

ARITHMETIC RIGIDITY AND UNITS IN GROUP RINGS

F. E. A. JOHNSON

ABSTRACT. For any finite group G the group $U(\mathbf{Z}[G])$ of units in the integral group ring $\mathbf{Z}[G]$ is an arithmetic group in a reductive algebraic group, namely the Zariski closure of $\mathbf{SL}_1(\mathbf{Q}[G])$. In particular, the isomorphism type of the \mathbf{Q} -algebra $\mathbf{Q}[G]$ determines the commensurability class of $U(\mathbf{Z}[G])$; we show that, to a large extent, the converse is true. In fact, subject to a certain restriction on the \mathbf{Q} -representations of G the converse is exactly true.

0. INTRODUCTION

Two abstract groups Γ_1, Γ_2 are said to be *commensurable*, written $\Gamma_1 \sim \Gamma_2$, when there exists a group Δ , and injections $\iota_r : \Delta \rightarrow \Gamma_r$ ($r = 1, 2$), such that $\iota_r(\Delta)$ has finite index in Γ_r . In this paper, we investigate the structure, up to commensurability, of the unit group $U(\mathbf{Z}[G])$ of the integral group ring of a finite group G . By Wedderburn's Theorem, the rational group ring $\mathbf{Q}[G]$ is a direct sum

$$\mathbf{Q}[G] = \mathcal{A}_1 \oplus \cdots \oplus \mathcal{A}_m$$

of simple two sided ideals; we say that a finite dimensional simple \mathbf{Q} -algebra is *small* when it is either (i) commutative (hence a field), or (ii) a quaternion algebra (possibly split) over \mathbf{Q} , or (iii) a negative definite quaternion algebra over a totally real field; otherwise, it is said to be *big*. A finite dimensional semisimple \mathbf{Q} -algebra \mathcal{A} is naturally a sum $\mathcal{A} \cong \mathcal{A}_{\text{small}} \oplus \mathcal{A}_{\text{big}}$ where $\mathcal{A}_{\text{small}}$ (resp. \mathcal{A}_{big}) is the sum of all the small (resp. big) two sided ideals. We shall see that, for a finite group G , $\mathbf{Q}[G]_{\text{big}}$ is an invariant, not only of the isomorphism class of $U(\mathbf{Z}[G])$, but even of its commensurability class.

Theorem I. *Let G_1, G_2 be finite groups; if $U(\mathbf{Z}[G_1])$ and $U(\mathbf{Z}[G_2])$ are commensurable, then $\mathbf{Q}[G_1]_{\text{big}} \cong \mathbf{Q}[G_2]_{\text{big}}$.*

The converse is false; if D_{2n} denotes the dihedral group of order $2n$, and Q_{4n} the generalised quaternion group of order $4n$, then $\mathbf{Q}[Q_{4n}]_{\text{big}} \cong \mathbf{Q}[D_{2n}]_{\text{big}}$. However, $U(Q_{4n})$ fails to be commensurable with $U(D_{2n})$ whenever $n \geq 4$. The difficulty arises from the fact that $\mathbf{Q}[Q_{4n}]$ has small factors; if these are excluded, we get

Corollary II. *Let G_1, G_2 be finite groups having no nontrivial small factors in their rational Wedderburn decompositions; then*

$$U(\mathbf{Z}[G_1]) \sim U(\mathbf{Z}[G_2]) \iff \mathbf{Q}[G_1] \cong \mathbf{Q}[G_2].$$

Received by the editors November 12, 1999 and, in revised form, August 28, 2000.
 2000 *Mathematics Subject Classification.* Primary 20C05; Secondary 20G20, 22E40.

We begin by giving a structure theorem for the commensurability class of a unit group $U(\mathbf{Z}[G])$; say that an infinite group G is *reducible* when it is commensurable to a direct product $G \sim H_1 \times H_2$ where H_1, H_2 are infinite groups; otherwise, G is *irreducible*. It is straightforward to see that a finitely generated infinite group G is irreducible if and only if it contains no subgroup of finite index which is isomorphic to a direct product of infinite groups.

A group Λ is said to be an \mathcal{L} -product when it is a direct product of the form

$$\Lambda = \Lambda_1 \times \cdots \times \Lambda_n \times \Lambda^{ab}$$

where Λ^{ab} is a free abelian group of finite rank (possibly zero), and $\Lambda_1, \dots, \Lambda_n$ are irreducible groups of finite cohomological dimension with the property that every subgroup of finite index has trivial centre. To cope with the degenerate cases which arise in the context of unit groups of group rings, (for example $U(\mathbf{Z}[Q_8])$) we allow for the possibility that $n = 0$. The following structural result is almost certainly known, but does not appear to have been stated in the literature in this form:

Theorem III. *Let G be a finite group; then $U(\mathbf{Z}[G])$ is commensurable with an \mathcal{L} -product whose irreducible factors are duality groups in the sense of [3].*

In fact, we will describe an \mathcal{L} -product representative for the commensurability class $U(\mathbf{Z}[G])$ directly from the rational Wedderburn decomposition of $\mathbf{Q}[G]$.

One should emphasise that the crux of Theorem I is Mostow's Rigidity Theorem [14]. However, in addition, our results are heavily dependent on the classical theory of lattices in Lie groups, and in particular, on the work of Borel [4], [5], [6] and Borel-Harish Chandra [7]. An excellent and convenient recent reference for this material is the text of Platonov and Rapinchuk [16].

The plan of the paper is as follows: in §1 we prove a uniqueness theorem for \mathcal{L} -product structures. Theorem III is proved in §2. In §3, we show how the theorem of Albert [1], [19] places restrictions on the possible irreducible components of $U(\mathbf{Z}[G])$ when G is finite. The rigidity result, Theorem I, is proved in §4. Finally, in §5 we give a calculation which relates the unit groups of generalised quaternion groups to those of dihedral groups and show that the converse to Theorem I is false. We wish to thank the referee for some helpful remarks, and in particular, for pointing out an oversight in the original formulation of (4.1).

1. A UNIQUENESS THEOREM FOR PRODUCT STRUCTURES

It is a consequence of the Borel Density Theorem [4] that a lattice in a connected linear semisimple Lie group admits, up to commensurability, an essentially unique decomposition into a product of irreducible semisimple lattices ([17], p.86). Here we give a generalisation of this fact under somewhat weaker hypotheses, allowing, in particular, for abelian factors.

If \mathcal{C} is a class of groups, we say that a group G admits a \mathcal{C} -product structure when it is the internal direct product, written $G = G_1 \circ \cdots \circ G_m$, of a finite sequence (G_1, \dots, G_m) of normal subgroups of G such that each $G_i \in \mathcal{C}$.

Let \mathcal{L}_s (the suffix connotes 'semisimple') denote the class of finitely generated infinite groups of finite cohomological dimension with the property that every subgroup of finite index has trivial centre, and let \mathcal{L}_0 denote the subclass of \mathcal{L}_s consisting of *irreducible* groups. An easy argument on Borel's Density Theorem shows that any torsion free lattice in a linear semisimple Lie group belongs to \mathcal{L}_s ; it is also

true, though not essential for our argument, that an infinite group G belongs to \mathcal{L}_s if and only if it is commensurable to a group possessing an \mathcal{L}_0 -product structure.

Let $\mathcal{L} = \mathcal{L}_0 \cup \{\text{free abelian groups of finite rank}\}$. By collecting together abelian factors, we observe that a group G has an \mathcal{L} -product structure precisely when $G \cong \Lambda_1 \times \cdots \times \Lambda_n \times \Lambda^{ab}$ where Λ^{ab} is free abelian of finite rank, and $\Lambda_i \in \mathcal{L}_0$ for $1 \leq i \leq n$. We will show that an \mathcal{L} -product structure is unique up to commensurability.

Lemma 1.1. *Let G_1, G_2 be groups such that*

$$G_1 = \Lambda_1^s \circ \Lambda_1^{ab} ; G_2 = \Lambda_2^s \circ \Lambda_2^{ab}$$

where Λ_1^s, Λ_2^s are \mathcal{L}_s -groups and $\Lambda_1^{ab}, \Lambda_2^{ab}$ are free abelian groups. Then G_1 is commensurable with G_2 if and only if Λ_1^s is commensurable with Λ_2^s and Λ_1^{ab} is commensurable with Λ_2^{ab} .

Proof. (\Rightarrow) Denote the centre of a group G by $\mathcal{Z}(G)$. First observe that for a group G which is an internal direct product $G = \Lambda^s \circ \Lambda^{ab}$ where Λ^{ab} is an abelian group, and $\Lambda^s \in \mathcal{L}_s$, we have $H \cap \Lambda^{ab} = \mathcal{Z}(H)$ for any subgroup H of finite index in G . Now suppose that $H_1 \subset G_1, H_2 \subset G_2$ are subgroups of finite index, and that $\varphi : H_1 \rightarrow H_2$ is an isomorphism. It follows that φ induces an isomorphism $\varphi : \mathcal{Z}(H_1) \rightarrow \mathcal{Z}(H_2)$. By the observation above, $\mathcal{Z}(H_1) = H_1 \cap \Lambda_1^{ab}$ and $\mathcal{Z}(H_2) = H_2 \cap \Lambda_2^{ab}$. We conclude that Λ_1^{ab} is commensurable with Λ_2^{ab} since $H_1 \cap \Lambda_1^{ab}$ has finite index in Λ_1^{ab} and $H_2 \cap \Lambda_2^{ab}$ has finite index in Λ_2^{ab} . Likewise, φ induces an isomorphism $\varphi_* : H_1/\mathcal{Z}(H_1) \rightarrow H_2/\mathcal{Z}(H_2)$. Let π_s denote the projection to Λ_i^s in each case. Since $H_i/\mathcal{Z}(H_i) \cong \pi_s(H_i)$, φ also induces an isomorphism $\varphi_* : \pi_s(H_1) \rightarrow \pi_s(H_2)$. Thus Λ_1^s is commensurable with Λ_2^s since $\pi_s(H_i)$ has finite index in Λ_i^s for $i = 1, 2$. This proves (\Rightarrow); the implication (\Leftarrow) is clear. \square

We obtain the following uniqueness result for \mathcal{L} -products:

Theorem 1.2. *Let $\Lambda = \Lambda_1 \times \cdots \times \Lambda_n \times \Lambda^{ab}$ and $\Omega = \Omega_1 \times \cdots \times \Omega_m \times \Omega^{ab}$ be \mathcal{L} -products; if $\Lambda \sim \Omega$ then $\text{rk}_{\mathbf{Z}}\Omega^{ab} = \text{rk}_{\mathbf{Z}}\Lambda^{ab}$, $m = n$ and there exists a permutation σ such that for all i ($1 \leq i \leq n$), $\Omega_{\sigma(i)} \sim \Lambda_i$.*

Proof. In the special case of an \mathcal{L}_0 -product structure, that is where $\Lambda^{ab} = \Omega^{ab} = 0$, the result is proved in [12] (Proposition 6.2).

In the general case, suppose that $\Lambda = \Lambda_1 \circ \cdots \circ \Lambda_n \circ \Lambda^{ab}$ and $\Omega = \Omega_1 \circ \cdots \circ \Omega_m \circ \Omega^{ab}$ are \mathcal{L} -products such that $\Lambda \sim \Omega$. Writing $\Lambda^s = \Lambda_1 \circ \cdots \circ \Lambda_n$ and $\Omega^s = \Omega_1 \circ \cdots \circ \Omega_m$ we have $\Lambda = \Lambda^s \circ \Lambda^{ab}$, $\Omega = \Omega^s \circ \Omega^{ab}$ satisfying the hypotheses of (1.1). We deduce that $\Lambda^{ab} \sim \Omega^{ab}$, so that $\text{rk}_{\mathbf{Z}}(\Lambda^{ab}) = \text{rk}_{\mathbf{Z}}(\Omega^{ab})$, and $\Lambda^s \sim \Omega^s$; the result now follows from the special case considered above. \square

2. \mathbf{Z} -FREE ALGEBRAS

If \mathcal{R} is a ring (associative with identity), we denote by $U(\mathcal{R})$ the group of units of \mathcal{R} ,

$$U(\mathcal{R}) = \{\mathbf{x} \in \mathcal{R} : \mathbf{xy} = \mathbf{yx} = \mathbf{1} \text{ for some } \mathbf{y} \in \mathcal{R}\}.$$

Observe that U commutes with direct products, $U(\mathcal{R}_1 \times \mathcal{R}_2) = U(\mathcal{R}_1) \times U(\mathcal{R}_2)$. For any ring \mathcal{B} , we denote by $GL_{\mathbf{Z}}(\mathcal{B})$ the group of automorphisms of the additive group of \mathcal{B} . There is a faithful representation $\lambda : U(\mathcal{B}) \rightarrow GL_{\mathbf{Z}}(\mathcal{B})$; $u \mapsto \lambda_u$ where $\lambda_u(x) = ux$. By a \mathbf{Z} -free algebra we mean an algebra over \mathbf{Z} whose underlying

additive group is \mathbf{Z} -free of finite rank. If \mathcal{A} is a finite dimensional \mathbf{Q} -algebra, then by a \mathbf{Z} -order in \mathcal{A} we mean a subring \mathcal{B} of \mathcal{A} with the property that \mathcal{B} is a free \mathbf{Z} -algebra which spans \mathcal{A} over \mathbf{Q} .

Proposition 2.1. *Let \mathcal{A} be a finite dimensional \mathbf{Q} -algebra; if $\mathcal{B}_1, \mathcal{B}_2$ are \mathbf{Z} -orders in \mathcal{A} then $U(\mathcal{B}_1)$ is commensurable with $U(\mathcal{B}_2)$.*

Proof. $\mathcal{B}_1, \mathcal{B}_2$, and $\mathcal{B}_1 + \mathcal{B}_2$ are all \mathbf{Z} -lattices in the \mathbf{Q} -vector space \mathcal{A} . In particular, \mathcal{B}_i has finite index in $\mathcal{B}_1 + \mathcal{B}_2$ for $i = 1, 2$. Thus $\mathcal{B}_1 \cap \mathcal{B}_2$, has finite index in \mathcal{B}_i for $i = 1, 2$, and contains an \mathbf{Q} -basis for \mathcal{A} . Thus $\mathcal{B}_1 \cap \mathcal{B}_2$ is also a \mathbf{Z} -order in \mathcal{A} since it is a subring. Thus it suffices to prove a more exact special case, namely that if $\mathcal{B}_2 \subset \mathcal{B}_1$ then $U(\mathcal{B}_2)$ is a subgroup of finite index in $U(\mathcal{B}_1)$.

Let $\text{Stab}(\mathcal{B}_2)$ be the stability group of \mathcal{B}_2 within $GL_{\mathbf{Z}}(\mathcal{B}_1)$. If $u \in \mathcal{B}_1$ has the property that $\lambda_u \in \text{Stab}(\mathcal{B}_2)$, then $u = \lambda_u(1) \in \mathcal{B}_2$. Thus $U(\mathcal{B}_2) = U(\mathcal{B}_1) \cap \text{Stab}(\mathcal{B}_2)$.

However, $\text{Stab}(\mathcal{B}_2)$ is the kernel of the natural map $GL_{\mathbf{Z}}(\mathcal{B}_1) \rightarrow \text{Aut}(\mathcal{B}_1/\mathcal{B}_2)$. Moreover, since $\mathcal{B}_1, \mathcal{B}_2$ both span \mathcal{A} , then \mathcal{B}_2 has finite index in \mathcal{B}_1 , hence $\text{Aut}(\mathcal{B}_1/\mathcal{B}_2)$ is finite and $\text{Stab}(\mathcal{B}_2)$ is a subgroup of finite index in $GL_{\mathbf{Z}}(\mathcal{B}_1)$. Thus $U(\mathcal{B}_2) = U(\mathcal{B}_1) \cap \text{Stab}(\mathcal{B}_2)$ is a subgroup of finite index in $U(\mathcal{B}_1) = U(\mathcal{B}_1) \cap GL_{\mathbf{Z}}(\mathcal{B}_1)$. \square

Corollary 2.2. *Let $\mathcal{A} = \mathcal{A}_1 \oplus \cdots \oplus \mathcal{A}_q$ be a decomposition as a direct sum of two sided ideals of the finite dimensional \mathbf{Q} -algebra \mathcal{A} . Let \mathcal{B} be a \mathbf{Z} -order in \mathcal{A} , and for each i , let \mathcal{B}_i be a \mathbf{Z} -order in \mathcal{A}_i . Then $U(\mathcal{B})$ is commensurable with $U(\mathcal{B}_1) \times U(\mathcal{B}_2) \times \cdots \times U(\mathcal{B}_q)$.*

Proof. Clearly $\mathcal{B}_1 \oplus \mathcal{B}_2 \oplus \cdots \oplus \mathcal{B}_q$ is also a \mathbf{Z} -order in \mathcal{A} , so that $U(\mathcal{B})$ is commensurable with $U(\mathcal{B}_1 \oplus \mathcal{B}_2 \oplus \cdots \oplus \mathcal{B}_q)$ by (2.2). The result now follows, since

$$U(\mathcal{B}_1 \oplus \mathcal{B}_2 \oplus \cdots \oplus \mathcal{B}_q) \cong U(\mathcal{B}_2) \times \cdots \times U(\mathcal{B}_q). \quad \square$$

If \mathcal{A} is a finite dimensional semisimple \mathbf{Q} -algebra, then $\mathcal{A} \otimes_{\mathbf{Q}} \mathbf{C}$ is a product of matrix algebras over \mathbf{C} , whereby $U(\mathcal{A})$ acquires the structure of a linear algebraic group. Moreover, if \mathcal{B} is a \mathbf{Z} -order in \mathcal{A} , then $U(\mathcal{B})$ is precisely the stability group of the lattice \mathcal{B} under the action of $U(\mathcal{A})$ by left multiplication on \mathcal{A} ; that is:

Proposition 2.3. *Let \mathcal{A} be a finite dimensional semisimple \mathbf{Q} -algebra, and let \mathcal{B} be a \mathbf{Z} -order in \mathcal{A} ; then $U(\mathcal{B})$ is an arithmetic subgroup of $U(\mathcal{A})$.*

For any finite group G , $\mathbf{Z}[G]$ is a \mathbf{Z} -order in the semisimple \mathbf{Q} -algebra $\mathbf{Q}[G]$; the following consequence of (2.3) is presumably well known, but difficult to find a reference for:

Corollary 2.4. *Let G be a finite group; then $U(\mathbf{Z}[G])$ is an arithmetic subgroup of $U(\mathbf{Q}[G])$.*

Let \mathcal{A} be a finite dimensional simple \mathbf{Q} -algebra with centre \mathbf{E} . Then $\mathcal{A} \otimes_{\mathbf{E}} \overline{\mathbf{Q}} \cong M_d(\overline{\mathbf{Q}})$. Thus $U(\mathcal{A})$ is an \mathbf{E} -form of GL_d . Observe that ([5], Chapter I) both the centre \mathcal{Z} and the commutator subgroup $SL_1(\mathcal{A}) = [U(\mathcal{A}), U(\mathcal{A})]$ are normal algebraic subgroups of $U(\mathcal{A})$ defined over \mathbf{E} . Moreover, the intersection $\Phi = SL_1(\mathcal{A}) \cap \mathcal{Z}$ is a finite group, isomorphic to the (finite) group of d^{th} -roots of unity. Thus $U(\mathcal{A})$ is an almost direct product over \mathbf{E}

$$U(\mathcal{A}) \cong SL_1(\mathcal{A}) \circ \mathcal{Z}.$$

Let Γ be an arithmetic subgroup of $U(\mathcal{A})$; we may suppose without loss of generality that Γ is torsion free, so that $\Gamma \cap SL_1(\mathcal{A}) \cap \mathcal{Z}$ is trivial. Let π_1, π_2 denote the projections to $PSL_1(\mathcal{A})$ and \mathcal{Z}/Φ respectively. Both π_1, π_2 are surjective algebraic homomorphisms defined over \mathbf{E} , so that $\Gamma^s = \pi_1(\Gamma)$ is an arithmetic subgroup of $PSL_1(\mathcal{A})$ and $\Gamma^{ab} = \pi_2(\Gamma)$ is an arithmetic subgroup of \mathcal{Z}/Φ . (See for example, Theorem 6 of [4]; see also [16], Chap 4, p. 204, Thm. 4.1). In particular, we obtain:

Proposition 2.5. *Let \mathcal{A} be a finite dimensional simple \mathbf{Q} -algebra, and let Γ be an arithmetic subgroup of $U(\mathcal{A})$; then Γ is commensurable with a direct product $\Gamma^s \times \Gamma^{ab}$ where Γ^s is an arithmetic subgroup of $PSL_1(\mathcal{A})$, and Γ^{ab} is a finitely generated abelian group.*

A straightforward application of Borel’s Density Theorem shows that if \mathcal{A} is a finite dimensional simple noncommutative \mathbf{Q} -algebra, and Γ^s is an infinite arithmetic subgroup of $PSL_1(\mathcal{A})$, then Γ^s is irreducible. For a more general statement compare, for example, [10], Thm. (3.4).

Borel and Serre [8] prove that if Γ is a torsion free arithmetic subgroup of the reductive \mathbf{Q} -group \mathbf{H} , then Γ is a duality group, and its cohomological dimension is given by

$$\text{cd}(\Gamma) = \text{gd}(\mathbf{H}_{\mathbf{R}}) - \text{rk}_{\mathbf{Q}}(\mathbf{H}),$$

where $\text{rk}_{\mathbf{Q}}(\mathbf{H})$ is the rank of a maximal \mathbf{Q} -split torus in \mathbf{H} and $\text{gd}(\mathbf{H})$ is the *geometric dimension* of \mathbf{H} ; that is, the dimension of the associated symmetric space $\text{gd}(\mathbf{H}_{\mathbf{R}}) = \dim(\mathbf{H}_{\mathbf{R}}/K)$ where $K \subset \mathbf{H}_{\mathbf{R}}$ is a maximal compact subgroup.

Proof of Theorem III. We must show that $U(\mathbf{Z}[G])$ is commensurable with an \mathcal{L} -product whose irreducible factors are duality groups. By Maschke’s Theorem, $\mathbf{Q}[G]$ decomposes as a sum $\mathcal{A}_1 \oplus \mathcal{A}_2 \oplus \dots \oplus \mathcal{A}_m$ where each \mathcal{A}_i is a simple two sided ideal. Let \mathcal{B}_i be a \mathbf{Z} -order in \mathcal{A}_i . Then $\mathcal{B}_1 \oplus \mathcal{B}_2 \oplus \dots \oplus \mathcal{B}_m$ is a \mathbf{Z} -order in $\mathbf{Q}[G]$, so that, by (2.2), \mathcal{B} is commensurable with $U(\mathcal{B}_1) \times \dots \times U(\mathcal{B}_m)$. By (2.5), $U(\mathcal{B}_i)$ is commensurable with a product $\Gamma_i^s \times \Gamma_i^{ab}$ where Γ_i^{ab} is free abelian of finite rank, and Γ_i^s is an irreducible lattice in a semisimple group and hence, by the Theorem of Borel and Serre, a duality group. Hence $U(\mathbf{Z}[G])$ is commensurable with $\Gamma_1^s \times \dots \times \Gamma_m^s \times \Gamma^{ab}$ where $\Gamma^{ab} = \Gamma_1^{ab} \times \dots \times \Gamma_m^{ab}$. \square

3. POSITIVE SEMISIMPLE ALGEBRAS

We review Albert’s classification [1] of simple \mathbf{Q} -algebras which admit a positive involution. Thus let \mathbf{K} be a subfield of \mathbf{R} , and let \mathcal{A} be a finite dimensional semisimple \mathbf{K} -algebra; by an *algebra involution* τ on \mathcal{A} , we mean an isomorphism of \mathcal{A} with its opposite algebra such that $\tau^2 = 1_{\mathcal{A}}$; τ is said to be *positive* when $\text{Tr}_{\mathbf{K}}(x\tau(x)) > 0$ for all nonzero $x \in \mathcal{A}$, where ‘ $\text{Tr}_{\mathbf{K}}$ ’ denotes ‘*reduced trace*’. If \mathcal{A} is expressed as a sum of simple ideals, $\mathcal{A} = \mathcal{A}_1 \oplus \mathcal{A}_2 \oplus \dots \oplus \mathcal{A}_n$, then from the uniqueness of the Wedderburn decomposition, an algebra involution τ induces an involution τ_* on the index set $\{1, 2, \dots, n\}$ by the condition that $\tau(\mathcal{A}_i) = \mathcal{A}_{\tau_*(i)}$. If $\tau_*(i) \neq i$, it is immediate that, for any $x \in \mathcal{A}_i$, $x\tau(x) = 0$. Hence the positivity condition forces $\tau_* = \text{Id}$; that is:

Proposition 3.1. *Let τ be a positive involution on finite dimensional semisimple K -algebra \mathcal{A} ; then there is an isomorphism of involuted K -algebras*

$$(\mathcal{A}, \tau) = (\mathcal{A}_1, \tau_1) \oplus (\mathcal{A}_2, \tau_2) \oplus \dots \oplus (\mathcal{A}_n, \tau_n),$$

in which each (\mathcal{A}_i, τ_i) is a simple positively involuted algebra.

If Φ is a finite group, $\mathbf{K}[\Phi]$ admits a positive involution τ given by

$$\tau(a) = \sum_{g \in \Phi} a_g g^{-1} \quad \text{where} \quad a = \sum_{g \in \Phi} a_g g.$$

If D is a finite dimensional division algebra over \mathbf{K} , an involution σ on D extends to an involution $\hat{\sigma}$ on $M_n(D)$; thus

$$\hat{\sigma}((x_{ij})) = (\sigma(x_{ji}))$$

with transposed indices as indicated. By the Skolem-Noether Theorem, each involution on $M_n(D)$ has this form. Moreover, $\hat{\sigma}$ is positive if and only if σ is positive. It follows from (3.1) that

Proposition 3.2. *Let Φ be a finite group; for any real field \mathbf{K} , there is an isomorphism of involuted \mathbf{K} -algebras*

$$(\mathbf{K}[\Phi], \tau) \cong (M_{n_1}(D_1), \hat{\tau}_1) \times \cdots \times (M_{n_m}(D_m), \hat{\tau}_m)$$

where each D_i is a finite dimensional division algebra over \mathbf{K} , and τ_i is positive.

When $\mathbf{K} = \mathbf{Q}$, the class of positively involuted division algebras has been determined by Albert [1], [19]. To recall his results we first fix the following notation:

\mathcal{R} will denote a commutative ring; n an integer ≥ 2 ; $s : \mathcal{R} \rightarrow \mathcal{R}$ is a ring automorphism satisfying $s^n = \text{Id}$; a will denote a nonzero element of \mathcal{R} with the property that $s(a) = a$. With this notation, the *cyclic algebra* $\mathcal{C}_n(\mathcal{R}, s, a)$ is the two sided free \mathcal{R} -module of rank n , with basis $([X^r])_{0 \leq r \leq n-1}$, subject to the relations

$$[X^r]\lambda = s^r(\lambda)[X^r] \quad (\lambda \in \mathcal{R}).$$

$\mathcal{C}_n(\mathcal{R}, s, a)$ is an algebra over the fixed point ring $\mathbf{E} = \{x \in \mathcal{R} : s(x) = x\}$ with multiplication determined by

$$[X][X^r] = \begin{cases} [X^{r+1}], & 0 \leq r < n-1, \\ a[X^0], & r = n-1. \end{cases}$$

We note that when $\mathcal{R} = \mathbf{K}$ is a field and s has order n (rather than merely satisfying $s^n = \text{Id}$) then the fixed point field ${}^s\mathbf{K} = \mathbf{E}$ is actually the centre of $\mathcal{C}_n(\mathbf{K}, s, a)$. This construction is natural with respect to direct products; that is, we have.

Proposition 3.3.

$$\mathcal{C}_n(\mathcal{R}_1 \times \mathcal{R}_2, s_1 \times s_2, (a_1, a_2)) \cong \mathcal{C}_n(\mathcal{R}_1, s_1, a_1) \times \mathcal{C}_n(\mathcal{R}_2, s_2, a_2).$$

A quaternion algebra $\left(\frac{a,b}{\mathbf{E}}\right)$ admits two essentially distinct involutions, namely *conjugation* c , and *reversion* r , defined thus

$$\begin{aligned} c(x_0 + x_1i + x_2j + x_3k) &= x_0 - x_1i - x_2j - x_3k, \\ r(x_0 + x_1i + x_2j + x_3k) &= x_0 + x_1i - x_2j + x_3k. \end{aligned}$$

Albert showed that a positively involuted division algebra (D, τ) , of finite dimension over \mathbf{Q} , falls into one of four classes; here \mathbf{E} and \mathbf{K} are algebraic number fields.

I: $D = \mathbf{E}$ is totally real and $\tau = 1_{\mathbf{E}}$;

II: $D = \left(\frac{a,b}{\mathbf{E}}\right)$, where \mathbf{E} is totally real, a is totally positive, b is totally negative, and τ is reversion;

III: $D = \left(\frac{a,b}{\mathbf{E}}\right)$, where \mathbf{E} is a totally real, a and b are both totally negative, and τ is conjugation;

IV: $D = \mathcal{C}_m(\mathbf{K}, s, a)$, where s is an automorphism of \mathbf{K} , of order m , whose fixed point field \mathbf{E} is an imaginary quadratic extension, $\mathbf{E} = \mathbf{E}_0(\sqrt{b})$, of a totally real field \mathbf{E}_0 , and $a \in \mathbf{E}$. Moreover, if \mathbf{L} is a maximal totally real subfield of \mathbf{K} , there exists a totally positive element $d \in \mathbf{L}$ such that $N_{\mathbf{E}/\mathbf{E}_0}(a) = N_{\mathbf{L}/\mathbf{E}_0}(d)$.

The possible simple summands which can occur in the Wedderburn decomposition of a finite group are restricted to these four types. Not all such simple algebras occur in this way, however, and there is an extensive literature on the problem of determining which algebras do in fact occur (‘the Schur subgroup problem’). Nevertheless, *all types* of algebra occur. Algebras of Type I, that is matrix algebras $M_n(\mathbf{E})$ over a totally real field \mathbf{E} , occur in the rational Wedderburn decomposition of dihedral groups D_{2n} . Fields [9] has shown that for any rational quaternion division algebra $\mathcal{D} = \left(\frac{a,b}{\mathbf{Q}}\right)$ there exists a finite group G such that some matrix algebra $M_n(\mathcal{D})$ occurs as a simple summand in $\mathbf{Q}[G]$. This takes care of Types II and III. Finally, algebras of Type IV already occur in the Wedderburn decompositions of cyclic groups, although these are rather trivial, being simply cyclotomic fields. Less trivially, Amitsur [2] showed that non-commutative division algebras of Type IV occur as summands for certain metacyclic groups.

In §4, we will apply Mostow Rigidity [14] to the irreducible semisimple lattices obtained from the group of units of an integral group ring. In this section, however, we study the noncommutative simple algebras (types LDI, LDII, LDIII below) whose associated irreducible lattices are nonrigid.

LDI: $M_2(\mathbf{Q})$;

LDII: $\left(\frac{a,b}{\mathbf{Q}}\right)$, where $a > 0, b < 0$, and the form $ax_1^2 + bx_2^2 - abx_3^2$ is \mathbf{Q} -anisotropic;

LDIII: $\left(\frac{a,b}{\mathbf{E}}\right)$, where \mathbf{E} is a totally real number field, and a and b are both totally negative.

Proposition 3.4. *Let \mathcal{A} be a finite dimensional simple \mathbf{Q} -algebra admitting a positive involution; then*

(i) $SL_1(\mathcal{A})_{\mathbf{R}} \cong SL_2(\mathbf{R}) \iff \mathcal{A}$ is of Type LDI or LDII;

(ii) $SL_1(\mathcal{A})_{\mathbf{R}} \cong \underbrace{SU(2) \times \cdots \times SU(2)}_d \iff \mathcal{A}$ is of Type LDIII.

Disregarding compact factors (which in our context occur only in the degenerate class LDIII), the only irreducible semisimple lattices which fail to be Mostow rigid are those in $SL_2(\mathbf{R})$ or $PSL_2(\mathbf{R})$. In fact, we need only consider nonrigid lattices Γ in $PSL_2(\mathbf{R})$, since up to commensurability, we may replace a lattice in $SL_2(\mathbf{R})$ by a torsion free lattice in $PSL_2(\mathbf{R})$. When $PSL_2(\mathbf{R})/\Gamma$ is noncompact, Γ is a free group of finite rank; when it is compact, Γ is a Surface group; that is, the fundamental group of an orientable surface of genus $g \geq 2$, with a presentation of the form

$$\Gamma = \langle X_1, \dots, X_g, Y_1, \dots, Y_g : \prod_{i=1}^g X_i Y_i X_i^{-1} Y_i^{-1} = 1 \rangle.$$

Again modulo compact factors and isogeny, neither Surface groups nor finitely generated free groups occur as irreducible lattices in any semisimple group other than $PSL_2(\mathbf{R})$. In terms of algebras, we have

Proposition 3.5. *Let \mathcal{A} be a simple \mathbf{Q} -algebra admitting a positive involution, and let Γ be a torsion free arithmetic subgroup of $SL_1(\mathcal{A})$; then*

- (i) \mathcal{A} is of Type LDI $\iff \Gamma$ is a nonabelian free group of finite rank;
- (ii) \mathcal{A} is of Type LDII $\iff \Gamma$ is a Surface group;
- (iii) \mathcal{A} is of Type LDIII $\iff \Gamma$ is trivial.

4. THE RIGIDITY THEOREM

Let \mathcal{A} be a finite dimensional simple \mathbf{Q} -algebra. We say that \mathcal{A} is *small* if either \mathcal{A} is commutative or a simple algebra of Type LD according to the definition of §3. Otherwise, \mathcal{A} is said to be *big*. Any finite dimensional semisimple \mathbf{Q} -algebra \mathcal{A} is naturally a sum $\mathcal{A} \cong \mathcal{A}_{\text{small}} \oplus \mathcal{A}_{\text{big}}$ where $\mathcal{A}_{\text{small}}$ (resp. \mathcal{A}_{big}) is the sum of all the small (resp. big) summands.

Let \mathbf{E} be a finite algebraic extension of \mathbf{Q} , and let \mathcal{A} be a central simple \mathbf{E} algebra with $\dim_{\mathbf{E}}(\mathcal{A}) = n^2$; the centre $\mathcal{Z}U(\mathcal{A})$ of $U(\mathcal{A})$ is isomorphic to \mathbf{E}^* . Moreover, $U(\mathcal{A}) = GL_1(\mathcal{A})$ is an \mathbf{E} -form of GL_n , and the *projective unit group* $PU(\mathcal{A}) = U(\mathcal{A})/\mathcal{Z}U(\mathcal{A})$ is an \mathbf{E} -form of PGL_n . Let \mathcal{M}_n denote the algebra valued functor $\mathbf{F} \mapsto M_n(\mathbf{F})$. PGL_n acts as the automorphism group of \mathcal{M}_n under the action

$$\begin{aligned} \bullet : PGL_n \times \mathcal{M}_n &\rightarrow \mathcal{M}_n, \\ \alpha \bullet X &= \alpha X \alpha^{-1}. \end{aligned}$$

We observe that the group isomorphism $\theta : GL_n \rightarrow GL_n$, defined by

$$\theta(X) = (X^{-1})^T = (X^T)^{-1},$$

descends to an automorphism, denoted by the same symbol, $\theta : PGL_n \rightarrow PGL_n$. However, for $n \geq 2$ the Dynkin diagram of PGL_n admits a single nontrivial symmetry, of order 2; that is, $\text{Out}(PGL_n) \cong C_2$, the generator being represented by θ . Thus $\text{Aut}(PGL_n)$ is a semidirect product

$$\text{Aut}(PGL_n) \cong PGL_n \times_{\theta} C_2.$$

Fix an algebraic number field \mathbf{E} , and let $\Gamma = \text{Gal}(\overline{\mathbf{Q}}/\mathbf{E})$. It is a standard result of Galois cohomology, essentially the Skolem-Noether Theorem, that central simple \mathbf{E} -algebras of dimension n^2 , that is, \mathbf{E} -forms of \mathcal{M}_n , are in 1-1 correspondence with elements of $H^1(\mathbf{E}, PGL_n) = H^1(\Gamma, PGL_n)$ (See, for example, [18], p. III-5.) The isomorphism $\mathcal{M}_n \rightarrow \mathcal{M}_n^{\text{opp}}$; $X \mapsto X^T$ is θ -equivariant; that is,

$$(\alpha \bullet X)^T = \theta(\alpha) \bullet X^T.$$

It follows that under the above correspondence, if the 1-cocycle $(a_{\gamma})_{\gamma \in \Gamma}$ represents the algebra \mathcal{A} , then the opposite algebra \mathcal{A}^{opp} is represented by the 1-cocycle $(\theta(a_{\gamma}))_{\gamma \in \Gamma}$.

If \mathcal{A} is a central simple \mathbf{E} -algebra, then \mathbf{E} is the field of definition of $PU(\mathcal{A})$, which is an \mathbf{E} -form of PGL_n . \mathbf{E} -forms of PGL_n are in 1-1 correspondence with elements of $H^1(\Gamma, \text{Aut}(PGL_n)) = H^1(\Gamma, PGL_n \times_{\theta} C_2)$; moreover, the mapping $\mathcal{A} \mapsto PU(\mathcal{A})$ is modelled by the mapping

$$i_* : H^1(\Gamma, PGL_n) \rightarrow H^1(\Gamma, PGL_n \times_{\theta} C_2)$$

induced by the inclusion $i : PGL_n \rightarrow PGL_n \times_{\theta} C_2$ of coefficients. Let \mathcal{A}, \mathcal{B} be central simple \mathbf{E} -algebras represented in $H^1(\Gamma, PGL_n)$ respectively by 1-cocycles $\mathbf{a} = (a_{\gamma})_{\gamma \in \Gamma}, \mathbf{b} = (b_{\gamma})_{\gamma \in \Gamma}$, and suppose that $PU(\mathcal{A}) \cong PU(\mathcal{B})$. This means that \mathbf{a}, \mathbf{b} become cohomologous in $Z^1(\Gamma, PGL_n \times_{\theta} C_2)$; that is, there exists $\mathbf{d} \in PGL_n \times_{\theta} C_2$ such that, for all $\gamma \in \Gamma$,

$$(b_{\gamma}, 1) = \mathbf{d}^{-1}(a_{\gamma}, 1) \gamma \mathbf{d}.$$

Now either $\mathbf{d} = (d, 1)$ or $\mathbf{d} = (d, \theta)$. In the first case,

$$b_{\gamma} = d^{-1} a_{\gamma} \gamma d$$

and \mathbf{a}, \mathbf{b} are already cohomologous in $Z^1(\Gamma, PGL_n)$; that is $\mathcal{B} \cong \mathcal{A}$. In the second case,

$$b_{\gamma} = e^{-1} \theta(a_{\gamma}) \gamma e,$$

where $e = \theta(d)$, so that $\mathcal{B} \cong \mathcal{A}^{opp}$. Thus we have shown

Theorem 4.1. *Let \mathcal{A}, \mathcal{B} be finite dimensional simple \mathbf{Q} -algebras; if $PU(\mathcal{A}) \cong PU(\mathcal{B})$, then either $\mathcal{A} \cong \mathcal{B}$ or $\mathcal{A}^{opp} \cong \mathcal{B}$.*

We first treat rigidity in the case of a single simple factor:

Theorem 4.2. *Let $\mathcal{A}, \mathcal{A}'$ be finite dimensional simple \mathbf{Q} -algebras which are big in the above sense, and let $\Gamma \subset SL_1(\mathcal{A})$ and $\Gamma' \subset SL_1(\mathcal{A}')$ be arithmetic subgroups; if $\Gamma \sim \Gamma'$, then either $\mathcal{A} \cong \mathcal{A}'$ or $\mathcal{A}^{opp} \cong \mathcal{A}'$.*

Proof. Put $G = PU(\mathcal{A})_{\mathbf{R},0}$ and $G' = PU(\mathcal{A}')_{\mathbf{R},0}$. By descending to subgroups of finite index, and projecting from SL_1 to PU , we may, without loss of generality, suppose that Γ, Γ' are both torsion free, and that $\Gamma \subset G$ and $\Gamma' \subset G'$. By hypothesis, $\Gamma \sim \Gamma'$, so there exists a group Δ together with injective homomorphisms $i : \Delta \rightarrow \Gamma, j : \Delta \rightarrow \Gamma'$ such that $\text{Im}(i)$ has finite index in Γ , and $\text{Im}(j)$ has finite index in Γ' . By Mostow's Rigidity Theorem [14], [15], there exists an isomorphism $\alpha : G' \rightarrow G$ such that $\alpha \circ j = i$. In the notation of [11], $(PU(\mathcal{A}), \text{Id})$ and $(PU(\mathcal{A}'), \alpha)$ are arithmetic structures for the inclusion $i : \Delta \rightarrow G$. It follows, by the Uniqueness Theorem of [11], that $PU(\mathcal{A}) \cong PU(\mathcal{A}')$. The conclusion follows by (4.1). \square

If G is a finite group which has ν simple summands in the Wedderburn decomposition of $\mathbf{Q}[G]$, we denote by ν_1 the number of *big* simple summands in the Wedderburn decomposition of $\mathbf{Q}[G]$, whilst ν_2 (resp. ν_3) will denote the total number of simple summands which are either of type LDI or LDII (resp. which are either commutative or of type LDIII). Moreover, if $\mathbf{Q}[G] = \mathcal{A}_1 \oplus \dots \oplus \mathcal{A}_{\nu}$ is the decomposition of $\mathbf{Q}[G]$ into its simple summands (so that $\nu = \nu_1 + \nu_2 + \nu_3$), we agree to arrange the summands so that \mathcal{A}_i is big for $1 \leq i \leq \nu_1$, of Type LDI or LDII for $\nu_1 + 1 \leq i \leq \nu_1 + \nu_2$, and commutative or of Type LDIII otherwise. We describe such an ordering as *nice*.

Choosing a nice ordering of the summands, let $\Lambda_i \subset SL_1(\mathcal{A}_i)$ be a torsion free lattice for $1 \leq i \leq \nu_1 + \nu_2$; for some finitely generated free abelian group Λ^{ab} ,

$$\Lambda = \Lambda_1 \times \dots \times \Lambda_{\nu_1 + \nu_2} \times \Lambda^{ab}$$

is an \mathcal{L} -product representative for $U(\mathbf{Z}[G])$. Similarly, let

$$\mathbf{Q}[G'] = \mathcal{A}'_1 \oplus \dots \oplus \mathcal{A}'_{\mu}$$

be a nice ordering of the summands for a finite group G' , and let

$$\Omega = \Omega_1 \times \cdots \times \Omega_{\mu_1+\mu_2} \times \Omega^{ab}$$

be the corresponding \mathcal{L} -product representative for $U(\mathbf{Z}[G'])$.

Suppose that $U(\mathbf{Z}[G]) \sim U(\mathbf{Z}[G'])$; then $\Lambda \sim \Omega$. By Theorem IV, $\mu_1 + \mu_2 = \nu_1 + \nu_2$, and for some permutation σ , $\Omega_{\sigma(i)} \sim \Lambda_i$. Since we chose a nice arrangement for the summands, in the \mathcal{L} -product decomposition

$$\Lambda = \Lambda_1 \times \cdots \times \Lambda_{\nu_1+\nu_2} \times \Lambda^{ab},$$

Λ_i is either a free group or a Surface group if and only if $\nu_1 + 1 \leq i \leq \nu_1 + \nu_2$. Likewise, Ω_j is either a free group or a Surface group if and only if $\mu_1 + 1 \leq j \leq \mu_1 + \mu_2$.

Now a finitely generated torsion free group is commensurable with a free group if and only if it is itself free [20]; likewise, an orientable Poincaré Duality group is commensurable with a Surface group if and only if it is itself a Surface group [13]. It follows that $\mu_2 = \nu_2$ and hence $\mu_1 = \nu_1$. We may now, without loss, arrange the indices so that $\Omega_i \sim \Lambda_i$ for $1 \leq i \leq \nu_1 + \nu_2 = \mu_1 + \mu_2$. By (4.2), it follows that for all i , $1 \leq i \leq \nu_1$, either $\mathcal{A}_i \cong \mathcal{A}'_i$ or $\mathcal{A}_i^{opp} \cong \mathcal{A}'_i$. However, since we are dealing with the simple components of a positively involuted algebra $\mathbf{Q}[G]$, each \mathcal{A}_i admits a positive involution and in particular $\mathcal{A}_i \cong \mathcal{A}_i^{opp}$. Thus $\mathcal{A}_i \cong \mathcal{A}'_i$ for all i , $1 \leq i \leq \nu_1$. Hence $\mathbf{Q}[G]_{big} = \bigoplus_{i=1}^{\nu_1} \mathcal{A}_i \cong \bigoplus_{i=1}^{\nu_1} \mathcal{A}'_i = \mathbf{Q}[G']_{big}$, and we have shown

Theorem I. *Let G_1, G_2 be finite groups such that $U(\mathbf{Z}[G_1]) \sim U(\mathbf{Z}[G_2])$; then*

$$\mathbf{Q}[G_1]_{big} \cong \mathbf{Q}[G_2]_{big}.$$

For any finite group G , there is at least one small factor in $\mathbf{Q}[G]$, namely the copy of \mathbf{Q} corresponding to the trivial representation. If G_1, G_2 are finite groups in which this trivial factor is the only small factor, then clearly $\mathbf{Q}[G_1]_{small} \cong \mathbf{Q}[G_2]_{small}$. We deduce from this and Theorem I that

Corollary II. *Let G_1, G_2 be finite groups having no nontrivial small factors in their rational Wedderburn decompositions; then*

$$U(\mathbf{Z}[G_1]) \sim U(\mathbf{Z}[G_2]) \iff \mathbf{Q}[G_1] \cong \mathbf{Q}[G_2].$$

The hypothesis of Corollary II is reasonably easy to satisfy; for example, a product of nonabelian simple groups has no nontrivial small factors in its rational Wedderburn decomposition.

5. UNITS OF DIHEDRAL AND GENERALISED QUATERNION GROUPS

For any integer $n \geq 3$, the generalised quaternion group Q_{4n} is defined by the presentation

$$Q_{4n} = \langle a, b \mid a^{2n} = b^2, \quad aba = b \rangle,$$

whilst we take the dihedral group D_{2n} in the presentation

$$D_{2n} = \langle \xi, \eta \mid \xi^n = \eta^2 = 1, \quad \xi\eta\xi = \eta \rangle.$$

There is a nontrivial central extension

$$1 \rightarrow C_2 \rightarrow Q_{4n} \xrightarrow{\psi_n} D_{2n} \rightarrow 1$$

defined by assigning $\psi_n(a) = \xi$, $\psi_n(b) = \eta$. This enables us to relate the structure of $\mathbf{Q}[Q_{4n}]$ directly to that of $\mathbf{Q}[D_{2n}]$. Denote by $\mathbf{Q}\langle n \rangle$ the quotient

$$\mathbf{Q}\langle n \rangle = \mathbf{Q}[x]/(x^n + 1).$$

Proposition 5.1. *For each $n \geq 2$, there is an algebra isomorphism*

$$\mathbf{Q}[Q_{4n}] \cong \mathbf{Q}[D_{2n}] \oplus \mathcal{C}_2(\mathbf{Q}\langle n \rangle, \sigma_n, -1).$$

Proof. Let z denote the central element $z = a^m = b^2 \in Q_{4m}$, and let

$$\theta : \mathbf{Q}[Q_{4n}] \rightarrow \mathbf{Q}[Q_{4n}]$$

denote the translation map $\theta(\mathbf{v}) = z\mathbf{v}$. Then $\theta^2 = \text{Id}$, so that we have a decomposition

$$\mathbf{Q}[Q_{4n}] = J_+ \oplus J_-$$

as a direct sum of two sided ideals, where J_+ , J_- denote respectively the $+1$ and -1 eigenspaces of θ . In fact, J_+ is spanned over \mathbf{Q} by elements of the form $a^r b^s (\frac{1+z}{2})$ where $0 \leq r \leq n-1$, $0 \leq s \leq 1$, from which it is easy to see that the homomorphism ψ_n induces an algebra isomorphism $\psi_n : J_+ \rightarrow \mathbf{Q}[D_{2n}]$.

To complete the proof, it suffices to show that $J_- \cong \mathcal{C}_2(\mathbf{Q}\langle n \rangle, \sigma_n, -1)$. In fact, J_- is spanned over \mathbf{Q} by elements of the form $a^r b^s (\frac{1-z}{2})$ where $0 \leq r \leq n-1$ and $0 \leq s \leq 1$. We regard

$$S = \text{span}_{\mathbf{Q}} \{ a^r (\frac{1-z}{2}) : 0 \leq r \leq n-1 \}$$

as a ring where $\frac{1-z}{2}$, which is a central idempotent of $\mathbf{Q}[Q_{4n}]$, acts as the identity. It is straightforward to see that $S \cong \mathbf{Q}\langle n \rangle$. Now J_- is a free module of rank 2 over S , generated by $\{X^0, X^1\}$, where $X^0 = (\frac{1-z}{2})$ and $X^1 = b(\frac{1-z}{2})$. However, conjugation by X^1 on S corresponds to the action of σ_n on $\mathbf{Q}\langle n \rangle$, and $(X^1)^2 = -X^0$. Thus

$$J_- \cong \mathcal{C}_2(\mathbf{Q}\langle n \rangle, \sigma_n, -1)$$

as required. □

Let $\Omega \subset \mathbf{C}^*$ be the multiplicative subgroup of roots of unity, and let

$$\Omega(d) = \{ \omega \in \Omega : \text{ord}(\omega) = d \}.$$

Then $x^n + 1 = \prod_{d|2n, d/n} c_d(x)$ where $c_d(x)$ is the cyclotomic polynomial

$$c_d(x) = \prod_{\lambda \in \Omega(d)} (x - \lambda).$$

It follows that

$$\mathbf{Q}\langle n \rangle \cong \prod_{d|2n, d/n} \mathbf{Q}(d)$$

where $\mathbf{Q}(d) = \mathbf{Q}[x]/(c_d(x))$. Under the isomorphism $\mathbf{Q}[C_n] \cong \mathbf{Q}[x]/(x^n - 1) \cong \prod_{d|n} \mathbf{Q}(d)$ the canonical involution $\hat{} : \mathbf{Q}[C_n] \rightarrow \mathbf{Q}[C_n]$ induces an involution $c_d : \mathbf{Q}(d) \rightarrow \mathbf{Q}(d)$ which is the identity for $d = 1, 2$, and complex conjugation otherwise; we obtain

Proposition 5.2. *For each $n \geq 2$, there is an algebra isomorphism*

$$\mathbf{Q}[Q_{4n}] \cong \mathbf{Q}[D_{2n}] \times \prod_{d|2n, d/n} \mathcal{C}_2(\mathbf{Q}(d), c, -1).$$

Put $\zeta_d = \cos(\frac{2\pi}{d}) + i \sin(\frac{2\pi}{d})$; the fixed field of $\mathbf{Q}(d)$ under complex conjugation is $\mathbf{Q}(\mu_d)$ where $\mu_d = 2\cos(\frac{2\pi}{d})$. Put $s(d) = \sin(\frac{2\pi}{d})$. When $d \geq 3$, $\mathcal{C}_2(\mathbf{Q}(d), c, -1)$ is a free module of rank 4 over $\mathbf{Q}(\mu_d)$. As a basis over $\mathbf{Q}(\mu_d)$ we may take $1 = X^0$; $i = (\zeta_d - \bar{\zeta}_d)$; $j = X^1$; $k = (\zeta_d - \bar{\zeta}_d)X^1$. Noting that $(\zeta_d - \bar{\zeta}_d)^2 = -4s(d)^2$, we check easily that $ij = -ji = k$ and $i^2 = -4s(d)^2$; $j^2 = -1$, so that

Proposition 5.3. *For any $d \geq 3$*

$$\mathcal{C}_2(\mathbf{Q}(d), c, -1) \cong \left(\frac{-4s(d)^2, -1}{\mathbf{Q}(\mu_d)} \right).$$

For $d \geq 3$, the rational division algebra $\left(\frac{-4s(d)^2, -1}{\mathbf{Q}(\mu_d)} \right)$ has the property that

$$\left(\frac{-4s(d)^2, -1}{\mathbf{Q}(\mu_d)} \right) \otimes_{\mathbf{Q}} \mathbf{R} \cong \underbrace{\mathbf{H} \times \cdots \times \mathbf{H}}_{\nu(d)}.$$

As $\mathcal{C}_2(\mathbf{Q}(2), c, -1)$ is isomorphic to the field $\mathbf{Q}(i) = \mathbf{Q}\sqrt{-1}$, the factors $\mathcal{C}_2(\mathbf{Q}(d), c, -1)$ of $\mathbf{Q}[Q_{4n}]$ are all small; from (5.2), it follows that $\mathbf{Q}[Q_{4n}]_{\text{big}} \cong \mathbf{Q}[D_{2n}]_{\text{big}}$.

However, the factor $\left(\frac{-4s(2n)^2, -1}{\mathbf{Q}(\mu_{2n})} \right)$ of $\mathbf{Q}[Q_{4n}]$ contains a copy of the unit group of $\mathbf{Z}[\mu_{2n}]$, and so contains an infinite free abelian group whenever $n \geq 4$. Thus the virtual cohomological dimension of $U(\mathbf{Q}[Q_{4n}])$ is in general greater than that of $U(\mathbf{Q}[D_{2n}])$, and the converse statement to Theorem I is false.

REFERENCES

- [1] A. A. Albert; Involutorial simple algebras and real Riemann matrices: Ann. of Math. 36 (1935) 886 - 964.
- [2] S.A. Amitsur; Finite subgroups of division rings: Trans. Amer. Math. Soc. 80 (1955) 361 - 386. MR **17**:577c
- [3] R. Bieri and B. Eckmann; Groups with homological duality generalising Poincaré Duality: Invent. Math. 20 (1973) 103 - 124. MR **49**:5204
- [4] A. Borel; Density and maximality of arithmetic subgroups: J. Reine Angew. Math. 224 (1966) 78-89. MR **34**:5824
- [5] A. Borel; Linear algebraic groups: Benjamin, New York 1969. MR **40**:4273
- [6] A. Borel; Introduction aux groupes arithmétiques: Hermann, Paris 1969. MR **39**:5577
- [7] A. Borel and Harish-Chandra; Arithmetic subgroups of algebraic groups: Ann. of Math. 65 (1962) 485-535. MR **26**:5081
- [8] A. Borel and J.P. Serre; Corners and arithmetic groups: Comment. Math. Helv. 48 (1973) 436-491. MR **52**:8337
- [9] K.L. Fields; On the Brauer-Speiser Theorem: Bull. A.M.S. 77 (1971) 223. MR **42**:3192
- [10] F.E.A. Johnson; On the existence of irreducible discrete subgroups in isotypic Lie groups of classical type: Proc. L.M.S. 56 (1988) 51 - 77. MR **89f**:22017
- [11] F.E.A. Johnson; On the uniqueness of arithmetic structures: Proc. Roy. Soc. Edin. 124A (1994) 1037 - 1044. MR **95h**:22013
- [12] F.E.A. Johnson; Linear properties of poly-Fuchsian groups: Collectanea Math. 45, 2 (1994) 183-203. MR **95m**:20030
- [13] S.P. Kerckhoff; The Nielsen realisation problem: Ann. of Math. 117 (1983) 235 - 265. MR **85e**:32029
- [14] G. D. Mostow; Strong rigidity of locally symmetric spaces: Annals of Mathematics Studies no. 78. Princeton University Press 1974. MR **52**:5874

- [15] G. Margulis; Discrete subgroups of semisimple Lie groups: Ergebnisse der Math. 3 Folge, Bd. 17. Springer-Verlag, Berlin (1991). MR **92h**:22021
- [16] V. Platonov and A. Rapinchuk: Algebraic groups and number theory. Academic Press (1994). MR **95b**:11039
- [17] M.S. Raghunathan; Discrete subgroups of Lie groups: Ergebnisse der Math. no. 68. Springer-Verlag (1972). MR **58**:22394a
- [18] J.P. Serre; Cohomologie Galoisienne: Springer Lecture Notes 5 (1965). MR **34**:1328
- [19] G. Shimura; On analytic families of polarised abelian varieties and automorphic function: Ann. of Math. 78 (1963) 149 - 192. MR **27**:5934
- [20] J.R. Stallings; On torsion free groups with infinitely many ends: Ann. of Math. 88 (1968) 312-334. MR **37**:4153

DEPARTMENT OF MATHEMATICS, UNIVERSITY COLLEGE LONDON, GOWER STREET, LONDON WC1E 6BT, UNITED KINGDOM

E-mail address: feaj@math.ucl.ac.uk