Structure of group rings and the group of units of integral group rings[*]

E. Jespers

GROUP ALGEBRAS, REPRESENTATIONS AND COMPUTATION
14 October 2019 to 23 October 2019
ICTS Bangalore

Abstract

The main focus of this three hour course is outlining how to compute a large torsion-free subgroup (i.e. of finite index) of the unit group of the integral group ring of a finite group G. To do so several topics will be handled: the link between the isomorphism problem and the study of the unit group; constructions of units; examples of unit group calculations; Wedderburn decomposition of rational group algebras, including exceptional and non-exceptional components; generators of general linear groups over orders; large central subgroups and construction of central units; large subgroup constructions in unit groups of group rings; structure theorems of unit groups; abelianisation and amalgamation of unit groups.

[*] The author is supported in part by Onderzoeksraad of Vrije Universiteit Brussel, Fonds voor Wetenschappelijk Onderzoek (Belgium) and ICTS

1 Introduction

Most of these notes are based on [1, 2]. For further references we refer to the bibliography in these books.

Let R be a ring and G a group. The group ring RG is the free R-module with basis G, i.e. it consists of all formal sums

$$\sum_{g\in G} r_g g$$

with only a finite number of coefficients r_g different from 0, and with addition defined as

$$\sum_{g\in G} r_g g + \sum_{g\in G} r'_g g = \sum_{g\in G} (r_g + r'_g) g,$$

and it is equipped with the natural product that extends the products of both R and G, i.e.

$$\left(\sum_{g\in G} r_g g\right) \left(\sum_{h\in G} s_h h\right) = \sum_{x\in G} \left(\sum_{g,h\in G,\, gh=x} r_g s_h\right) x.$$

The support of an element $\alpha = \sum_{g\in G} r_g g \in RG$ is the finite set $\mathrm{supp}(\alpha) = \{g \in G \mid r_g \neq 0\}$.

The augmentation map of RG is the ring homomorphism

$$\mathrm{aug} : RG \to R : \sum_{g\in G} r_g g \mapsto \sum_{g\in G} r_g.$$

More generally, for a normal subgroup N of G, the augmentation map modulo N (also called the relative augmentation map) is the ring homomorphism

$$\mathrm{aug}_{G,N,R} RG \to R(G/N) : \sum_{g\in G} r_g g \mapsto \sum_{g\in G} r_g (gN).$$

The kernel of $\mathrm{aug}_{G,N,R}$ is the augmentation ideal of RG modulo N. If the ring is clear from the context we simply denote this map as $\mathrm{aug}_{G,N}$. It is readily verified that

$$\mathrm{Ker}(\mathrm{aug}_{G,N,R}) = \sum_{n\in N} (n-1) RG = \sum_{n\in N} RG(n-1).$$

If, furthermore, N is finite then

$$\widetilde{N} = \sum_{n\in N} n$$

is a central element of RG and $\widetilde{N}(1-n)=0$ for all $n \in N$. Hence,

$$\widetilde{N}^2 = |N|\widetilde{N}.$$

Moreover,

$$\mathrm{Ker}(\mathrm{aug}_{G,N,R} = \mathrm{Ann}_{RG}(\widetilde{N}) = \{\alpha \in RG \mid \alpha\widetilde{N} = 0\}.$$

If, furthermore $|N|$ is invertible in R then

$$\widehat{N} = \frac{1}{|N|}\widetilde{N}$$

is a central idempotent in RG and

$$RG = RG\widehat{N} \oplus RG(1-\widehat{N}) \quad \text{and} \quad R(G/N) = RG\widehat{N}.$$

The unit group of a ring R, denoted $\mathcal{U}(R)$, is the group

$$\mathcal{U}(R) = \{u \in R \mid uv = 1 = vu, \text{ some } v \in R\}.$$

The main theme of this course is the unit group of the integral group ring $\mathbb{Z}G$ of a finite group G. Of course, if $\alpha = \sum_{g\in G} r_g g \in \mathcal{U}(\mathbb{Z}G)$ then $\mathrm{aug}(\alpha) = \sum_{g \in G} r_g = \pm 1$. A unit $\alpha \in \mathbb{Z}G$ is said to be *normalized* if $\mathrm{aug}(\alpha) = 1$. The group consisting of all normalized units of $\mathbb{Z}G$ is often denoted by $V(\mathbb{Z}G)$. In this text I use the more indicative notation $\mathcal{U}_1(\mathbb{Z}G)$. Clearly

$$\mathcal{U}(\mathbb{Z}G) = \pm\mathcal{U}_1(\mathbb{Z}G).$$

Note that if R is a commutative ring then the group ring RG is endowed with an involution $*$ (often called the classical involution)

$$* : RG \to RG : \sum_{g\in G} r_g g \mapsto \sum_{g \in G} r_g g^{-1}.$$

The integral group ring is the ring that links group theory to ring theory. One hence has a natural fundamental question: the isomorphism problem for integral group rings of finite groups G and H:

$$\mathbb{Z}G \cong \mathbb{Z}H \implies G \cong H. \quad \text{(ISO)}$$

The following proposition is a remarkable fact for group rings: an integral group ring isomorphism is equivalent with unit group isomorphisms. To prove this, we first need a lemma. Of course $\mathbb{Z}G$ is a subring of the rational group algebra $\mathbb{Q}G$; and thus we can talk of ($\mathbb{Q}$-) independent elements in $\mathbb{Z}G$.

Lemma 1.1 *Let G be a finite group. The following properties hold for a finite subgroup H of G.*

1. *(Berman) If $\alpha = \sum_{g \in G} z_g g$ is a unit of finite order in $\mathcal{U}_1(ZG)$ such that $z_1 \neq 0$ (with 1 the identity of G) then $\alpha = 1$. In particular, if α is a normalized central unit of finite order then $u \in Z(G)$.*
2. *H is a set of independent elements; in particular, $|H| \leq |G|$.*
3. *If $|H| = |G|$ then $\mathbb{Z}G = \mathbb{Z}H$.*

Proof. (1) This will be proved in the session on torsion units.

(2) Assume that $\sum_{h \in H} z_h h = 0$, with each $z_h \in \mathbb{Z}$. Let $x \in H$. Since, by assumption, H is finite, also hx^{-1} is unit of finite order in $\mathcal{U}_1(\mathbb{Z}G)$. Clearly, $hx^{-1} \neq 1$ if $h \neq x$. Hence, by part (1), the coefficient of 1 in $hx^{-1} = 0$. Since the coefficient of 1 in $\sum_{h \in H} z_h hx^{-1}$ equals z_x, we conclude that $z_x = 0$. Since x is arbitrary, part (2) follows.

(3) Assume H is a finite subgroup of $\mathcal{U}_1(\mathbb{Z}G)$ and $|H| = |G|$. By part (2) the elements of H are independent and thus $\mathbb{Q}G = \mathbb{Q}H$. So, $\mathbb{Z}H \subseteq \mathbb{Z}G$ and $n\mathbb{Z}G \subseteq \mathbb{Z}H$ for some positive integer n. It remains to show that if $g \in G$ then $g \in \mathbb{Z}H$. So, let $g \in G$ and write $ng = \sum_{h \in H} z_h h$, with each $z_h \in \mathbb{Z}$. Then $ngh^{-1} = z_h + \sum_{h' \in H, h' \neq h} z_h (h'h^{-1})$. As $1 \neq h'h^{-1}$ is periodic, it follows from part (1) that the coefficient of 1 of $h'h^{-1}$ is 0. Therefore, the coefficient of 1 in ngh^{-1} equals z_h. Hence it has to be divisible by n. As h is arbitrary we have shown that for every $h \in H$ in the support of ng we have that $n|h$. Consequently, $ng \in n\mathbb{Z}H$ and thus $g \in \mathbb{Z}H$, as desired. $\blacksquare$

Proposition 1.2 *Let G and H be finite groups. The following statement are equivalent.*

1. *$\mathbb{Z}G \cong \mathbb{Z}H$ (ring isomorphism),*
2. *$\mathcal{U}_1(\mathbb{Z}G) \cong \mathcal{U}_1(\mathbb{Z}H)$ (group isomorphism),*
3. *$\mathcal{U}(\mathbb{Z}G) \cong \mathcal{U}(\mathbb{Z}H)$ (group isomorphism).*

Proof. Clearly (1) implies (3). For the other implication it is useful to turn any isomorphism into a normalized isomorphism. This is done as follows, for any commutative ring R. Let $f : \mathcal{U}(RG) \to \mathcal{U}(RH)$ be a group isomorphism. Define

$$f^* : \mathcal{U}(RG) \to \mathcal{U}(RH) : \sum_{g \in G} r_g g \mapsto \sum_{g \in G} r_g \left(\operatorname{aug}_H(f(g))\right)^{-1} f(g).$$

It is readily verified that f^* is an isomorphism that preserves augmentation, i.e. $\text{aug}_H(f^*(g)) = 1$ for all $g \in G$ and thus $\text{aug}_H(f^*(\alpha)) = \text{aug}_G(\alpha)$ for all $\alpha \in \mathcal{U}(RG)$. Hence, (3) implies (2).

Now, assume (2) holds, i.e. assume $f : \mathcal{U}_1(\mathbb{Z}H) \to \mathcal{U}_1(\mathbb{Z}G)$ is a group isomorphism. Then $f(H)$ is a finite subgroup of $\mathcal{U}_1(\mathbb{Z}G)$ that is isomorphic to H. Hence, by Lemma 1.1, $|H| = |f(H)| \leq |G|$. Similarly, $|G| \leq |H|$ and thus $|H| = |G|$. Furthermore, by Lemma 1.1, the $\mathbb{Z}f(H) = \mathbb{Z}G$ and thus we obtain an isomorphism $\mathbb{Z}H \to \mathbb{Z}G$, as desired. ∎

Hence, (ISO) is equivalent with

$$\mathcal{U}(\mathbb{Z}G) \cong \mathcal{U}(\mathbb{Z}H) \implies G \cong H. \quad \text{(ISO')}$$

It is a hard problem to fully describe the unit group of the integral group ring of a finite group, and hence one often focusses on describing a large subgroup, i.e. a subgroup of finite index. Preferably one would like a torsion-free subgroup of index exactly $|G|$. In other words we have the following problem.

Problem 1.3 *: Let G be a finite group. Does there exists a torsion-free subgroup of finite index, say N such that $|\mathcal{U}_1(\mathbb{Z}G)/N| = |G|$. This means that*

$$\mathcal{U}_1(\mathbb{Z}G) = N \rtimes G,$$

a semidirect product of groups (i.e the inclusion $G \to \mathcal{U}_1(\mathbb{Z}G)$ splits).

It easily is verified that an affirmative answer to Problem 1.3 gives an affirmative answer to (ISO). In case G is a nilpotent group it is sufficient to check that there is a normal complement.

Note that Roggenkamp and Scott gave a metabelian counter example to the problem (nevertheless, Withcomb proved (ISO) holds for finite metabelian groups). However, because of the link with (ISO), it remains a challenge to determine classes of groups for which there is a positive answer. A positive answer to Problem 1.3 has been proved in case G is a finite abelian group, and more general for finite groups G having an abelian normal subgroup A such that either G/A has exponent dividing 4 or 6, or G/A is abelian of odd order (by Cliff-Sehgal-Weiss).

However, the general problem remains open. In [3] two problems in this context are being stated.

Problem 1.4 *Does Problem 1.3 have an affirmative answer if G is a finite nilpotent group? Even in case G has nilpotency class three the answer is not known. For class two the answer is affirmative.*

Nevertheless, using other methods, for finite groups, (ISO) has been proven for metabelian groups (Whitcomb), nilpotent groups (Roggenkamp and Scott) and simple groups (Kimmerle, Lyons, Sandling). Hertweck has given a counter example to the isomorphism problem. It is a group of order $2^{21}97^{28}$, with a normal Sylow 97-subgroup and the group has derived length 4.

2 Construction of Units

In order to study the unit group $\mathcal{U}(\mathbb{Z}G)$, with G a finite group, one first would like to know some generic construction of units.

Trivial units
Clearly $\pm G \subseteq \mathcal{U}(\mathbb{Z}G)$. These are called the trivial units.

Unipotent units and bicyclic units
Let R be an associative ring with identity element 1. Let η be a nilpotent element of R, i.e. $\eta^k = 0$ for some positive integer k. Then

$$(1-\eta)(1+\eta+\cdots+\eta^{k-1}) = 1 = (1+\eta+\cdots+\eta^{k-1})(1-\eta).$$

So from nilpotent elements one can construct units. Note that the rational group algebra $\mathbb{Q}G$ has no non-zero nilpotent elements if and only if $\mathbb{Q}G$ is a direct sum of division algebras (excercise). Hence for most finite groups the group algebra has nilpotent elements (the only exceptions being the abelian groups and the Hamiltonian groups of order $2^m t$, with t an odd number such that the multiplicative order of 2 modulo t is odd).

One can construct nilpotent elements from almost idempotent elements $e \in R$ (i.e. $e^2 = ne$ for some positive integer n). For any $r \in R$,

$$((n-e)re)^2 = 0$$

and thus

$$1 + (n-e)re$$

is a unipotent unit (with inverse $1-(n-e)re$).

Let G be a finite group and let e be an idempotent in $\mathbb{Q}G$ (recall that $\mathbb{Z}G$ only contains 0 and 1 as idempotents, see Section 5). Let n_e be the smallest positive integer such that $n_e e \in \mathbb{Z}G$. Then, for $h \in G$,

$$b(h,e) = 1 + n_e^2(1-e)he \quad \text{and} \quad b(e,h) = 1 + n_e^2 eh(1-e)$$

are unipotent units in $\mathbb{Z}G$. They are called *generalized bicyclic units.*

In group rings one can easily construct idempotents. Indeed, let $g \in G$ be an element of order n. Then,

$$\widehat{g} = \widehat{\langle g \rangle} = \frac{1}{n}\widetilde{\langle g \rangle} = \frac{1}{n}\widetilde{g} = \frac{1}{n}\sum_{0 \le i \le n-1} g^i$$

is an idempotent in $\mathbb{Q}G$ and $\widetilde{g}$ is an almost idempotent in $\mathbb{Z}G$. The units

$$b(h, \widetilde{g}) = 1 + (1-g)h\widetilde{g} \quad \text{and} \quad b(\widetilde{g}, h) = 1 + \widetilde{g}h(1-g)$$

are called the *bicyclic units* of $\mathbb{Z}G$. Obviously, $b(h, \widetilde{g})^{-1} = b(-h, \widetilde{g})$. Note that a bicyclic unit $b(h, \widetilde{g})$ is trivial unit if and only if $h \in N_G(\langle g \rangle)$; otherwise it is a unit of infinite order.

Note that $b(h, \widehat{g}) = b(\alpha, \widetilde{g})$ for some $\alpha \in \mathbb{Z}\langle g \rangle$. Further note that for a bicyclic unit it is easy to verify that such a unit either is trivial or it is of infinite order. Also note that $b(h, \widetilde{g})$ is a non-trivial unit precisely when h is not in the normalizer of $\langle g \rangle$. Similarly for $b(\widetilde{g}, h)$.

Cyclotomic units and Bass units

Let R be an associative ring and x a unit of finite order n. Let k and n be relatively prime positive integers and let m be a positive integer such that $k^m \equiv 1 \bmod n$. Then

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

is an invertible element in R with inverse $u_{l,m}(x^k)$, where l is a positive integer such that $kl \equiv 1 \bmod n$. Note that if R is a domain and $x \neq 1$ then $(1-x)((1 + x + \cdots + x^{n-1}) = 0$ implies that $1 + x + \cdots + x^{n-1} = 0$ and thus, in this case, $u_{k,m} = (1 + x + \cdots + x^{k-1})^m$. If, furthermore, R is a field then $u_{k,m} = (1 + x + \cdots + x^{k-1})^m = \left(\frac{1-x^k}{1-x}\right)^m$. The unit $\frac{1-x^k}{1-x}$ is called a *cyclotomic unit* and is denoted

$$\eta_k(x) = \frac{1-x^k}{1-x}.$$

Note that $(\eta_k(x))^{-1} = \eta_l(x^k)$, where l is a positive integer such that $lk \equiv 1 \bmod n$. Hence $\eta_k(x) \in \mathcal{U}(\mathbb{Z}[x])$.

We also remark that if $x \in R$ is a unit of finite odd order then $-x$ has even order and $u_{k,m}(-x) = (1 - x + x^2 + \cdots + (-1)^{k-1})^m$. Such units are called *alternating units* in integral group rings [3].

Let G be a finite group. We remark that, for $g \in G$,

$$u_{k,m}(g) = u_{k',m}(g) \qquad \text{if } k \equiv k' \bmod |g|.$$

Hence, in the definition of $u_{k,m}(g)$ we may assume that $1 < k < |g|$. The units $u_{k,m}(g)$, with $g \in G$ and $(k, |g|) = 1$ are called the *Bass units* of $\mathbb{Z}G$. One can also show that

$$u_{k,m}(g)u_{k,m_1}(g) = u_{k,m+m_1}(g).$$

We now show that almost all Bass units are of infinite order.

Lemma 2.1 *Let G be a finite group and $g \in G$. A Bass unit $u_{k,m}(g)$ is torsion if and only if $k \equiv \pm 1 \mod |g|$.*

Proof. Let $n = |g|$ and let $u = u_{k,m}(g)$. If $k \equiv 1 \bmod n$ then $u = 1$ and the result is clear in this case.

So, assume that $k \not\equiv 1 \bmod n$ and in particular $n > 1$. If $k = n - 1$ and $m = 2$ then $u = (\widetilde{g} - g^{n-1})^2 - \frac{1-(n-1)^2}{n}\widetilde{g} = g^{-2}$. If $k \equiv -1 \bmod n$ then m is a multiple of 2 and thus $u = u_{n-1,m}(g) = u_{n-1,2}(g)^{\frac{m}{2}} = g^{-m}$. This proves that if $k \equiv \pm 1 \bmod n$ then u is torsion.

Conversely, assume that u is torsion. Let ζ be a complex root of unity of order n. By the Universal Property of Group Rings, the group isomorphism $\langle g \rangle \to \langle \zeta \rangle$, mapping g to ζ, extends to a ring homomorphism $f : \mathbb{Z}G \to \mathbb{C}$. As $n > 1$, $f(\widetilde{g}) = 0$ and therefore $f(u) = \eta_k(\zeta)^m$. Since u is torsion, $f(u)$ is a root of unity, hence so is $\eta_k(\zeta)$. This implies that $|\zeta^k - 1| = |\zeta - 1|$. Thus ζ and ζ^k are two vertices of a regular polygon with n vertices so that ζ and ζ^k are at the same distance to 1. This implies that ζ^k is either ζ or $\overline{\zeta} = \zeta^{-1}$. Then $k \equiv \pm 1 \bmod n$, as desired. ∎

We have so far introduced two type of units, the Bass units and the bicyclic units. The constructions of these are based on the cyclotomic units and unipotent units. These units are of great importance for the unit group $\mathcal{U}(\mathbb{Z}G)$. The main reason being the following results.

Theorem 2.2 *Let ξ be a complex root of unity. The cyclotomic units of $\mathbb{Z}[\xi]$ generate a subgroup of finite index in $\mathcal{U}(\mathbb{Z}[\xi])$.*

For a ring R and positive integer n, we denote by

$$e_{ij}(r) \in M_n(R)$$

the unipotent matrix $1 + rE_{ij}$, where E_{ij} is the elementary matrix that has only one nonzero entry (at position (i, j)) and this entry equals 1. A useful formula is

$$E_{ij}E_{kl} = \delta_{jk}E_{il}.$$

Proposition 2.3

1. *The group $SL_n(\mathbb{Z})$ is generated by the matrices e_{ij} with $i \neq j$.*
2. *(Sanov) Let $z_1, z_2 \in \mathbb{C}$ such that $|z_1 z_2| \geq 4$ then $\langle e_{12}(z_1), e_{21}(z_2)\rangle$ is a free group of rank 2, where $e_{ij} = 1 + E_{ij}$ and E_{ij} has a one on the (i,j) spot and zeroes elsewhere.*
3. *The group $\left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) \mid a \equiv d \equiv 1 \ mod \ 4, \right\}$ is a free group of rank 2 generated by $e_{12}(2)$ and $e_{21}(2)$.*

Let R be a commutative Noetherian domain with field of fractions F and let A be a finite dimensional F-algebra. A full R-lattice in a finite dimensional F-vectorspace V is a finitely generated R-submodule of V (i.e. an R-lattice in V) that contains a basis of V. An R-order in A is a subring of A which also is a full R-lattice in A. A $\mathbb{Z}$-order will be simply called an order. Because $\mathbb{Z}$ is a PID, an order contains a $\mathbb{Z}$-basis and this obviously also is a $\mathbb{Q}$-basis of A. Obviously, if G is a finite group then $\mathbb{Z}G$ is an order in $\mathbb{Q}G$ and $M_n(R)$ is an R-order in $M_n(F)$. Also, if $\mathcal{O}$ is an order in A then $M_n(\mathcal{O})$ is an order in $M_n(A)$. The integral quaternions $\left(\frac{-1,-1}{\mathbb{Z}}\right)$ is a order in the division algbera $\left(\frac{-1,-1}{\mathbb{Q}}\right)$ (see Section 4).

With "elementary methods" one can calculate the unit group of some some well known rings. By ξ_n we denote a complex root of unity of order n.

1. $\mathcal{U}(\mathbb{Z}) = \{-1, 1\}$.
2. $\mathcal{U}(\mathbb{Z}[i]) = \{1, -1, i, -i\}$.
3. $\mathcal{U}(\mathbb{Z}[\xi_3]) = \{\pm 1, \pm\xi_3, \pm\xi_3^2\}$.
4. $\mathcal{U}(\mathbb{Z}[\xi_6]) = \langle \xi_6 \rangle$.
5. $\mathcal{U}(\mathbb{Z}[\xi_8]) = \langle \xi_8 \rangle \times \langle 1+\sqrt{2}\rangle = \langle \xi_8 \rangle \times \langle \eta_3(\xi_8)\rangle = C_8 \times C_\infty$ and $\eta_3(\xi_8) = 1 + \xi_8 + \xi_8^2$.
6. $U(\mathbb{Z}C_5) = \pm C_5 \times \langle g + g^4 - 1\rangle$, where $C_5 = \langle g \mid g^5 = 1\rangle$.
7. $U_1(\mathbb{Z}C_8) = C_8 \times \langle u_{3,2}(g)\rangle = C_8 \times C_\infty$, where $C_8 = \langle g \mid g^8 = 1\rangle$.
8. $\mathcal{U}\left(\left(\frac{-1,-1}{\mathbb{Z}}\right)\right) = Q_8$, where Q_8 is the quaternion group of order 8.
9. (Higman) $\mathcal{U}_1(\mathbb{Z}Q_8) = Q_8$
10. $\mathcal{U}_1(\mathbb{Z}D_8) = B \rtimes D_8$, where B is the subgroup generated by the bicyclic units. Furthermore, B is a free group of rank 3

The previous list contains several examples of unit groups that are finite. Actually all relevant groups are included in these examples as shown by the following result of Higman.

Theorem 2.4 *(Higman) The following conditions are equivalent for a finite group G.*

1. *$\mathcal{U}_1(\mathbb{Z}G)$ is finite.*
2. *$\mathcal{U}_1(\mathbb{Z}G) = G$.*
3. *G is an abelian group of exponent dividing 4 or 6, or $G \cong Q_8 \times E$, with Q_8 the quaternion group of order 8 and E an elementarry abelian 2-group (i.e. a direct product of copies of the cyclic group C_2 of order 2.*

For the proof of this result one can make use of the Bass units and bicylic units and of the fact that if $\mathcal{U}_1(\mathbb{Z}G)$ is finite then so is the unit group $\mathcal{U}_1(|Z(G \times C_2))$.

So, for almost all finite groups G, the unit group $\mathcal{U}_1(\mathbb{Z}G)$ is infinite. Actually one can prove that if the unit group $\mathcal{U}(\mathbb{Z}G)$ is infinite and G is not abelian and not a Hamiltonian group, i.e. not all subgroups are normal, then $\mathcal{U}(\mathbb{Z}G)$ contains a free group of rank 2 generated by two bicyclic units.

To prove this result we show a more general result due to Salwa.

Theorem 2.5 *Let R be a torsion-free ring and $a, b \in R$ such that $a^2 = b^2 = 0$. Then the group $\langle 1+a, 1+b\rangle$ is free if and only if either ab is transcendental or ab is algebraic (over $\mathbb{Q}$) and one of the eigenvalues λ of ab is a free point (that is $\langle e_{12}(1), e_{21}(\lambda)\rangle$ is a free group).*

Proof. In these notes we are interested in group rings of finite groups. Hence, we will indicate a proof in the case ab is algebraic. Without loss of generality, we may assume that $R = \mathbb{Z}[a, b]$, that is, R is a $\mathbb{Z}$-module and as a ring it is generated by $\mathbb{Z}$ and a and b. Let $A = \mathbb{Q}[a, b]$. Let $J = J(A)$ denote the Jacobson radical of A. By assumption ab is algebraic over $\mathbb{Q}$ and thus $\mathbb{Q}[a, b] = \mathbb{Q}[ab] + b\mathbb{Q}[ab] + \mathbb{Q}[ab]a + b\mathbb{Q}[ab]a$ is finite dimensional over $\mathbb{Q}$ and J is a nilpotent ideal. As $(1 + J^n)/(1 + J^{n+1})$ is central in $(1 + J)/(1 + J^{n+1})$ we deduce that $1 + J$ is a nilpotent group and hence so is $(1+J) \cap \langle 1+a, 1+b\rangle$. Thus $\langle 1+a, 1+b\rangle$ is free if and only if so is $\langle 1+\overline{a}, 1+\overline{b}\rangle \subseteq \mathcal{U}(A/J)$.

Now, let ρ denote the regular representation of A over $\mathbb{Q}$. Let $\lambda_1, \ldots, \lambda_k$ be the non-zero eigenvalues of $\rho(ab)$. One then can prove that

$$\overline{A} = A/J \cong \mathbb{Q}^m \oplus \prod_{i=1}^{n} M_2(\mathbb{Q}(\mu_i)),$$

with $\{\mu_1, \dots, \mu_n\} = \{\lambda_1, \dots, \lambda_k\}$ and the isomorphism associates $1+\overline{a}$ and $1+\overline{b}$ with $(1, \dots, 1, e_{12}(1), \dots, e_{12}(1))$ and $(1, \dots, 1, e_{21}(\mu_1), \dots, e_{21}(\mu_k))$ respectively. It follows that $\langle 1+a, 1+b\rangle$ is free if and only if each $\langle e_{12}(1), e_{21}(\mu_i)\rangle$ is a free group and thus the result follows. ▮

If G is a finite group of order n and R is a commutative ring then the trace function of RG is the map $T : RG \to R$ associating to each element of RG the coefficient of 1, i.e. $T(\sum_{g\in G} r_g g) = r_1$. Let ρ denote the regular representation given by left multiplication. Then $T(x) = \frac{1}{n}\mathrm{tr}(\rho(x))$, for every $x \in RG$. So, in case $R = \mathbb{C}$ then T can be considered as the restriction of $\frac{1}{n}\mathrm{tr}$ to $\mathbb{C}G$. Salwa also proved the following

Recall that a trace function T on a complex algebra A is a $\mathbb{C}$ linear map $A \to \mathbb{C}$ such that $T(ab) = T(ba)$ for $a, b \in A$, $T(e)$ is a positive real number for all non-zero idempotents $e \in A$ and $T(a) = 0$ for every nilpotent element $a \in A$.

Proposition 2.6 *Let A be a complex algebra and let T be a trace function on A. If $a, b \in A$ are such that $a^2 = b^2 = 0$ and $|T(ab)| \geq 2T(1)$ then $\langle 1+a, 1+b\rangle$ is a free group.*

Theorem 2.7 *(Marciniak-Sehgal) Let G be a finite group and let u be a non-trivial bicyclic unit then $\langle u, u^*\rangle$ is a free group of rank 2.*

Proof. Let T be the above mentioned trace map om $\mathbb{C}G$ and let $u = b(g, \widetilde{h}) \neq 1$ with $g, h \in G$. Let $a = u - 1 = (1-h)g\widetilde{h}$ and $b = a^* = \widetilde{h}g^{-1}(1-h^{-1})$. Then $ba = \widetilde{h}g^{-1}(2-h-h^{-1})g\widetilde{h} = \widetilde{h}(2-z-z^{-1})\widetilde{h}$, with $z \notin \langle h\rangle$. Therefore, $T(ab) = T(ba) = 2|h| \geq 4 = 4T(1)$. Hence, $\langle u = 1+1, u^* = 1+b\rangle$ is free by the previous Proposition. This proves the result for $u = b(g, \widetilde{h}) \neq 1$. A similar argument deals with $u = b(\widetilde{h}, g)$. ▮

3 Wedderburn decomposition and primitive central idempotents

We begin by recalling the fundamental theorem describing semisimple rings.

Theorem 3.1 *(Wedderburn-Artin) A ring R is semisimple if and only if R is isomorphic to a finite direct product of matrix rings over division rings.*

So, if R is a semisimple algebra then

$$R = M_{n_1}(D_1) \times \cdots \times M_{n_k}(D_k) = Re_1 \times \cdots \times Re_k,$$

where $n_1, \ldots, n_k$ are positive integers, each D_i is a division ring and each e_i is a primitive central idempotent.

Theorem 3.2 *Let R be a ring and G a group. The group ring RG is semisimple if and only if R is semisimple, G is finite and $|G|$ is invertible in R (i.e. $|G|r = 1$ for some $r \in R$). In case R is a field, the latter means that $|G|$ is not a multiple of the characteristic of R*

If F is a field and G is a finite group such that FG is semisimple then

$$FG = M_{n_1}(D_1) \times \cdots \times M_{n_k}(D_k) = FGe_1 \times \cdots \times FGe_k,$$

and each simple algebra FGe_i is as an F-algebra generated by the finite group $Ge_i = \{ge_i \mid g \in G\}$. Clearly, $Ge_i \cong G/S_G(e_i)$, where $S_G(e_i) = \{g \in G \mid ge_i = e_i\}$, the stabiliser of e_i in G. In case G is abelian then, of course, each $n_i = 1$ and D_i is a field. Since finite subgroups of a field are cyclic, we get that, in this case each $FGe_i = F(\xi_{n_i})$, where ξ_{n_i} is a primitive n_i-th root of unity in the algebraic closure of F. One can then prove the following result.

Theorem 3.3 *(Perlis-Walker) Let G be a finite abelian group and F a field of characteristic 0. Let k_d denote the number of cyclic subgroups of G of order d. Then*

$$FG \cong \prod_{d,\ d||G|} F(\xi_d)^{k_d \frac{[\mathbb{Q}(\xi_d):\mathbb{Q}]}{[F(\xi_d):F]}}.$$

In particular,

$$\mathbb{Q}G \cong \prod_{d,\ d||G|} \mathbb{Q}(\xi_d)^{k_d}.$$

One can also compute the primitive central idempotents of a rational group algebra of a finite abelian group. To do so, we introduce some notation.

Let G be a finite group and N a normal subgroup of G. Let F be a field whose characteristic does not divide $|G|$. In FG consider the elements

$$\varepsilon(G, N) = \begin{cases} \widehat{G} & \text{if } G = N \\ \prod_{D/N \in M(G/N)} (\widehat{N} - \widehat{D}), & \text{otherwise} \end{cases}$$

Here $M(G/N)$ denotes the set of the minimal non-trivial normal subgroups D/N of G/N, with D a subgroup of G containing N. It easily is verified that $\varepsilon(G, N)$ is a central idempotent of FG.

Lemma 3.4 *If e is a primitive central idempotent of $\mathbb{Q}G$ such that $\mathbb{Q}G$ is a field then $e = \varepsilon(G, N)$ where $N = S_G(e)$ and $\mathbb{Q}Ge = \mathbb{Q}(\xi_d)$, where $d = |G/N|$.*

Corollary 3.5 *Let G be a finite abelian group. The primitive central idempotents of $\mathbb{Q}G$ are the elements $\varepsilon(G, N)$ with N a subgroup of G such that G/N is a cyclic group.*

Note that primitive central idempotents of a complex group $\mathbb{C}G$ of a finite group also are well known. Indeed, denote by $\mathrm{Irr}(G)$ the set of the irreducible complex characters of G. If $\chi \in \mathrm{Irr}(G)$ then

$$e(\chi) = \frac{\chi(1)}{|G|} \sum_{g \in G} \chi(g^{-1})g$$

is a primitive central idempotent of $\mathbb{C}G$. Moreover, it is the unique primitive central idempotent $e \in \mathbb{C}G$ such that $\chi(e) \neq 0$. One can replace, in the above, the field $\mathbb{C}$ by any splitting field F of G. That is, $FG = \prod_i M_{n_i}(F)$. The Brauer splitting theorem states that $\mathbb{Q}(\xi_{|G|})$ is a splitting field of G (where $\xi_{|G|}$ is a primitve $|G|$-th root of unity). More generally, it says that if F is a field and FG is semisimple then $F(\xi_{|G|})$ is a splitting field of G.

If FG is not necessarily split then it much more complicated to describe the primitive central idempotents of FG. In theory one can determine the primitive central idempotents of FG, via Galois-descent, from the primitive central idempotents of $F(\xi_{|G|})G$. However this does not necessarily result in some nice generic formulas. However, for some classes of groups one can obtain nice descriptions in terms of the group G. The class includes the abelian-by-supersolvable groups. We will explain such formulas for $\mathbb{Q}G$.

We need to introduce some terminology and notation.

Proposition 3.6 *Let G be a finite group and H and K subgroups of G such that $K \subseteq H$. Then, Lin$(H, K) = \{\chi \mid \chi$ a linear complex character with $\mathrm{Ker}(\chi) = K\} \neq \emptyset$ if and only if the following conditions hold*

(S1) $K \lhd H$,

(S2) H/K is cyclic.

Assume that (S1) and (S2) hold for $\chi \in$ Lin(H, K). Then χ^G is absolutely irreducible if and only if (H, K) satisfies the following condition:
(S3) for every $g \in G \setminus H$ there exists $h \in H$ such that $(h, g) \in H \setminus K$.

A Shoda pair of a finite group G is a pair (H, K) of subgroups of G satisfying conditions (S1), (S2) and (S3).

Proof. The first part follows from the fact that every finite subbgroup of a field is cyclic. The second part is due to Shoda. ∎

Theorem 3.7 *(Olivieri, del Río, Simón) If (H,K) is a Shoda pair of a finite subgroup G and $\chi \in Lin(H,K)$ then χ^G is an absolutely irreducible character and there is a unique primitve central idempotent e of $\mathbb{Q}G$, denoted, $e_{\mathbb{Q}}(\chi)$, such that $\chi^G(e) \neq 0$. Furthermore,*

$$e_{\mathbb{Q}}(\chi^G) = \frac{[Cen_G(\varepsilon(H,K)) : H]}{[\mathbb{Q}(\chi) : \mathbb{Q}(\chi^G)]} e(G,H,K),$$

where

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

and T is a right transversal of $Cen_G(\varepsilon(H,K))$ in G. The unique Wedderburn component containing $e(G,H,K)$ is $\mathbb{Q}Ge(G,H,K)$, it will be denoted $A_{\mathbb{Q}}(G,H,K)$.

A character of a finite group is said to be monomial if it is the character afforded by a representation induced from a linear character. One says that G is a monomial group if every irreducible complex character of G is monomial.

Corollary 3.8 *A finite group G is monomial if and only if every primitive central idempotent of $\mathbb{Q}G$ is of the form $qe(G,H,K)$ for (H,K) a Shoda pair of G and $q \in \mathbb{Q}$.*

This result allows to compute all primitive central idempotents of $\mathbb{Q}G$ for G a finite monomial group and this without actually computing the monomial absolutely irreducible characters of G. It suffices to compute all the Soda pairs (H,K) of G, compute $e(G,H,K)$ and then compute the rational q such that $qe(G,H,K)$ is an idempotent. Note that different Shoda pairs can determine the same primitive central idempotent. Janssens determined a formula for all primitive central idempotents of $\mathbb{Q}G$ for arbitrary finite groups G (the main tool used is Artin's Induction Theorem). Note that the formula yields a rational linear combination of elements of the form $e(G,C,C)$ where C is a cyclic subgroup of G; but in general $e(G,C,C)$ is not an idempotent.

So, for some classes of groups one can compute explicitly the primitive central idempotents e. A next step is to determine a description of the simple component $\mathbb{Q}Ge$. In order to compute the unit group $\mathcal{U}(\mathbb{Z}G)$ one would like to obtain a concrete description that yields control on the rational representations (without having to calculate the character table of G). We now show how this can be done for $e(G, H, K)$ provided the Shoda Pair satisfies some additional conditions.

A useful lemma is the following.

Lemma 3.9 *Let H and K be subgroups of a finite group G such that $K \lhd H$ and H/K is cyclic. Assume $\varepsilon(H, K)\varepsilon(H, K)^g = 0$ for all $g \in G \setminus Cen_G(\varepsilon(H, K))$. Then $Cen_G(\varepsilon(H, K)) = N_G(K) = \{g \in G \mid g^{-1}Kg = K\}$.*

Proposition 3.10 *Let G be a finite group and let H and K be subgroups such that $K \subseteq H$. The following conditions are equivalent.*

1. *(H, K) is a Shoda pair of G, $H \lhd N_G(K)$ and the different G-conjugates of $\varepsilon(H, K)$ are orthognal.*

2. *(H, K) is a strong Shoda pair, that is,*

   (SS1) $H \lhd N_G(K)$,

   (SS2) H/K is cyclic and maximal abelian subgroup of $N_G(K)/K$ and

   (SS3) for every $g \in G \setminus N_G(K)$, $\varepsilon(H, K)\varepsilon(H, K)^g = 0$

3. *The following conditions hold*

   (SS1') $H \lhd Cen(\varepsilon(H, K))$,

   (SS2') H/K is cyclic and a maximal abelian subgroup of $Cen(\varepsilon(H, K))$ and

   (SS3') for every $g \in G \setminus Cen(\varepsilon(H, K))$, $\varepsilon(H, K)\varepsilon(H, K)^g = 0$.

A finite group is said to be strongly monomial if every irreducible complex character of G is strongly monomial, i.e. it is of the form χ^G for $\chi \in Lin(H, K)$ and (H, K) a strong Shoda pair of G. Note that for such a group every primitive central idempotent of $\mathbb{Q}G$ is of the form $e(G, H, K)$ with (H, K) a strong Soda pair of G.

Theorem 3.11 *Every abelian-by-supersolvable finite group is strongly monomial.*

A useful fact to prove this result is the following. If G is finite supersolvable group and N a maximal abelian normal subgroup of G then N is a maximal abelian subgroup of G. Prove this as an excercise.

Proposition 3.12 *Let (H, K) be a pair of subgroups of a finite group G such that $K \lhd H \lhd G$ and satisfying (SS2) (i.e. H/K is cyclic and a maximal abelian subgroup of $N_G(K)/K$). Then (H, K) is a strong Shoda pair of G.*

Theorem 3.13 *Let G be a finite metabelian group and let A be a maximal abelian subgroup of G containing the commutator subgroup G'. The primitive central idempotents of $\mathbb{Q}G$ are the elements of the form $e(G, H, K)$ where (H, K) is a pair of subgroups of G satisfying the following conditions:*

1. *H is a maximal element in the set $\{B \leq G \mid A \leq B$ and $B' \subseteq K \subseteq B\}$ and*
2. *H/K is cyclic.*

One can describe the simple components of $\mathbb{Q}G$ for G a finite strongly monomial group.

Theorem 3.14 *Let (H, K) be a strong Shoda pair of the finite group G and $\chi \in Lin(H, K)$, $N = N_G(K)$, $n = [G : N]$, $h = [H : K]$ and $\overline{x} = xK$ a generator of the group H/K. The following properties hold.*

1. *$N = Cen_G(\varepsilon(H, K))$,*
2. *$e_{\mathbb{Q}}(\chi^G) = e(G, H, K)$,*
3. *The mapping $\sigma : N/H \to Gal(\mathbb{Q}(\xi_h)/\mathbb{Q}(\chi^G))$ defined by $\overline{y} \mapsto \sigma_{\overline{y}}$, for $\overline{y} \in N/H$, with*
$$\sigma_{\overline{y}}(\xi_h) = \xi_h^i$$
where i is such that $\overline{yxy}^{-1} = \overline{x}^i$, is an isomorphism.
4. *$A_{\mathbb{Q}}(G, H, K) \cong M_n\left(\mathbb{Q}(\xi_h) * (N/H)\right) \cong M_n(\mathbb{Q}(\xi_h)/\mathbb{Q}(\chi^G), f)$, where f is the element of $H^2(N/H, H/K)$ associated to the extension*
$$1 \to H/K \overset{\chi}{\cong} \langle \xi_h \rangle \to N/K \to N/H \overset{\sigma}{\cong} Gal(\mathbb{Q}(\xi_h)/\mathbb{Q}(\chi^G)) \to 1.$$
More precisely, for every $a \in N/H$ fix a preimage u_a of $a \in N/K$. Then,
$$f(a, b) = \xi_h^j,$$
where j is such that $u_a u_b = \overline{x}^j u_{ab}$. More explicit, choose a right transversal T of H in N. Then
$$\mathbb{Q}(\xi_h) * (N/H) = \sum_{t \in T} \mathbb{Q}(\xi_h) u_t$$
The action $\alpha : N/H \to Aut(\mathbb{Q}(\xi_h))$ is defined in part (3) as follows. For $\overline{y} \in N/H$, $\alpha_{\overline{y}} = \sigma_{\overline{y}}$. The twisting $f : N/H \times N/H \to \mathcal{U}(\mathbb{Q}(\xi_h))$ is defined by $f(\overline{x}, \overline{y}) = \xi_h^j$ if $t_x t_y = x^j k_{xy} t_{xy}$ with $t_x, t_y \in T$ so that $t_x H = \overline{x}$, $t_y H = \overline{y}$, $k_{xy} \in K$ and $j \in \mathbb{Z}$.

5. *Let F be a field of characteristic zero and let $G_F = Gal(F(\chi)/F(\chi^G))$. Consider G_F as a subgroup of $G_{\mathbb{Q}}$ via the restriction $G_F \to G_{\mathbb{Q}}$. Then*

$$A_F(\chi^G) = M_{nd}(F(\xi_h)/F(\chi^G), f'),$$

where $d = \frac{[\mathbb{Q}(\xi_h):\mathbb{Q}(\chi^G)]}{[F(\xi_h):F(\chi^G)]}$ and $f'(\sigma, \tau) = f(\sigma|_{\mathbb{Q}(\xi_h)}, \tau|_{\mathbb{Q}(\xi_h)})$ (and this is the unique simple component FGe with $\chi^G(e) \neq 0$).

structure of unit group of abelian group rings, Higman page 228

4 Rational Wedderburn decomposition

Let F be a field of characteristic different from 2. Recall that an F-algebra A is said to be a quaternion algebra over F if there exists $a, b \in \mathcal{U}(F)$ such that

$$A = \left(\frac{a, b}{F}\right) = \frac{F\langle i, j\rangle}{(i^2 = a,\ j^2 = b,\ ij = -ji)} = F1 + Fi + Fj = Fk,$$

where $k = ij$. Recall the norm map $N : \left(\frac{a,b}{F}\right) \to F$, defined by $x = x_0 + x_1 i + x_2 j + x_3 k \mapsto \overline{x} = x_0 - x_1 i - x_2 j - x_3 k$, (with $x_0, x_1, x_2, x_3 \in F$). The latter defines an involution on $\left(\frac{a,b}{F}\right)$, called the quaternion conjugation.

Note that $A = \left(\frac{a,b}{F}\right)$ is a simple algebra with center F (i.e. it is a central simple F-algebra) and thus it is either a division algebra or it is isomorphic to $\mathrm{M}_2(F)$. The following conditions are equivalent:

1. $A = \mathrm{M}_2(F)$,
2. $N(x) = 0$ for some $0 \neq x \in A$,
3. $u^2 = av^2 + bw^2$ for some $0 \neq (u, v, w) \in F^3$.

Definition 4.1 *A simple finite dimensional rational algebra is said to be exceptional if it is one of the following types:*

type 1: a non-commutative division algebra other then a totally definite quaternion algebra $\left(\frac{a,b}{F}\right)$ over a number field F, that is, F is totally real and $a, b < 0$.

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 $\mathbb{Q}$.

Amitsur described the finite subgroups that are contained in an exceptional simple component of type 1. Note that, because of Dirichlet's unit theorem (see below) and a result of Kleinert, the exceptional simple components of type 2 are precisely those $\mathrm{M}_2(D)$ for which an order $\mathcal{O}$ in D has only finitely many units. Further, all finite dimensional rational non-commutative division algebras are of type 1 except those for which the unit group of an order has a central subgroup of finite index.

For a field F and a A a finite dimensional semisimple rational algebra A, we denote by $r_F(A)$ the number of of simple Wedderburn components of $F \otimes_{\mathbb{Q}} A$.

Theorem 4.2 *(Dirichlet's Unit Theorem) Let F be a number field and assume that F has r real embeddings and s pairs of complex non-real embedding. If R is the ring of integers of F then*

$$\mathcal{U}(R) = T \times A,$$

where T is a finite group formed by roots of units in F and A is a free abelian group of rank $r + s - 1$. Note that this rank equals $r_{\mathbb{R}}(F) - r_{\mathbb{Q}}(F)$ and $F \otimes_{\mathbb{Q}} \mathbb{R} \cong \mathbb{R}^r \times \mathbb{C}^s$.

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 $M_{n_i}(\mathcal{O}_i)$.

Let $\mathcal{O}$ be an order in a finite dimensional rational division algebra D. Then

$$\mathrm{SL}_n(\mathcal{O}) = \{x \in \mathrm{GL}_n(\mathcal{O}) : \mathrm{nr}(x) = 1\},$$

where nr is the reduced norm, and for subset I in $\mathcal{O}$ we put

$$E(I) = \langle I + xE_{lm} \mid x \in I,\ 1 \leq l, m \leq n_i,\ l \neq m,\ E_{lm} \text{ a matrix unit}\rangle \subseteq \mathrm{SL}_n(\mathcal{O}).$$

Theorem 4.3 (Bass-Vaseršteĭn-Liehl-Venkataramana)
Let $\mathcal{O}$ be an order in a finite dimensional rational division algebra D. Assume that n is an integer and $n \geq 2$. If the simple algebra $M_n(D)$ is not exceptional then $[\mathrm{SL}_n(\mathcal{O}) : E(I)] < \infty$ for any non-zero ideal I of $\mathcal{O}$.

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 (i.e. G embeds naturally into the simple component).

Surprisingly, if one assumes $\mathrm{M}_2(D)$ to be an exceptional component of $\mathbb{Q}G$, then the possible parameters d (resp. (a,b)) of $D = \mathbb{Q}(\sqrt{-d})$ (resp. $\left(\frac{a,b}{\mathbb{Q}}\right)$) are very limited. It was proven by Eisele, Kiefer and Van Gelder that only a finite number of division algebras can occur and, moreover, the possible parameters were described.

Theorem 4.4 *Let G be a finite group and e a primitive central idempotent of $\mathbb{Q}G$ such that $\mathbb{Q}Ge$ is exceptional. Then*

1. *If $\mathbb{Q}Ge$ is of type 2 over a field $\mathbb{Q}(\sqrt{-d})$, then $d \in \{0, -1, -2, -3\}$,*
2. *If $\mathbb{Q}Ge$ is of type 2 over a quaternion algebra $\left(\frac{a,b}{\mathbb{Q}}\right)$, then $(a,b) \in \{(-1,-1), (-1,-3), (-2,-5)\}$,*
3. *If G is cut, i.e. all central units are trivial, and $\mathbb{Q}Ge \cong M_2\left(\frac{-1,-3}{\mathbb{Q}}\right)$ or $\mathbb{Q}Ge \cong M_2(\mathbb{Q}(\sqrt{-2}))$ then there exists another primitive central idempotent e' such that $\mathbb{Q}Ge' \cong M_2(\mathbb{Q})$ or $\mathbb{Q}Ge' \cong M_2(\mathbb{Q}(i))$,*
4. *There exists a primitive central idempotent e of $\mathbb{Q}G$ such that $\mathbb{Q}Ge \cong M_2\left(\frac{-2,-5}{\mathbb{Q}}\right)$ if and only if G maps onto $G_{240,90}$,*
5. *If G is solvable and cut, then $\mathbb{Q}Ge \ncong M_2\left(\frac{-2,-5}{\mathbb{Q}}\right)$,*
6. *If G is cut, then $\mathbb{Q}Ge$ cannot be of type 1.*

Definition 4.5 *Let R be a domain. One calls R a* left Euclidean *ring if there exists a map $\delta : R \setminus \{0\} \to \mathbb{N}$ such that*

$$\forall\ a,b \in R \text{ with } b \neq 0, \exists\ q,r \in R : a = qb + r \text{ with } \delta(r) < \delta(b) \text{ or } r = 0.$$

One calls R a right Euclidean *ring if there exists a map $\delta : R \setminus \{0\} \to \mathbb{N}$ such that*

$$\forall\ a,b \in R \text{ with } b \neq 0, \exists\ q,r \in R : a = bq + r \text{ with } \delta(r) < \delta(b) \text{ or } r = 0.$$

All the fields and division algebras appearing in the previous theorem have the peculiar property to contain a Euclidean order $\mathcal{O}$ which therefore is maximal and unique up to conjugation. This yields that also all the 2×2-matrix algebras in the Thoerem have, up to conjugation, a unique maximal order, namely $\mathrm{M}_2(\mathcal{O})$. Recall that in case of $\mathbb{Q}(\sqrt{-d})$, with $d \in \{0, 1, 2, 3\}$, the unique maximal order is their respective ring of integers $\mathcal{I}_d$ and in case of $\mathbb{H}_2, \mathbb{H}_3, \mathbb{H}_5$ the respective maximal orders can easily be described. Recall that we use the following shorthands for quaternion algebras appe aring:

$$\mathbb{H}_2 = \left(\frac{-1, -1}{\mathbb{Q}}\right), \quad \mathbb{H}_3 = \left(\frac{-1, -3}{\mathbb{Q}}\right) \quad \text{and} \quad \mathbb{H}_5 = \left(\frac{-2, -5}{\mathbb{Q}}\right)$$

SmallGroupID	Structure	cut	dℓ	cℓ	exceptional components of type (II)	quotients
[6, 1]	S_3	✓	2	∞	$1\times M_2(\mathbb{Q})$	
[8, 3]	D_8	✓	2	2	$1\times M_2(\mathbb{Q})$	
[12, 4]	D_{12}	✓	2	∞	$2\times M_2(\mathbb{Q})$	[6, 1]
[16, 6]	$C_8 : C_2$	✓	2	2	$1\times M_2(\mathbb{Q}(i))$	
[16, 8]	$QD16$	✓	2	3	$1\times M_2(\mathbb{Q})$, $1\times M_2(\mathbb{Q}(\sqrt{-2}))$	[8, 3]
[16, 13]	$(C_4 \times C_2) : C_2$	✓	2	2	$1\times M_2(\mathbb{Q}(i))$	
[18, 3]	$C_3 \times S_3$	✓	2	∞	$1\times M_2(\mathbb{Q})$, $1\times M_2(\mathbb{Q}(\sqrt{-3}))$	[6, 1]
[24, 1]	$C_3 : C_8$	×	2	∞	$1\times M_2(\mathbb{Q})$, $1\times M_2(\mathbb{Q}(i))$	[6, 1]
[24, 3]	$\mathrm{SL}(2,3)$	✓	3	∞	$1\times M_2(\mathbb{Q}(\sqrt{-3}))$	
[24, 5]	$C_4 \times S_3$	✓	2	∞	$2\times M_2(\mathbb{Q})$, $1\times M_2(\mathbb{Q}(i))$	[6, 1], [12, 4]
[24, 8]	$(C_6 \times C_2) : C_2$	✓	2	∞	$3\times M_2(\mathbb{Q})$, $1\times M_2(\mathbb{Q}(\sqrt{-3}))$	[6, 1], [8, 3], [12, 4]
[24, 10]	$C_3 \times D_8$	✓	2	2	$1\times M_2(\mathbb{Q})$, $1\times M_2(\mathbb{Q}(\sqrt{-3}))$	[8, 3]
[24, 11]	$C_3 \times Q_8$	✓	2	2	$1\times M_2(\mathbb{Q}(\sqrt{-3}))$	
[32, 8]	$(C_2 \times C_2).(C_4 \times C_2)$	✓	2	3	$2\times M_2(\mathbb{Q})$, $1\times M_2(\mathbb{H}_2)$	[8, 3]
[32, 11]	$(C_4 \times C_4) : C_2$	✓	2	3	$2\times M_2(\mathbb{Q})$, $2\times M_2(\mathbb{Q}(i))$	[8, 3]
[32, 44]	$(C_2 \times Q_8) : C_2$	✓	2	3	$2\times M_2(\mathbb{Q})$	[8, 3]
[32, 50]	$(C_2 \times Q_8) : C_2$	✓	2	2	$1\times M_2(\mathbb{H}_2)$	
[36, 6]	$C_3 \times (C_3 : C_4)$	×	2	∞	$1\times M_2(\mathbb{Q})$, $2\times M_2(\mathbb{Q}(\sqrt{-3}))$	[6, 1], [18, 3]
[36, 12]	$C_6 \times S_3$	✓	2	∞	$2\times M_2(\mathbb{Q})$, $2\times M_2(\mathbb{Q}(\sqrt{-3}))$	[6, 1], [12, 4], [18, 3]
[40, 3]	$C_5 : C_8$	×	2	∞	$1\times M_2(\mathbb{H}_5)$	
[48, 16]	$(C_3 : Q_8) : C_2$	✓	2	∞	$3\times M_2(\mathbb{Q})$, $1\times M_2(\mathbb{Q}(\sqrt{-2}))$, $1\times M_2(\mathbb{Q}(\sqrt{-3}))$, $1\times M_2(\mathbb{H}_2)$	[6, 1], [8, 3], [12, 4], [16, 8], [24, 8]
[48, 18]	$C_3 : Q_{16}$	×	2	∞	$3\times M_2(\mathbb{Q})$, $1\times M_2(\mathbb{Q}(\sqrt{-3}))$, $1\times M_2(\mathbb{H}_3)$	[6, 1], [8, 3], [12, 4], [24, 8]
[48, 28]	$\mathrm{SL}(2,3).C_2$	×	4	∞	$1\times M_2(\mathbb{Q})$, $1\times M_2(\mathbb{H}_3)$	[6, 1]
[48, 29]	$\mathrm{GL}(2,3)$	✓	4	∞	$1\times M_2(\mathbb{Q})$, $1\times M_2(\mathbb{Q}(\sqrt{-2}))$	[6, 1]
[48, 33]	$((C_4 \times C_2) : C_2) : C_3$	×	3	∞	$1\times M_2(\mathbb{Q}(i))$	
[48, 39]	$(C_4 \times S_3) : C_2$	✓	2	∞	$4\times M_2(\mathbb{Q})$, $1\times M_2(\mathbb{Q}(i))$, $1\times M_2(\mathbb{H}_3)$	[6, 1], [12, 4], [16, 13]
[48, 40]	$Q_8 \times S_3$	✓	2	∞	$4\times M_2(\mathbb{Q})$, $1\times M_2(\mathbb{H}_2)$	[6, 1], [12, 4]
[64, 37]	$(C_4 \times C_2).(C_4 \times C_2)$	✓	2	4	$2\times M_2(\mathbb{Q})$, $2\times M_2(\mathbb{H}_2)$	[8, 3]
[64, 137]	$(C_4 : Q_8) : C_2$	✓	2	3	$6\times M_2(\mathbb{Q})$, $2\times M_2(\mathbb{H}_2)$	[8, 3]
[72, 19]	$(C_3 \times C_3) : C_8$	×	2	∞	$2\times M_2(\mathbb{H}_3)$	
[72, 20]	$(C_3 : C_4) \times S_3$	✓	2	∞	$4\times M_2(\mathbb{Q})$, $1\times M_2(\mathbb{Q}(i))$, $1\times M_2(\mathbb{H}_3)$	[6, 1], [12, 4], [24, 5]
[72, 22]	$(C_6 \times S_3) : C_2$	✓	2	∞	$5\times M_2(\mathbb{Q})$, $2\times M_2(\mathbb{Q}(\sqrt{-3}))$, $1\times M_2(\mathbb{H}_3)$	[6, 1], [8, 3], [12, 4], [24, 8]
[72, 24]	$(C_3 \times C_3) : Q_8$	×	2	∞	$4\times M_2(\mathbb{Q})$, $1\times M_2(\mathbb{H}_3)$	[6, 1], [12, 4]
[72, 25]	$C_3 \times \mathrm{SL}(2,3)$	✓	3	∞	$4\times M_2(\mathbb{Q}(\sqrt{-3}))$	[24, 3]
[72, 30]	$C_3 \times ((C_6 \times C_2) : C_2)$	✓	2	∞	$3\times M_2(\mathbb{Q})$, $6\times M_2(\mathbb{Q}(\sqrt{-3}))$	[6, 1], [8, 3], [12, 4], [18, 3], [24, 8], [24, 10], [36, 12]
[96, 67]	$\mathrm{SL}(2,3) : C_4$	✓	4	∞	$1\times M_2(\mathbb{Q})$, $2\times M_2(\mathbb{Q}(i))$	[6, 1]
[96, 190]	$(C_2 \times \mathrm{SL}(2,3)) : C_2$	✓	4	∞	$2\times M_2(\mathbb{Q})$	[6, 1], [12, 4]
[96, 191]	$\mathrm{SL}(2,3).C_2) : C_2$	×	4	∞	$2\times M_2(\mathbb{Q})$	[6, 1], [12, 4]
[96, 202]	$((C_2 \times Q_8) : C_2) : C_3$	✓	3	∞	$1\times M_2(\mathbb{H}_2)$	
[120, 5]	$\mathrm{SL}(2,5)$	×	∞		$1\times M_2(\mathbb{H}_3)$	
[128, 937]	$(Q_8 \times Q_8) : C_2$	✓	3	4	$6\times M_2(\mathbb{Q})$, $4\times M_2(\mathbb{H}_2)$	[8, 3]
[144, 124]	$\mathrm{SL}(2,3).C_2)$	×	4	∞	$4\times M_2(\mathbb{Q})$, $4\times M_2(\mathbb{H}_3)$	[6, 1], [48, 28]
[144, 128]	$S_3 \times \mathrm{SL}(2,3)$	✓	3	∞	$1\times M_2(\mathbb{Q})$, $3\times M_2(\mathbb{Q}(\sqrt{-3}))$, $1\times M_2(\mathbb{H}_2)$	[6, 1], [18, 3], [24, 3]
[144, 135]	$(C_3 \times C_3) : (C_8 : C_2)$	✓	2	∞	$1\times M_2(\mathbb{Q}(i))$, $4\times M_2(\mathbb{H}_3)$	[16, 6]
[144, 148]	$(C_3 \times C_3) : ((C_4 \times C_2) : C_2)$	✓	2	∞	$8\times M_2(\mathbb{Q})$, $1\times M_2(\mathbb{Q}(i))$, $4\times M_2(\mathbb{H}_3)$	[6, 1], [12, 4], [16, 13], [48, 39]
[160, 199]	$((C_2 \times Q_8) : C_2) : C_5$	×	3	∞	$1\times M_2(\mathbb{H}_2)$	
[192, 989]	$(\mathrm{SL}(2,3) : C_4) : C_2$	✓	4	∞	$3\times M_2(\mathbb{Q})$, $1\times M_2(\mathbb{Q}(\sqrt{-3}))$, $2\times M_2(\mathbb{H}_2)$	[6, 1], [8, 3], [12, 4], [24, 8]
[240, 89]	$\mathrm{SL}(2,5).C_2$	×	∞		$1\times M_2(\mathbb{H}_5)$	
[240, 90]	$\mathrm{SL}(2,5) : C_2$	✓	∞		$1\times M_2(\mathbb{H}_5)$	
[288, 389]	$(C_3 \times C_3) : ((C_4 \times C_4) : C_2)$	✓	3	∞	$2\times M_2(\mathbb{Q})$, $2\times M_2(\mathbb{Q}(i))$, $2\times M_2(\mathbb{H}_3)$	[8, 3], [32, 11]
[320, 1581]	$(((C_2 \times Q_8) : C_2) : C_5).C_2$	×	4	∞	$2\times M_2(\mathbb{H}_2)$	
[384, 618]	$((Q_8 \times Q_8) : C_2) : C_3$	✓	3	∞	$1\times M_2(\mathbb{H}_2)$	
[384, 18130]	$((Q_8 \times Q_8) : C_3) : C_2$	✓	4	∞	$1\times M_2(\mathbb{Q})$, $1\times M_2(\mathbb{H}_2)$	[6, 1]
[720, 409]	$\mathrm{SL}(2,9)$	×	∞		$2\times M_2(\mathbb{H}_3)$	
[1152, 155468]	$(((Q_8 \times Q_8) : C_3) : C_2) : C_3$	✓	4	∞	$1\times M_2(\mathbb{Q})$, $1\times M_2(\mathbb{Q}(\sqrt{-3}))$, $1\times M_2(\mathbb{H}_2)$	[6, 1], [18, 3]
[1920, 241003]	$C_2.((C_2 \times C_2 \times C_2 \times C_2) : A_5)$	×	∞		$1\times M_2(\mathbb{H}_2)$	

5 Generators for a subgroup of finite index

Let G be a finite group. We know that $\mathbb{Z}G$ is an order in $\mathbb{Q}G$ and that $\mathbb{Z}G$ only has trivial idempotents.

Indeed,

Lemma 5.1 *Let K be a field extension of $\mathbb{Q}$ and let $e = \sum_{g \in G} e_g g \in KG$, with each $e_g \in K$. If $e^2 = e \notin \{0, 1\}$ then e_1 is a rational number in the interval $(0, 1)$.*

Proof. This will be proven in the lectures on torsion units. ∎

Now if $e_1, \dots, e_n$ are the primitive central idempotents of $\mathbb{Q}G$ then also $\sum_{i=1}^{n} \mathbb{Z}Ge_i$ is an order in $\mathbb{Q}G$ that contains $\mathbb{Z}G$. Their unit groups, however, do not differ a lot in size. Indeed we have the following properties.

Lemma 5.2 *Let A be a semisimple finite dimensional rational algebra. Let $e_1, \dots, e_n$ be the primitive central idempotents of A.*

1. *Every element of an order $\mathcal{O}$ in A is integral over $\mathbb{Z}$.*
2. *The intersection of two orders of A is again an order in A.*
3. *Every order of A is contained in a maximal order of A, say $\mathcal{M}$. Furthermore, $\mathcal{M} = \sum_{i=1}^{n} \mathcal{M}e_i$ and each $\mathcal{M}e_i$ is a maximal order in Ae_i.*
4. *Suppose $\mathcal{O}_1 \subseteq \mathcal{O}_2$ are two orders in A. Then*
   - *(a) $u \in \mathcal{O}_1$ is invertible in $\mathcal{O}_2$ if $u^{-1} \in \mathcal{O}_2$.*
   - *(b) the index of the unit groups $(\mathcal{U}(\mathcal{O}_2) : \mathcal{U}(\mathcal{O}_1))$ is finite.*

Proof. We only prove part (4).

(a) Let $u \in \mathcal{O}_1$ and assume $u^{-1} \in \mathcal{O}_2$. Using indices of additive subgroups, we get $[\mathcal{O}_2 : u\mathcal{O}_1] = [u\mathcal{O}_2 : u\mathcal{O}_1] \leq [\mathcal{O}_2 : \mathcal{O}_1]$. Hence, $u\mathcal{O}_2 = \mathcal{O}_1$ and thus u is invertible in $\mathcal{O}_1$. The converse is obvious.

(b) Since $\mathcal{O}_2$ is a free $\mathbb{Z}$-module containing $\mathcal{O}_1$, they both have equal $\mathbb{Z}$-rank, say n. Thus the index of the addtive groups satisfies $[\mathcal{O}_2 : \mathcal{O}_1] = m < \infty$. Hence, $m\mathcal{O}_2 \subseteq \mathcal{O}_1$. Suppose now that $u, v \in \mathcal{U}(\mathcal{O}_2)$ such that $u + m\mathcal{O}_2 = v + m\mathcal{O}_2$. Then $u^{-1}v - 1 \in m\mathcal{O}_2 \subseteq \mathcal{O}_1$ and thus $u^{-1}v \in \mathcal{O}_1$. Similarly, $v^{-1}u \in \mathcal{O}_1$. So, $u^{-1}v \in \mathcal{U}(\mathcal{O}_1)$. Hence, we have shown that $(\mathcal{U}(\mathcal{O}_2) : \mathcal{U}(\mathcal{O}_1) \subseteq [\mathcal{O}_2 : m\mathcal{O}_2] < \infty$. ∎

Hence, to compute a subgroup of finite index in $\mathcal{U}(\mathbb{Z}G)$ it is sufficient to construct for each primitive central idempotent e_i of $\mathbb{Q}G$ units of $\mathcal{U}(\mathbb{Z}G)$, that belong to $\mathbb{Z}Ge_i$, and that generate a subgroup of finite index in $\mathcal{U}(\mathbb{Z}Ge_i)$. The next proposition shows that for the latter we have to describe units that contribute to a large subgroup of the center of $\mathcal{U}(\mathbb{Z}Ge_i)$ and to a large subgroup of the units of reduced norm one in $\mathbb{Z}Ge_i$.

Proposition 5.3 *Let $\mathcal{O}$ be an order in a simple finite dimensional rational algebra A. Then $\mathrm{GL}_n(\mathcal{O})$ contains a subgroup of finite which is isomorphic to a subgroup of finite index in $\mathrm{SL}_n(\mathcal{O}) \times \mathcal{U}(R)$, where R is the unique maximal order in the center of A.*

Let us now focus on the units of reduced norm one. For this a crucial and well known lemma is the following.

Lemma 5.4 *Let D be a finite dimensional rational division algebra and let n be an integer with $n > 1$. If f is a non-central idempotent in $M_n(D)$ then there exist matrix units $E_{i,j}$, with $1 \leq i, j \leq n$ (that is, $\sum_{i=1}^{n} E_{i,i} = 1$ and $E_{i,j}E_{k,l} = \delta_{j,k}E_{i,l}$) such that*

$$f = E_{1,1} + \cdots + E_{l.l},$$

with $0 < l < n$. Moreover, $M_n(D) = M_n(D')$, with D' the centraliser of all $E_{i,j}$.

One can then prove the following result.

Let A be a semisimple finite dimensional rational algebra such that AG is semisimple. Let R be an order in A and let $x_1, \ldots, x_m$ be a generating set of of R as an $\mathbb{Z}$-module. For a given set of idempotents $\mathcal{F}$ of AG we put

$$\mathrm{GBic}^{\mathcal{F}}(RG) = \langle b(x_i g, f),\ b(f, x_i g) \mid f \in \mathcal{F},\ g \in G,\ 1 \leq i \leq m \rangle.$$

If $R = \mathbb{Z}$ then we simply put

$$\mathrm{GBic}^{\mathcal{F}}(G).$$

If, furthermore, $\mathcal{F} = \{\widehat{g} \mid g \in G\}$ then we put

$$\mathrm{Bic}(G)$$

for this group.

Theorem 5.5 *(Jespers-Leal) Let G be a finite group and R an order in a semisimple finite dimensional algebra A. Assume AG is semisimple, e is a primitive central idempotent of AG and $\mathcal{O}$ is an order in AGe. Assume the simple component AGe is not exceptional. If f is an idempotent of AG such that ef is non-central (in AGe) then $GBic^{\{e\}}(RG)$ contains a subgroup of finite index in the reduced norm one elements of $1-e+\mathcal{O}$.*

Proof. Let n_f be the minimal positive integer such that $n_f f \in RG$. Let $x_1, \ldots, x_m$ be a generating set of R as a $\mathbb{Z}$-module. As $AGe = M_n(D)$, for some division algebra D, by Lemma 5.4 there is a set of matrix units $\{E_{i,j} : 1 \leq i,j \leq n\}$ of AGe with $f = E_{1,1} + \cdots + E_{l,l}$ for some $0 < l < n$. Recall from Lemma 5.2 that the unit groups of two orders in AGe are commensurable. Hence, without loss of generality, we may assume that $M_n(\mathcal{O})$ is the order chosen in the statement, with $\mathcal{O}$ an order in D. Let $J = \mathrm{GBic}^{\{f\}}(RG)$. Note that

$$\left[1 + n_f^2 f x_i g(1-f)\right]^k \left[1 + n_f^2 f x_j h(1-f)\right]^l = \left[1 + n_f^2 f(kx_i g + lx_j h)(1-f)\right],$$

for every $k, l \in \mathbb{Z}$, $g, h \in G$ and $1 \leq i, j \leq m$. So, the group generated by these units contains all elements of the form

$$1 + n_f^2 f\alpha(1-f), \quad \text{and} \quad 1 + n_f^2(1-f)\alpha f,$$

with $\alpha \in RG$.

Since

$$\left\{1 + n_f^2 f\alpha(1-f),\ 1 + n_f^2(1-f)\alpha f : \alpha \in RG\right\} \subseteq J,$$

it follows that

$$\left\{1 + n_e n_f^2 f\alpha(1-f)e,\ 1 + n_e n_f^2(1-f)\alpha f e : \alpha \in RG\right\} \subseteq J.$$

Let $i \leq l$ and $l+1 \geq j \geq n$. Then,

$$f\mathcal{O}E_{i,j}(1-f)e = \mathcal{O}E_{i,j}.$$

Hence, as $\mathcal{O}$ is a finitely generated $\mathbb{Z}$-module, there exists a positive integer $n_{i,j}$ such that

$$1 + n_{i,j}\mathcal{O}E_{i,j} \subseteq J \cap \mathrm{SL}_n(\mathcal{O}).$$

And similarly,

$$1 + n_{j,i}\mathcal{O}E_{j,i} \subseteq J \cap \mathrm{SL}_n(\mathcal{O}),$$

for some positive integer $n_{j,i}$.

So we have shown the existence of a positive integer x with

$$1 + x\mathcal{O}E_{i,j} \subseteq J \cap \mathrm{SL}_n(\mathcal{O}) \quad \text{and} \quad 1 + x\mathcal{O}E_{j,i} \subseteq J \cap \mathrm{SL}_n(\mathcal{O}),$$

for all $1 \leq i \leq l$ and $l+1 \leq j \leq n$.

Now let $1 \leq i, j \leq l$, $i \neq j$ and $\alpha \in \mathcal{O}$. Then one easily verifies that

$$1 + x^2\alpha E_{i,j} = (1 + x\alpha E_{i,l+1},\ 1 + xE_{l+1,j}) \in J \cap \mathrm{SL}_n(\mathcal{O}).$$

Similarly, for $l+1 \leq i, j \leq n_i$, $i \neq j$, it follows that

$$1 + x^2\mathcal{O}E_{i,j} \subseteq J \cap \mathrm{SL}_n(\mathcal{O}).$$

Because of the assumptions, the result now follows from Theorem 4.3. ▮

The next step is to construct in a simple component $\mathbb{Q}Ge$ a non-central idempotent. This can be done if Ge is not fixed point free and one can show that this can be done with an idempotent of the type $\widehat{g}e$. Recall that a finite group is said to be *fixed point free* if it has an (irreducible) complex representation ρ such that 1 is not an eigenvalue of $\rho(g)$ for all $1 \neq g \in G$. Such groups show up naturally, as every non-trivial finite subgroup of a division algebra is fixed point free.

Indeed, Let e be a primitive central idempotent of $\mathbb{Q}(\xi)G$ with Ge not commutative and Ge not fixed point free. Thus, there exists a primitive central idempotent e_1 of $\mathbb{C}Ge$ such that the non-linear complex representation $\rho : G \to (\mathbb{C}G)e_1$ mapping x onto xe_1 has eigenvalue 1 for some $\rho(g)$, with $g \in G$ and $ge_1 \neq e_1$. Since $\rho(g)$ is diagonalizable one may assume that

$$\rho(g) = \begin{pmatrix} I_j & 0 \\ 0 & D \end{pmatrix} \text{ with } 1 \leq j < n \text{ and } D = \mathrm{diag}(\xi_{j+1}, \ldots, \xi_n)$$

and $\xi_{j+1}, \ldots, \xi_n$ are roots of unity different from 1. Consequently

$$\rho(\widehat{g}) = \begin{pmatrix} I_j & 0 \\ 0 & 0 \end{pmatrix}.$$

Hence $\widehat{g}e_1$ is a non-central idempotent of $\mathbb{C}G$. It follows that $\widehat{g}e$ is a non-zero idempotent in $\mathbb{Q}(\xi)Ge$. Furthermore $\widehat{g}e \neq e$, because otherwise $\widehat{g}e_1 = \widehat{g}e_1e = e_1e = e_1$, a contradiction.

Now it remains to find units that cover the center of $\mathcal{U}(\mathbb{Z}G)$. This is done via a beautiful result of Bass-Milnor. It says that the units of $Z(R)C$, where C runs through the cyclic subgroups of G, give a subgroup of finite index in $K_1(RG)$. Now another beautiful result of Bass-Milnor says that the Bass units $u_{k,m}(\xi^i g)$ generate a subgroup of finite index in $\mathcal{U}(\mathbb{Z}[\xi]\langle g\rangle)$. One knows even specific Bass units that are a basis of free abelian subgroup of finite index..

All the above mentioned results then give the following result.

Theorem 5.6 *Let G be a finite group and ξ a root of unity. Suppose that $\mathbb{Q}(\xi)G$ does not have exceptional simple components. Let $\mathcal{C} = \{\widehat{g} \mid g \in G\}$. Suppose that for every primitive central idempotent e of $\mathbb{Q}G$ the group Ge is not fixed point free. Then*

$$\langle GBic^{\mathcal{C}}(\mathbb{Z}[\xi]G) \cup Bass\ (\mathbb{Z}[\xi]G)\rangle$$

is of finite index in $\mathcal{U}(\mathbb{Z}[\xi]G)$.

The result also implies that the unit group is finitely generated. One has a much stronger result due to Siegel.

Theorem 5.7 *Let $\mathcal{O}$ be an order in a finite dimensional semisimple rational algebra A. Then $\mathcal{U}(\mathcal{O})$ is finitely presented.*

We give some examples of finite 2-groups G such that the Bass units together with the bicyclic units do not generate a subgroup of finite index in $\mathcal{U}(\mathbb{Z}G)$. The following result is due to Jespers and Parmenter.

Theorem 5.8 *Let $D_8 = \langle a, b \mid a^4 = 1,\ b^2 = 1,\ ba = a^3 b\rangle$, the quaternion group of order 8. Let G be a finite 2-group and suppose there exists an epimorphism $f : G \to D_8$. If at least two of the elements b, ab, a^2b, a^3b do note have preimages in G of order 2, then the Bass units together with the bicyclic units in $\mathbb{Z}G$ do not generate a subgroup of finite index in $\mathcal{U}(\mathbb{Z}G)$.*

In particular, this applies to the groups Q_{16}, $\langle a, b \mod a^8 = 1,\ b^2 = 1, ba = a^3 b\rangle$, $C_4 \rtimes C_2$ and $(\langle z\rangle_2 \times \langle a\rangle_4) \rtimes \langle b\rangle_2$, with z central and $a^b = za$.

Proof. The $\mathbb{Z}$-linear extension of f to a ring epimorphism $\mathbb{Z}G \to \mathbb{Z}D_8$, as well as the induced group homomorphism $\mathcal{U}(\mathbb{Z}G) \to \mathcal{U}(\mathbb{Z}D_8)$, we also denote by f.

Since every Bass unit of $\mathbb{Z}D_8$ belongs to D_8, every Bass unit in $\mathbb{Z}G$ must map to an element of D_8.

Next consider a bicyclic unit $b(g, \widetilde{h})$ in $\mathbb{Z}G$. Then either $f(b(g, \widetilde{h})) = 1$ or

$$f(b(g, \widetilde{h})) = 1 + c(1 - f(g))f(h)\widetilde{f(g)} = (1 + (1 - f(g))f(h)\widetilde{f(g)})^c,$$

where $c = \frac{o(g)}{o(f(g))}$.

The bicyclic units of $\mathbb{Z}D_8$ are $u_1 = b(a, \widetilde{b})$, $u_2 = b(a, \widetilde{ab})$, $u_3 = b(a, \widetilde{a^2b})$ and $u_4 = b(a, \widetilde{a^3b})$. Further $u_4 = u_3^{-1}u_2^{-1}u_1^{-1}$. It is easily verified that the given condition on G yields that at least two of these bicyclic units are not images of bicyclic units in $\mathbb{Z}G$.

It is known that

$$V = \mathcal{U}(\mathbb{Z}D_8) \cap (1 + \mathrm{Ker}(\mathrm{aug})(1 - a^2)) = \mathcal{U}(\mathbb{Z}D_8) \cap (1 + \mathrm{Ker}(\mathrm{aug})(1 - a))$$

is a normal complement of the trivial units $\pm D_8$ and it is a free group of rank three, generated by the bicyclic units of the type $b(g, \widetilde{h})$. Let B be the subgroup of $\mathcal{U}(\mathbb{Z}G)$ generated by the Bass units and the bicyclic units of the type $b(g, \widetilde{h})$. Since G is a 2-group, it follows from the remarks above that $f(B)$ is a proper subgroup of V requiring at most 4 generators. Since V is a free group of rank 3, we conclude that $f(B)$ must be of infinite index in V. Indeed, by the Nielsen-Schreier, if $f(B)$ has index n in V then $f(B)$ is free of rank $2n + 1$. As $f(B)$ is generated by at most 4 elements, necessarily $n = 1$ and hence $f(B) = V$, a contradiction.

For a positive integer i, let V_i denote the subgroup of V consisting of those units which can be written in the form $1 + 2^i\beta(1 - a^2)$ for some $\beta \in \mathbb{Z}D_8$. Because $(1 - a^2)^2 = 2(1 - a^2)$, it follows that each $V_i \subseteq V$. Also note that for all i, V_i is a normal subgroup of V and that the groups V/V_1 and V_i/V_{i+1} are of exponent 2 and thus abelian. Since $\mathcal{U}(\mathbb{Z}D_8)$ is finitely generated, so is the group V. Consequently, V/V_1 and all V_i/V_{i+1} are finite. So, each V/V_i is finite.

Let $K = \mathrm{Ker}(f)$. Obviously, $|K| = 2^l$ for some $l \geq 1$. We claim that $V_l \subseteq f(\mathcal{U}(\mathbb{Z}G))$. Indeed, let $1 + 2^l\beta(1 - a^2) \in V_l$. Choose $a_1, \beta_1 \in \mathbb{Z}G$ such that $f(a_1) = a$ and $f(\beta_1) = \beta$. Put $u = 1 + \widetilde{K}\beta_1(1 - a_1^2)$. Clearly $u\widehat{K} = \widehat{K}(1 + 2^l\beta_1(1 - a_1^2))$ is a unit in $\mathbb{Z}G\widehat{K} \cong \mathbb{Z}D_8$. Since $u(1 - \widehat{K}) = 1 - \widehat{K}$ is a unit in $\mathbb{Z}G(1 - \widehat{K})$, we get that $u \in \mathbb{Z}G$ is a unit in the order $\mathbb{Z}G\widehat{K} \oplus \mathbb{Z}G(1 - \widehat{K})$. Hence, because of Lemma 5.2, $u \in \mathcal{U}(\mathbb{Z}G)$. Obviously, $f(u) = 1 + 2^l\beta(1 - a^2)$. So, $u \in f(\mathcal{U}(\mathbb{Z}G))$ and the claim has been proved.

Suppose that $f(B)$ is of finite index in $f(\mathcal{U}(\mathbb{Z}G))$. Since $f(B) \subseteq V$, this yields $f(B)$ is of finite index in $f(\mathcal{U}(\mathbb{Z}G)) \cap V$. Because $V_l \subseteq f(\mathcal{U}(\mathbb{Z}G))V$ and V_l is of finite index in V, it follows that $f(B)$ is of finite index V. However this contradicts the earlier fact that $f(B)$ is of infinite index in V. Therefore, we have shown that $f(B)$ is of infinite index in $f(\mathcal{U}(\mathbb{Z}G))$.

To finish the proof we note that if $f(b(g, \widetilde{h})) \neq 1$ then it is a power of a bicyclic unit $b(\widetilde{f(h)}, f(g)) = 1 + (1 + f(h))f(g)(1 - f(h))$. Since $b(\widetilde{f(h)}, f(g)) = b(f(g), \widetilde{a^2f(h)})$, we obtain that $f(\mathrm{Bix}(G)) = f\left(\langle b(g, \widetilde{h}) \mid g, h \in G\rangle\rangle\right)$. So, from the previous, $f\left(\langle \mathrm{Bix}(G)\cup \mathrm{Bass}(G)\rangle\right)$ is of infinite index in $f(\mathcal{U}(\mathbb{Z}G))$ and thus $\langle \mathrm{Bix}(G)\cup \mathrm{Bass}(G)\rangle$ is of infinite index in $\mathcal{U}(\mathbb{Z}G)$. ▮

6 Constructions of central units from Bass units

The rank of the central units also can be determined.

Theorem 6.1 *Let A be a finite dimensional semisimple rational algebra and $\mathcal{O}$ an order in A. Then*

$$\mathcal{U}(Z(\mathcal{O})) = T \times F,$$

where T is a finite group and F is a free abelian group of rank $r_{\mathbb{R}}(A) - r_{\mathbb{Q}}(A)$.

If G is a finite group then for any finite field extension F of $\mathbb{Q}$, $r_F(FG)$ is the number of irreducible F-characters of G and it also equals the number of Wedderburn components of FG.

Hence

$$Z(\mathcal{U}(\mathbb{Z}G)) = \pm Z(G) \times F,$$

where F is a free abelian group of rank $r_{\mathbb{R}}(\mathbb{R}G) - r_{\mathbb{Q}}(\mathbb{Q}G)$.

In particular, if G is a finite abelian group of order n. Then F has rank

$$\frac{n+1+k_2-2c}{2} = \sum_{d|n,\, d>2} k_d\left(\frac{\varphi(d)}{2}-1\right),$$

where c is the number of cyclic subgroups of G and k_d is the number of cyclic subgroups of G of order d.

A result of Artin says that if G is a finite group then $r_{\mathbb{Q}}(\mathbb{Q}G)$, the number of irreducible $\mathbb{Q}$-characters of G, equals the number of conjugacy classes of cyclic subgroups of G.

As a consequence one obtains the following formula for the rank of the central units in a group ring.

Corollary 6.2 *Let G be a finite group. Then, the rank of $\mathbb{Z}(\mathcal{U}(\mathbb{Z}G))$ is*

$$\frac{c+c'}{2} - d,$$

where c' is the number of conjugacy classes of G closed under taking inverses and d is the number of conjugacy classes of cyclic subgroups of G

Ritter and Sehgal determined necessary and sufficient conditions for all central units to be trivial. A proof relies on the following lemma.

The following notation is used. Let G be a finite group and K a field. One says that two elements g and h of G are *K-conjugate* in G if there exists $r \in \mathcal{U}_K(n) = \{r \in \mathbb{Z}_n \mid \sigma(\xi_n) = \xi_n^r, \text{ for some } \sigma \in \text{ Gal}(K(\xi_n)/K)\}$ (ξ_n a primitive n-th root of unity in an extension of K) such that g and h^r are conjugate in G; where n is the exponent of G. This defines an equivalence relation $\sim_K$ in G. The equivalence class containing $g \in G$ is called the *K-conjugacy class* of g in G and it is denoted g_K^G. The conjugacy class of g in G is simply denoted g^G. Hence,

$$g_K^G = \cup_{r \in \mathcal{U}_K(n)} (g^r)^G.$$

Note that if K contains a primitive n-th root of unity, then $g_K^G = g^G$. Further note that $g \sim_{\mathbb{Q}} h$ if and only if g is conjugate of h^r in G for some r coprime with n; equivalently $\langle g \rangle$ is a conjugate of $\langle h \rangle$ in G. One can also easily verify that $g \sim_{\mathbb{R}} h$ if and only if g is a conjugate of h or h^-1, that is $g_{\mathbb{R}}^G = g^G \cup (g^{-1})^G$.

Lemma 6.3 *Let G be a finite group of exponent n and let $g \in G$. Then $g_{\mathbb{Q}}^G = g_{\mathbb{R}}^G$ if and only if g is conjugate to g^m or g^{-m} for every integer m with $(m, n) = 1$.*

Corollary 6.4 *For a finite group the following properties are equivalent.*

1. *$Z(\mathcal{U}(\mathbb{Z}G))$ is finite, i.e. all central units are trivial.*
2. *For every $g \in G$ and every integer m with $(m, |G|) = 1$ the elements g^m and g^{-m} are conjugate.*

Also for strongly monomial groups one can determine a formula for the rank of the central units and, with some restriction, one can determine an independent set of central units that generates a subgroup of finite index.

We have seen that for many finite groups the group generated by the Bass units and the bicyclic units generate a subgroup of finite index in $\mathcal{U}(\mathbb{Z}G)$. In particular, the subgroup contains a subgroup of finite index in the center $Z(\mathcal{U}(\mathbb{Z}G))$. As the bicyclic units contain a subgroup of finite index in reduced norm one subgroups of orders in the simple components, one might be tempted to think that the Bass units contain a subgroup of finite index in the center of $\mathcal{U}(\mathbb{Z}G)$. Note, however, that Bass units in general are not central elements.

Jespers, Parmenter and Sehgal showed that for finite nilpotent groups the group generated by the Bass units contains a subgroup of finite index in the unit group of the center. To do so, one needs, in first instance, a method to construct from a Bass unit a central unit. Jespers, Olteanu, Van Gelder and del Río proved that this also can be done for the class of abelian-by-supersolvable groups G such that every cyclic subgroup of order not a divisor of 4 or 6 is subnormal in G. Obviously, dihedral groups are examples of such groups. Also nilpotent finite groups N are examples. Indeed, let $Z_= Z_i(N)$ denote the i-th center of N, i.e $Z_0 = \{1\}$ and $Z_i/Z_{i-1} = Z(G/Z_{i-1})$ for $i \geq 1$. Then, for $x \in N$, the series $\langle x \rangle \lhd \langle Z_1, x\rangle \lhd \cdots \lhd \langle Z_n, x\rangle = N$ (for some integer n) is a subnormal series in N.

So, suppose G is an finite abelian-by-supersolvable group such that every cyclic subgroup of order not a divisor of 4 or 6 is subnormal in G. Let $g \in G$ be of order not a divisor or 4 or 6 and let

$$\mathcal{N} : N_= \langle g \rangle \lhd N_1 \lhd N_2 \lhd \cdots \lhd N_m = G$$

be a subnormal series in G. For $u \in \mathcal{U}(\mathbb{Z}\langle g \rangle)$ put

$$c_o^{\mathcal{N}}(u) = u$$

and

$$c_i^{\mathcal{N}}(u) = \prod_{h \in T_i} c_{i-1}^{\mathcal{N}}(u)^h,$$

where T_i is a transversal for N_{i-1} in N_i, $i \geq 1$. That this construction is well defined follows from the following lemma.

Lemma 6.5 *With notation as above.*

1. $c_{i-1}^{\mathcal{N}}(u)^x \in \mathbb{Z}N_{i-1}$ *for* $x \in N_i$,

2. $c_{i-1}^{\mathcal{N}}(u)^x = c_{i-1}^{\mathcal{N}}(u)$ *for* $x \in N_{i-1}$,

3. $c_i^{\mathcal{N}}(u)$ *is independent of the chosen transversal* T_i.

In particular, $c_m^{\mathcal{N}}(u) \in Z(\mathcal{U}(\mathbb{Z}G))$.

Because the class of abelian-by-supersolvable groups is is closed under taking subgroups (a property that does not hold for the larger class of consisting of strongly monomial groups) one can prove the following result.

Theorem 6.6 *Let G be a finite abelian-by-supersolvable group such that every cyclic subgroup of order not a divisor of* 4 *or* 6 *is subnormal in G. Let $g \in G$ be of order not a divisor or* 4 *or* 6*. Then, the group generated by the Bass units of $\mathbb{Z}G$ contain a subgroup of finite index in $Z(\mathbb{Z}(\mathcal{U}(\mathbb{Z}G)))$.*

Acrtually, for each subgroup $\langle g\rangle$, of order not dividing 4 or 6, fix a subnormal series $\mathcal{N}_g$ from $\langle g\rangle$ to G. Then

$$\langle c^{\mathcal{N}_g}(b_g) \mid b_g \text{ a Bass unit based on } g,\ g \in G\rangle,$$

is of finite index in $Z(\mathcal{U}(\mathbb{Z}G))$.

7 Structure theorems of unit groups

The exceptional simple components are an obstruction for the construction of finitely many generators for a subgroup of finite index in the unit group of $\mathbb{Z}G$ for a finite group G. Maybe surprisingly, many of these components are not an obstruction for proving a "structure theorem", on the contrary.

According to Kleinert[4] a "Unit Theorem" for the unit group $\mathcal{U}(\mathbb{Z}G)$ is a statement that should at least consist, in purely group theoretical terms, of a class of groups $\mathcal{G}$ such that almost all torsionfree subgroups of finite index in $\mathcal{U}(\mathbb{Z}G)$ are members of $\mathcal{G}$.

So one can pose the following general problem.

Problem 7.1 *For a class of groups $\mathcal{G}$, classify the finite groups G, such that $\mathcal{U}(\mathbb{Z}G)$ constains a subgroup of finite index in $\mathcal{G}$.*

In the following results we state the answer for the class of groups $\mathcal{G}$ that consists of direct products of free products of abelian groups (Jespers and del Río) and for the class of groups that consists of the direct products of free-by-free groups (Jespers, Pita, del Río, Ruiz, P. Zalesskii).

Theorem 7.2 *The following properties are equivalent for a finite group G.*

1. *$\mathcal{U}(\mathbb{Z}G)$ is either virtually abelian or virtually nonabelian free.*
2. *$\mathcal{U}(\mathbb{Z}G)$ is virtually a free product of abelian groups.*
3. *$\mathbb{Q}G$ is a direct product of fields, division rings of the form $\left(\frac{-1,-3}{\mathbb{Q}}\right)$, or $\mathbb{H}(K)$ with $K=\mathbb{Q}$, $\mathbb{Q}(\sqrt{2})$ or $\mathbb{Q}(\sqrt{3})$ and at most one copy of $M_2(\mathbb{Q})$.*
4. *One of the following conditions hold:*
   (a) *$G = Q_8 \times C_2^n$,*

(b) *G is abelian,*

(c) *G is one of the following groups: D_6, $D_8, Q_{12} = \langle a, b \mid a^6 = 1,\ b^2 = a^3,\ ba = a^5 b\rangle$, $P = \langle a, b \mid a^4 = 1,\ b^4 = 1, aba^{-1}b^{-1} = a^2\rangle$ (in this case $\mathcal{U}(\mathbb{Z}G)$ is virtually nonabelian free).*

Note that he respective Wedderburn decomposition of mentioned rational group algebras is as follows (prove this as en excercise).
is (cf. [**?**, **?**, **?**]:

$$\begin{aligned}
\mathbb{Q}D_6 &\cong 2\mathbb{Q} \oplus M_2(\mathbb{Q}),\\
\mathbb{Q}D_8 &\cong 4\mathbb{Q} \oplus M_2(\mathbb{Q}),\\
\mathbb{Q}Q_8 &\cong 4\mathbb{Q} \oplus \mathbb{H}(\mathbb{Q}),\\
\mathbb{Q}P &\cong 4\mathbb{Q} \oplus 2\mathbb{Q}(i) \oplus \mathbb{H}(\mathbb{Q}) \oplus M_2(\mathbb{Q})\\
\mathbb{Q}Q_{12} &\cong 2\mathbb{Q} \oplus \mathbb{Q}(\sqrt{-3}) + \left(\frac{-1, -3}{\mathbb{Q}}\right) \oplus M_2(\mathbb{Q}),
\end{aligned}$$

Theorem 7.3 *The following properties are equivalent for a finite group G.*

1. *$\mathcal{U}(\mathbb{Z}G)$ is virtually a direct product of free-by-free groups.*

2. *For every simple component A of $\mathbb{Q}G$ and some (every) order $\mathcal{O}$ in A, the group of reduced norm one elements in $\mathcal{O}$ is virtually free-by-free.*

3. *Every simple component of $\mathbb{Q}G$ is either a field, a totally definite quaternion algebra, or $M_2(K)$ where K is either $\mathbb{Q}(i)$, $\mathbb{Q}(\sqrt{-2})$, $\mathbb{Q}(\sqrt{-3})$.*

4. *G is either abelian or an epimorphic image of $A \times H$, where A is an abelian group and one of the following conditions holds:*

   (a) *A has exponent 6 and H is one of the groups $\mathcal{W}$, $\mathcal{W}_{1n}$ or $\mathcal{W}_{2n}$.*

   (b) *A has exponent 4 and H is one of the groups $\mathcal{V}$, $\mathcal{V}_{1n}$, $\mathcal{V}_{2n}$, $\mathcal{U}_1$ or $\mathcal{U}_2$.*

   (c) *A has exponent 2 and H is one of the group $\mathcal{T}$, $\mathcal{T}_{1n}$, $\mathcal{T}_{2n}$ or $\mathcal{T}_{3n}$.*

   (d) *$H = M \rtimes P = (M \times Q) : \langle \overline{u} \rangle_2$, where M is an elementary abelian 3-group, $P = Q : \langle \overline{u} \rangle_2$, $m^u = m^{-1}$ for every $m \in M$, and one of the following conditions holds:*

      - *A has exponent 4 and $P = C_8$,*
      - *A has exponent 6, $P = W_{1n}$ and $Q = \langle y_1, \ldots, y_n, t_1, \ldots, t_n, x^2 \rangle$,*

- *A has exponent 2, $P = W_{21}$ and $Q = \langle y_1^2, x\rangle$.*

The non-nilpotent groups are those listed in (4) with M non-trivial.

The first class consists of the following groups.

$$\begin{aligned}
\mathcal{W} &= \left(\langle t\rangle_2 \times \langle x^2\rangle_2 \times \langle y^2\rangle_2\right) : \left(\langle \overline{x}\rangle_2 \times \langle \overline{y}\rangle_2\right), \\
&\quad \text{with } t = (x, y) \text{ and } Z(\mathcal{W}) = \langle x^2, y^2, t\rangle. \\
\mathcal{W}_{1n} &= \left(\prod_{i=1}^{n} \langle t_i\rangle_2 \times \prod_{i=1}^{n} \langle y_i\rangle_2\right) \rtimes \langle x\rangle_4, \\
&\quad \text{with } t_i = (x, y_i) \text{ and } Z(\mathcal{W}_{1n}) = \langle t_1, \dots, t_n, x^2\rangle. \\
\mathcal{W}_{2n} &= \left(\prod_{i=1}^{n} \langle y_i\rangle_4\right) \rtimes \langle x\rangle_4, \\
&\quad \text{with } t_i = (x, y_i) = y_i^2 \text{ and } Z(\mathcal{W}_{2n}) = \langle t_1, \dots, t_n, x^2\rangle.
\end{aligned}$$

The second class of groups consists of the following groups.

$$\begin{aligned}
\mathcal{V} &= \left(\langle t\rangle_2 \times \langle x^2\rangle_4 \times \langle y^2\rangle_4\right) : \left(\langle \overline{x}\rangle_2 \times \langle \overline{y}\rangle_2\right), \\
&\quad \text{with } t = (x, y) \text{ and } Z(\mathcal{V}) = \langle x^2, y^2, t\rangle. \\
\mathcal{V}_{1n} &= \left(\prod_{i=1}^{n} \langle t_i\rangle_2 \times \prod_{i=1}^{n} \langle y_i\rangle_4\right) \rtimes \langle x\rangle_8, \\
&\quad \text{with } t_i = (x, y_i) \text{ and } Z(\mathcal{V}_{1n}) = \langle t_1, \dots, t_n, y_1^2, \dots, y_n^2, x^2\rangle. \\
mathcalV_{2n} &= \left(\prod_{i=1}^{n} \langle y_i\rangle_8\right) \rtimes \langle x\rangle_8, \\
&\quad \text{with } t_i = (x, y_i) = y_i^4 \text{ and } Z(\mathcal{V}_{2n}) = \langle t_1, \dots, t_n, x^2\rangle.
\end{aligned}$$

The third class consists of the following groups.

$$\begin{aligned}\mathcal{U}_1 &= \left(\prod_{1\leq i<j\leq 3}\langle t_{ij}\rangle_2\right) : \left(\prod_{k=1}^{3}\langle\overline{y_k}\rangle_4\right),\\ &\quad\text{with } Z(\mathcal{U}_1) = \langle t_{12}, t_{13}, t_{23}, y_1^2, y_2^2, y_3^2\rangle,\ t_{ij} = (y_i, y_j) \text{ and } y_i^4 = 1.\\ \mathcal{U}_2 &= \left(\prod_{1\leq i<j\leq 3}\langle t_{ij}\rangle_2\right) : \left(\prod_{k=1}^{3}\langle\overline{y_k}\rangle_4\right),\\ &\quad\text{with } Z(\mathcal{U}_2) = \langle t_{12}, t_{13}, t_{23}, y_1^2, y_2^2, y_3^2\rangle,\ t_{ij} = (y_i, y_j),\\ &\quad y_1^4 = 1,\ y_2^4 = t_{12} \text{ and } y_3^4 = t_{13}.\end{aligned}$$

The following groups form part of the fourth class of groups.

$$\begin{aligned}\mathcal{T}_{1n} &= \left(\prod_{i=1}^{n}\langle t_i\rangle_4 \times \prod_{i=1}^{n}\langle y_i\rangle_4\right) \rtimes \langle x\rangle_8,\\ &\quad\text{with } t_i = (x, y_i),\ (x, t_i) = t_i^2 \text{ and } Z(\mathcal{T}_{1n}) = \langle t_1^2, \ldots, t_n^2, x^2\rangle.\end{aligned}$$

A major issue remains the lack of knowledge of constructung large subgroups of the unit group of an order in a finite dimensional rational division algebra (so dealing with orders in exceptional components of type 1).

Problem 7.4 *Discover generic constructions of units in orders of division algebras that are simple components of a rational group algebra $\mathbb{Q}G$ of a finite group. Discover generators of large subgroups in such orders.*

Problem 7.5 *Describe finitely many generators for the following unit groups:*

$$\mathcal{U}(\mathbb{Z}(Q_8 \times C_3)) \quad \textit{and} \quad \mathcal{U}(\mathbb{Z}(Q_8 \times C_7)).$$

8 Exercises

1. Prove with elementary methods that the following unit groups are as described.

   (a) $\mathcal{U}(\mathbb{Z}[i]) = \{1, -1, i, -i\}$.

   (b) $\mathcal{U}(\mathbb{Z}[\xi_3]) = \{\pm 1, \pm\xi_3, \pm\xi_3^2\}$.

   (c) $\mathcal{U}(\mathbb{Z}[\xi_6]) = \langle\xi_6\rangle$.

   (d) $\mathcal{U}\left(\left(\frac{-1,-1}{\mathbb{Z}}\right)\right) = Q_8$, where Q_8 is the quaternion group of order 8.

2. Compute with elementary methods the Wedderburn decomposition of $\mathbb{Q}C_8$ and $\mathbb{Q}C_5$. Then prove that the following unit groups are as described.

   (a) $\mathcal{U}(\mathbb{Z}[\xi_8]) = \langle \xi_8 \rangle \times \langle 1+\sqrt{2} \rangle = \langle \xi_8 \rangle \times \langle \eta_3(\xi_8) \rangle = C_8 \times C_\infty$ where $\eta_3(\xi_8) = 1 + \xi_8 + \xi_8^2$.

   (b) $\mathcal{U}(\mathbb{Z}C_5) = \pm C_5 \times \langle g + g^4 - 1 \rangle$, where $C_5 = \langle g \mid g^5 = 1 \rangle$. Hint, first show that $\mathbb{Z}C_5 \subseteq \mathbb{Z} \oplus \mathbb{Z}[\xi_5]$.

   (c) $\mathcal{U}_1(\mathbb{Z}C_8) = C_8 \times \langle u_{3,2}(g) \rangle = C_8 \times C_\infty$, where $C_8 = \langle g \mid g^8 = 1 \rangle$. Hint, first prove that $\mathbb{Z}C_8 \subseteq \mathbb{Z}^2 \oplus \mathbb{Z}[i] \oplus \mathbb{Z}[\xi_8]$ and then use part (a).

3. Compute the Wedderburn decomposition of $\mathbb{Q}Q_8$ and prove that $\mathcal{U}_1(\mathbb{Z}Q_8) = Q_8$ (Higman).

4. Compute the Wedderburn decomposition of $\mathbb{Q}D_8$ and prove that $\mathcal{U}_1(\mathbb{Z}D_8) = B \rtimes D_8$, where B is the subgroup generated by the bicyclic units. Furthermore, B is a free group of rank 3

5. Prove that if $\mathcal{U}_1(\mathbb{Z}G)$ is finite then so is the unit group $\mathcal{U}_1(|Z(G \times C_2))$.

6. Let G be a finite group and N a normal subgroup of G. Let F be a field whose characteristic does not divide $|G|$. Prove that the following element is a central idempotent.

$$\varepsilon(G,N) = \begin{cases} \widehat{G} & \text{if } G = N \\ \prod_{D/N \in M(G/N)} (\widehat{N} - \widehat{D}), & \text{otherwise} \end{cases}$$

7. Let F be a field of characteristic different from 2. Prove that a quaternion algebra $A = \left(\frac{a,b}{F}\right)$ is a simple algebra with center F. Prove that the following conditions are equivalent:

   (a) $A = \mathrm{M}_2(F)$,

   (b) $N(x) = 0$ for some $0 \neq x \in A$,

   (c) $u^2 = av^2 + bw^2$ for some $0 \neq (u,v,w) \in F^3$.

8. Compute for some groups of small order a complete set of primitive central idempotents and a complete set of primitive idempotents of $\mathbb{Q}G$.

9. Prove Lemma 6.5.

References

[1] E. Jespers and Á. del Río, Group ring groups, Vol. 1: Orders and generic constructions of units, De Gruyter Graduate, De Gruyter, Berlin, 2016. xii+447 pp. ISBN: 978-3-11-037278-6; 978-3-11-038617-2

[2] E. Jespers and Á. del Río, Group ring groups, Vol. 2: structure theorems of unit groups, De Gruyter Graduate, De Gruyter, Berlin, 2016. xii+447 pp. ISBN: 978-3-11-041149-2; 978-3-11-041275-8.

[3] S.K. Sehgal, Units in integral group rings, vol 69 of Pitman Monographs and Suveys in Pure and Applied Mathematics, Longman Scientifiic & Technical, Harlow, 1993.

[4] E. Kleinert, Units of classical orders: a survey, Enseign. Math. 40 (1994), 205–248.