} : x \in B_i \right\}.$$

This construction yields a subgroup $U := \langle \mathcal{B}_1 \cup \mathcal{B}_2 \cup \bigcup_i U_i \rangle$ of $\mathbb{Q}G$ which is commensurable with $\mathcal{U}(\mathbb{Z}G)$.

Proof. Let $\mathcal{O}_i \subset D_i$ denote the maximal order in each division ring. It suffices to verify condition 2 of Proposition 2.7 for each simple component of $\mathbb{Q}G$, i.e. $U \cap (1 \times \cdots \times 1 \times \mathrm{SL}_{n_i}(\mathcal{O}_i) \times 1 \times \cdots \times 1)$ is of finite index in $1 \times \cdots \times 1 \times \mathrm{SL}_{n_i}(\mathcal{O}_i) \times 1 \times \cdots \times 1$.

For the components with $n_i = 1$, the result follows trivially since D_i is either commutative or a totally definite quaternion algebra. In both cases $\mathrm{SL}_1(\mathcal{O}_i)$ is finite [21].

For the components $M_2(D)$ with D equal to $\mathbb{Q}$, a quadratic imaginary extension of $\mathbb{Q}$ or a totally definite quaternion algebra over $\mathbb{Q}$, we know by Corollary 3.6 that a maximal order of D is norm Euclidean and unique. The result then follows from Proposition 4.1.

For the remaining components $\mathbb{Q}Ge_i$, there always exists a $g_i \in G$ such that $\widehat{g_i}e_i$ is a non-central idempotent in $\mathbb{Q}Ge_i$. By applying an adapted version of the proof of [5, Corollary 4.1] one can conclude that this implies that U contains a group of the form $1 \times \cdots \times 1 \times E(Q_i) \times 1 \times \cdots \times 1$ for some ideal $Q_i \trianglelefteq \mathcal{O}_i$ (where $E(Q_i)$ is defined as in Theorem 2.8). Now Theorem 2.8 implies that condition 2 holds for all these components, which finishes the proof. $\square$

Remark 4.3. In Method 4.2 we need a construction of non-central idempotents in $\mathbb{Q}Ge_i$ for two purposes:

- for the explicit determination of the isomorphisms $\iota_i : M_2(D_i) \xrightarrow{\sim} \mathbb{Q}Ge_i \subset \mathbb{Q}G$ when $\mathbb{Q}Ge_i$ is in the list $\{M_2(\mathbb{Q}), M_2(\mathbb{Q}(\sqrt{-1}), M_2(\mathbb{Q}(\sqrt{-2})), M_2(\mathbb{Q}(\sqrt{-3})), M_2(\left(\frac{-1,-1}{\mathbb{Q}}\right)), M_2(\left(\frac{-1,-3}{\mathbb{Q}}\right)), M_2(\left(\frac{-2,-5}{\mathbb{Q}}\right))\}$;

- for the use of bicyclic units or generalized bicyclic units (as in Definition 2.6) when $\mathbb{Q}Ge_i$ is non-commutative and not in the list above.

The components where no $\widehat{g}$ gives a non-central idempotent are classified. For each epimorphic image G/N of G which is isomorphic to a Frobenius complement, G has an irreducible representation ρ with kernel N such that $\rho(\widehat{g})$ acts as the identity for all $g \in G \setminus \{1\}$ [15, Theorem 18.1.v]. By [24, Theorem 12.2], we even know that each such epimorphism determines a unique representation with this property and hence a unique simple component of $\mathbb{Q}G$ in which we might lack idempotents.

This means that Method 4.2 applies to all finite groups G that do not have a non-commutative Frobenius complement as a quotient (it follows easy that under this condition $\mathbb{Q}G$ has no non-commutative division ring as a simple component). Although, if G has an epimorphic image onto a Frobenius complement and if one knows other constructions of non-central idempotents, one can just work with those idempotents. One only has to modify Method 4.2 to use the generalized bicyclic units based on those idempotents.

5. Examples

Before we give some examples, we recall some definitions from [25].
If $K \lhd H \leq G$ then let

$$\varepsilon(H, K) = \prod_{M/K \in \mathcal{M}(H/K)} (\widehat{K} - \widehat{M}) = \widehat{K} \prod_{M/K \in \mathcal{M}(H/K)} (1 - \widehat{M}),$$

where $\mathcal{M}(H/K)$ denotes the set of all minimal normal subgroups of H/K. We extend this notation by setting $\varepsilon(H, H) = \widehat{H}$. Clearly $\varepsilon(H, K)$ is an idempotent of the group algebra $\mathbb{Q}G$. Let $e(G, H, K)$ be the sum of the distinct G-conjugates of $\varepsilon(H, K)$, that is, if T is a right transversal of $C_G(\varepsilon(H, K))$ in G, then

$$e(G, H, K) = \sum_{t \in T} \varepsilon(H, K)^t.$$

Clearly, $e(G, H, K)$ lies in the center of $\mathbb{Q}G$ and if the G-conjugates of $\varepsilon(H, K)$ are orthogonal, then $e(G, H, K)$ is a central idempotent of $\mathbb{Q}G$.

5.1. $\mathcal{U}(\mathbb{Z}C_8 \rtimes C_2)$ up to finite index

Let G be the group with presentation $\langle a, b \mid a^8 = 1, b^2 = 1, bab = a^5 \rangle$. This is the group with SMALLGROUP ID [16,6]. The computation of $\mathcal{U}(\mathbb{Z}G)$ is also done in [26] using Poincaré's Polyhedron Theorem. We approach this example with more elementary techniques.

Using Wedderga [27] based on the papers [25, 28], we compute the Wedderburn decomposition

$$\mathbb{Q}G = 4\mathbb{Q} \oplus 2\mathbb{Q}(i) \oplus M_2(\mathbb{Q}(i))$$

and see that the primitive central idempotent e yielding the last simple component is afforded by the pair $(\langle a \rangle, 1)$ and equals $e = e(G, \langle a \rangle, 1) = \frac{1}{2} - \frac{1}{2}a^4$. Hence the simple component can be described as the crossed product $\mathbb{Q}Ge = \mathbb{Q}\langle a \rangle \varepsilon(\langle a \rangle, 1) * \langle b \rangle$. It is easy to see that $\widehat{b}$ is a non-trivial idempotent, which affords a description of $\mathbb{Q}Ge$ as

15

$M_2(\widehat{b}\mathbb{Q}Ge\widehat{b})$. Another simple calculation shows that $(\widehat{b}a^2 e\widehat{b})^2 = -e\widehat{b}$ and hence $\widehat{b}a^2 e\widehat{b}$ is mapped to $\begin{pmatrix} i & 0 \\ 0 & 0 \end{pmatrix}$ by an isomorphism between $\mathbb{Q}Ge$ and $M_2(\mathbb{Q}(i))$.

We will determine an explicit isomorphism

$$\iota : M_2(\mathbb{Q}(i)) \xrightarrow{\sim} \mathbb{Q}Ge \subset \mathbb{Q}G.$$

It suffices to find images of the following elements:

$$E := \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \ I := \begin{pmatrix} i & 0 \\ 0 & 0 \end{pmatrix}, \ A := \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \ B := \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}.$$

We already know possible images for E and I:

$$\iota(E) = e\widehat{b} \in \frac{1}{4}\mathbb{Z}G, \ \iota(I) = \widehat{b}a^2 e\widehat{b} \in \frac{1}{4}\mathbb{Z}G.$$

Hence it suffices to find images for A and B. These must merely satisfy

$$\iota(A) \cdot \iota(B) = \iota(E), \tag{5}$$

$$\iota(E) \cdot \iota(A) \cdot (1 - \iota(E)) = \iota(A) \tag{6}$$

and

$$(1 - \iota(E)) \cdot \iota(B) \cdot \iota(E) = \iota(B). \tag{7}$$

Define

$$\iota(A) = \widehat{b}ae(e - \widehat{b}) = \widehat{b}ae(1 - \widehat{b}) \in \frac{1}{4}\mathbb{Z}G \quad \text{and} \quad \iota(B) = \alpha(1 - \widehat{b})a^{-1}e\widehat{b} \in \alpha\frac{1}{4}\mathbb{Z}G,$$

where $\alpha \in \mathbb{Q}$ is an element yet to be determined. Equations (6) and (7) are satisfied by definition. Consider the standard involution

$$-^\circ : \mathbb{Q}G \longrightarrow \mathbb{Q}G : \sum_{g \in G} a_g g \mapsto \sum_{g \in G} a_g g^{-1}.$$

Clearly $\iota(B)^\circ = \alpha\iota(A)$. Hence $(\iota(A)\iota(B))^\circ = \iota(A)\iota(B)$. Note that $\iota(E)^\circ = \iota(E)$ and $\iota(I)^\circ = -\iota(I)$. It follows that $-^\circ$ induces the standard involution on the quaternion algebra $\iota(E)\mathbb{Q}G\iota(E)$. So the invariance of $\iota(A)\iota(B)$ implies that $\iota(A)\iota(B) = q\iota(E)$ for some $q \in \mathbb{Q}$. We want q to be equal to 1 and compute

$$\iota(A)\iota(B) = \alpha e\widehat{b}.$$

Hence

$$\alpha = 1.$$

Now we apply our results to compute $\mathcal{U}(\mathbb{Z}G)$ up to finite index. Since all components but one yield a finite group of units, it suffices to compute the group of units of $1 - e + \mathbb{Z}Ge$ up to finite index.

16

Let $\mathbb{Z}[i]$ be the maximal order of $\mathbb{Q}(i)$, then $\mathbb{Z}Ge$ and $\mathrm{SL}_2(\mathbb{Z}[i])$ are commensurable. From Method 4.2, we conclude that

$$1 + \iota \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, 1 + \iota \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, 1 + \iota \begin{pmatrix} 0 & i \\ 0 & 0 \end{pmatrix}, 1 + \iota \begin{pmatrix} 0 & 0 \\ i & 0 \end{pmatrix}$$

generates $\mathcal{U}(1 - e + \mathbb{Z}Ge)$ up to finite index. Hence this set of elements in $\mathbb{Q}G$ generates a group which is commensurable with $\mathcal{U}(\mathbb{Z}G)$.

However these images do not lie in $\mathbb{Z}G$ but in $\frac{1}{4}\mathbb{Z}G$. If one is not satisfied with commensurability, one has to deduce from the generators of $\mathrm{SL}_2(\mathbb{Z}[i])$ a list of generators of the congruence subgroup

$$C = \begin{pmatrix} 2\mathbb{Z}[i] + 1 & 4\mathbb{Z}[i] \\ 4\mathbb{Z}[i] & 2\mathbb{Z}[i] + 1 \end{pmatrix}_{\det = 1}$$

using techniques as for example Schreier's lemma. In order to use Schreier's lemma, one should go down from $\mathrm{SL}_2(\mathbb{Z}[i])$ to C in the lattice of subgroups in small steps.

Jespers and Leal [29] already deduced generators of

$$\overline{\Gamma} = \begin{pmatrix} 2\mathbb{Z}[i] + 1 & 4\mathbb{Z}[i] \\ 2\mathbb{Z}[i] & 2\mathbb{Z}[i] + 1 \end{pmatrix}_{\det = 1} \Big/ \{\pm \mathrm{id}\}$$

from generators of $\mathrm{PSL}_2(\mathbb{Z}[i])$ using the Reidemeister-Schreier theorem. They obtained the following list of generators:

$$l_1 = \begin{pmatrix} 5 - 2i & 4 + 4i \\ 2 & 1 + 2i \end{pmatrix}, l_2 = \begin{pmatrix} 5 & 4i \\ 4i & -3 \end{pmatrix}, l_3 = \begin{pmatrix} -3 - 6i & -4i \\ -4i & 1 - 2i \end{pmatrix},$$

$$l_4 = \begin{pmatrix} 3 - 2i & 4 \\ 2i & -1 + 2i \end{pmatrix}, l_5 = \begin{pmatrix} 29 + 2 & 44i \\ -8 + 20i & -31 - 10i \end{pmatrix}, l_6 = \begin{pmatrix} 17 - 12i & 20 + 24i \\ 8 & 1 + 12i \end{pmatrix},$$

$$l_7 = \begin{pmatrix} 11 + 38i & -56 + 20i \\ 22i & -33 + 2i \end{pmatrix}, l_8 = \begin{pmatrix} 27 - 2i & -32 + 16i \\ 18i & -9 - 22i \end{pmatrix},$$

$$l_9 = \begin{pmatrix} -7 - 14i & 20 - 12i \\ 10 - 8i & 13 + 14i \end{pmatrix}, r_1 = \begin{pmatrix} 1 & 4 \\ 0 & 1 \end{pmatrix}, r_2 = \begin{pmatrix} 3 & -4i \\ 2i & 3 \end{pmatrix}, r_3 = \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix},$$

$$r_4 = \begin{pmatrix} -7 - 6i & -4 - 8i \\ 4 - 4i & 5 - 2i \end{pmatrix}, r_5 = \begin{pmatrix} 29 + 44i & -64 + 48i \\ -30 + 16i & -27 - 44i \end{pmatrix},$$

$$r_6 = \begin{pmatrix} -5 - 8i & 12 - 8i \\ -2i & 3 \end{pmatrix}, r_7 = \begin{pmatrix} 13 + 6i & -8 + 20i \\ 12 & 1 + 18i \end{pmatrix},$$

$$r_8 = \begin{pmatrix} -7 - 18i & 16 + 16i \\ 12 - 4i & -11 + 10i \end{pmatrix}.$$

Clearly this list is also a list of generators of a subgroup of finite index in

$$\Gamma = \begin{pmatrix} 2\mathbb{Z}[i] + 1 & 4\mathbb{Z}[i] \\ 2\mathbb{Z}[i] & 2\mathbb{Z}[i] + 1 \end{pmatrix}_{\det = 1}.$$

It is easy to see that the congruence subgroup C has index 4 in Γ, and one can check that a right transversal is given by $T = \{I, r_2, r_3, r_2r_3\}$. Applying Schreier's lemma to Γ and C with transversal T and list of generators $X = \{l_1, ..., l_9, r_1, ..., r_8\}$, we get a set of 66 generators of C up to finite index of the form

$$\{tx(\overline{tx})^{-1} \mid t \in T, x \in X\},$$

where $\overline{tx} \in T$ is the representative of the right coset containing the element tx. Thus, up to finite index, $\mathcal{U}(\mathbb{Z}G)$ is generated by at most 66 generators which are of the following form

$$1 - e + \iota\left(tx(\overline{tx})^{-1}\right),$$

for $t \in T$ and $x \in X$.

Remark 5.1. One should note that also the generators of Proposition 4.1 could have been used to compute generators up to finite index of a congruence subgroup in $\mathrm{SL}_2(\mathbb{Z}[i])$.

5.2. $\mathcal{U}(\mathbb{Z}\mathrm{SL}(2,5))$ *up to commensurability*

By a classification of Frobenius complements [15, Theorem 18.6], we know that $\mathrm{SL}(2,5)$ is the smallest non-solvable Frobenius complement. Since this group does not satisfy the properties needed for the Jespers-Leal-result, we will apply our results to investigate the units of $\mathbb{Z}\mathrm{SL}(2,5)$. Using [27], we compute that $\mathbb{Q}\mathrm{SL}(2,5)$ is isomorphic to

$$\mathbb{Q} \oplus M_4(\mathbb{Q}) \oplus D_1 \oplus M_2(D_2) \oplus M_5(\mathbb{Q}) \oplus M_3(D_3) \oplus M_3(\mathbb{Q}[\sqrt{5}])$$

with

$$D_1 = \left(\frac{-1,-1}{\mathbb{Q}[\sqrt{5}]}\right) \quad D_2 = \left(\frac{-1,-3}{\mathbb{Q}}\right) \quad D_3 = \left(\frac{-1,-1}{\mathbb{Q}}\right).$$

The group $\mathrm{SL}(2,5)$ satisfies the condition of Method 4.2 since it can be shown that the only component where no $\widehat{g}$ projects to a non-central idempotent is $\left(\frac{-1,-1}{\mathbb{Q}[\sqrt{5}]}\right)$ [24, Theorem 9.1].

We take the maximal order $\mathcal{O} = \mathbb{Z}\left[1, i, \frac{1}{2}(1+j), \frac{1}{2}(i+k)\right]$ in the quaternion algebra D_2. Let e be the primitive central idempotent associated to the component $M_2(D_2)$ and let ι be the isomorphism between $M_2(D_2)$ and $\mathbb{Q}Ge$. Let U be the subset of $\mathbb{Q}G$ containing the elements

$$1 + \iota\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, 1 + \iota\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, 1 + \iota\begin{pmatrix} 0 & i \\ 0 & 0 \end{pmatrix}, 1 + \iota\begin{pmatrix} 0 & 0 \\ i & 0 \end{pmatrix},$$

$$1 + \iota\begin{pmatrix} 0 & \frac{1}{2}(1+j) \\ 0 & 0 \end{pmatrix}, 1 + \iota\begin{pmatrix} 0 & 0 \\ \frac{1}{2}(1+j) & 0 \end{pmatrix},$$

$$1 + \iota\begin{pmatrix} 0 & \frac{1}{2}(i+k) \\ 0 & 0 \end{pmatrix}, 1 + \iota\begin{pmatrix} 0 & 0 \\ \frac{1}{2}(i+k) & 0 \end{pmatrix}.$$

Then $\langle U \cup \mathcal{B}_1 \cup \mathcal{B}_2 \rangle$ is commensurable with $\mathcal{U}(\mathbb{Z}G)$.

References

[1] H. Bass, The Dirichlet unit theorem, induced characters, and Whitehead groups of finite groups, Topology 4 (1966) 391–410.

[2] J. Ritter, S. K. Sehgal, Generators of subgroups of $U(\mathbf{Z}G)$, in: Representation theory, group rings, and coding theory, vol. 93 of *Contemp. Math.*, Amer. Math. Soc., Providence, RI, 331–347, 1989.

[3] J. Ritter, S. K. Sehgal, Construction of units in integral group rings of finite nilpotent groups, Trans. Amer. Math. Soc. 324 (2) (1991) 603–621.

[4] J. Ritter, S. K. Sehgal, Construction of units in group rings of monomial and symmetric groups, J. Algebra 142 (2) (1991) 511–526.

[5] E. Jespers, G. Leal, Generators of large subgroups of the unit group of integral group rings, Manuscripta Math. 78 (1993) 303–315.

[6] B. Banieqbal, Classification of finite subgroups of 2×2 matrices over a division algebra of characteristic zero, J. Algebra 119 (2) (1988) 449–512.

[7] G. Nebe, Finite quaternionic matrix groups, Represent. Theory 2 (1998) 106–223 (electronic).

[8] M. Caicedo, Á. del Río, On the Congruence Subgroup Problem for integral group rings, J. Algebra 405 (2014) 1–34.

[9] E. Weiss, Algebraic number theory, Dover Publications, Inc., Mineola, NY, reprint of the 1963 original, 1998.

[10] R. W. Fitzgerald, Norm Euclidean quaternionic orders, Integers 12 (2) (2012) 197–208.

[11] E. Jespers, G. Olteanu, Á. del Río, Rational Group Algebras of Finite Groups: From Idempotents to Units of Integral Group Rings, Algebr. Represent. Theory 15 (2) (2012) 359–377.

[12] E. Jespers, Á. del Río, G. Olteanu, I. Van Gelder, Group rings of finite strongly monomial groups: Central units and primitive idempotents, J. Algebra 387 (2013) 99–116.

[13] M.-F. Vignéras, Arithmétique des algèbres de quaternions, vol. 800 of *Lecture Notes in Mathematics*, Springer, Berlin, 1980.

[14] I. Reiner, Maximal Orders, Academic Press, London, New York, San Fransisco, 1975.

[15] D. S. Passman, Permutation groups, W. A. Benjamin, Inc., New York-Amsterdam, 1968.

[16] S. K. Sehgal, Units in integral group rings, Longman Scientific and Technical, 1993.

[17] H. Bass, K-theory and stable algebra, Inst. Hautes Études Sci. Publ. Math. (22) (1964) 5–60.

[18] L. N. Vaseršteǐn, Structure of the classical arithmetic groups of rank greater than 1, Mat. Sb. (N.S.) 91(133) (1973) 445–470, 472.

[19] B. Liehl, On the group SL_2 over orders of arithmetic type, J. Reine Angew. Math. 323 (1981) 153–171.

[20] T. N. Venkataramana, On systems of generators of arithmetic subgroups of higher rank groups, Pacific J. Math. 166 (1) (1994) 193–212.

[21] E. Kleinert, Two theorems on units of orders, Abh. Math. Semin. Univ. Hambg. 70 (2000) 355–358.

[22] C. W. Curtis, I. Reiner, Methods of representation theory with applications to finite groups and orders. Vol. I, John Wiley & Sons Inc., New York, 1981.

[23] I. R. Shafarevich, Basic notions of algebra, vol. 11 of *Encyclopaedia of Mathematical Sciences*, Springer-Verlag, Berlin, translated from the 1986 Russian original by Miles Reid, Reprint of the 1997 English translation, Algebra, I, 2005.

[24] R. Brown, Frobenius groups and classical maximal orders, Mem. Amer. Math. Soc. 151 (717) (2001) viii+110.

[25] A. Olivieri, Á. del Río, J. J. Simón, On Monomial Characters and Central Idempotents of Rational Group Algebras, Comm. Algebra 32 (4) (2004) 1531–1550.

[26] A. Pita, Á. del Río, M. Ruiz, Groups of units of integral group rings of Kleinian type, Trans. Amer. Math. Soc. 357 (8) (2005) 3215–3237.

[27] O. Broche, A. Herman, A. Konovalov, A. Olivieri, G. Olteanu, Á. del Río, I. Van Gelder, *Wedderga - Wedderburn Decomposition of Group Algebras*, Version 4.6.0, http://www.cs.st-andrews.ac.uk/~alexk/wedderga, http://www.gap-system.org/Packages/wedderga.html, 2013.

[28] G. Olteanu, Á. del Río, An algorithm to compute the Wedderburn decomposition of semisimple group algebras implemented in the GAP package wedderga, Journal of Symbolic Computation 44 (5) (2009) 507 – 516.

[29] E. Jespers, G. Leal, Describing units of integral group rings of some 2-groups, Comm. Algebra 19 (6) (1991) 1809–1827.