Journal of Algebra 347 (2011) 60–68

Contents lists available at SciVerse ScienceDirect

Journal of Algebra

www.elsevier.com/locate/jalgebra

Subgroup separability in integral group rings ☆

Ángel del Río [a,*], Manuel Ruiz Marín [b], Pavel Zalesskii [c]

[a] Departamento de Matemáticas, Universidad de Murcia, Murcia 30100, Spain
[b] Departamento de Métodos Cuantitativos e Informáticos, Universidad Politécnica de Cartagena, C/ Real 3, 30201 Cartagena, Spain
[c] Departamento de Matemática, Universidade de Brasília, 70.910-900, Brasilia, DF, Brazil

ARTICLE INFO

Article history:
Received 11 March 2011
Available online 1 October 2011
Communicated by Nicolás Andruskiewitsch

MSC:
16S34
20C05
16U60

Keywords:
Group rings
Groups of units
Subgroup separable groups

ABSTRACT

We give a list of finite groups containing all finite groups G such that the group of units $\mathbb{Z}G^*$ of the integral group ring $\mathbb{Z}G$ is subgroup separable. There are only two types of these groups G for which we cannot decide whether $\mathbb{Z}G^*$ is subgroup separable, namely the central product $Q_8 Y D_8$ and $Q_8 \times C_p$ with p prime and $p \equiv -1 \bmod (8)$.

A group Γ is said to be subgroup separable if for every finitely generated subgroup H of Γ and $g \in \Gamma \setminus H$ there exists a subgroup of finite index K of Γ such that $g \notin KH$. In other words Γ is subgroup separable if every finitely generated subgroup of Γ is closed in the profinite topology of Γ (i.e. the topology generated by normal subgroups of finite index). The importance of subgroup separability has long been recognized, both in group theory and topology. This powerful property has attracted a good deal of attention in the last few years, largely motivated by questions which arise in low dimensional topology (see [28], and [3] for example). The first author who observed the importance of the subgroup separability property was Mal'cev: he noticed that a subgroup separable finitely presented group has solvable generalized word problem. It is clear that subgroup separability

☆ The first and second authors have been partially supported by the Ministerio de Ciencia y Tecnología of Spain and Fundación Séneca of Murcia. The third author is partially supported by CNPq.

* Corresponding author.
E-mail addresses: adelrio@um.es (Á. del Río), manuel.ruiz@upct.es (M.R. Marín), pz@mat.unb.br (P. Zalesskii).

0021-8693/$ – see front matter © 2011 Elsevier Inc. All rights reserved.
doi:10.1016/j.jalgebra.2011.09.012

of a group indicates that its profinite topology is strong. For arithmetic groups the meaning of the profinite topology being strong is defined concretely by means of the congruence subgroup property. It is known that the congruence subgroup property for non-polycyclic arithmetic groups implies non-subgroup separability.

There are few examples of non-abelian groups that are known to be subgroup separable. We give a list of arithmetic groups known to have this property, since it is relevant to the subject of this paper. M. Hall [10] provided the first non-trivial examples by proving that free groups are subgroup separable. R.G. Burns [5] and N.S. Romanovskii [26] showed that a free product of subgroup separable groups is subgroup separable. These results were all proved using algebraic methods. A more topological approach was developed by J. Hempel in [11], J.R. Stallings in [30] and P. Scott in [28]. Scott used hyperbolic geometry to prove that surface groups are subgroup separable. More recently, D.D. Long and A.W. Reid [17] adapted Scott's approach to show that geometrically finite subgroups of certain hyperbolic Coxeter groups are subgroup separable. In fact a combination of the Agol, Long and Reid results [2,3] proves subgroup separability of Bianchi groups (see Theorem 3.4 in [18]) and so for all non-uniform arithmetic lattices.

In this paper we consider the problem of classifying finite groups G such that $\mathbb{Z}G^*$, the group of units of the integral group ring $\mathbb{Z}G$, is subgroup separable. To this end, we first prove that $\mathbb{Z}G^*$ is subgroup separable if and only if the simple components of the rational group algebra $\mathbb{Q}G$ satisfy some special conditions. To classify the finite groups G with such rational group algebra we use firstly some representation theory techniques and secondly some results of Jespers and Leal [12,13] and Gow and Huppert [7,8] on simple components of rational group algebras. Throughout the paper we will need to compute the Wedderburn decomposition of $\mathbb{Q}G$ for some finite groups G. The reader can check these computations using a method introduced in [22] or the GAP package Wedderga [4,9].

We start introducing the basic notation.

The group of units of a ring R is denoted by R^*. We will use ζ_n to denote a complex primitive n-th root of unity.

The commutator subgroup of a group G is denoted by G'. If $x, y \in G$ then $x^y = y^{-1}xy$ and $(x, y) = x^{-1}y^{-1}xy$. The cyclic group of order n is denoted by C_n. We also use $\langle x\rangle_n$ to denote a cyclic group of order n generated by x. By D_{2n} we denote the dihedral group of order $2n$ and by Q_{4n} the quaternion group of order $4n$. The following finite groups will play an important role in the paper:

$$\begin{aligned}
D^+_{2^{n+2}} &= \langle a\rangle_{2^{n+1}} \rtimes \langle b\rangle_2, \quad \text{with } ba = a^{2^n+1}b;\\
D^-_{2^{n+2}} &= \langle a\rangle_{2^{n+1}} \rtimes \langle b\rangle_2, \quad \text{with } ba = a^{2^n-1}b;\\
\mathcal{D} &= \bigl\langle a, b, c \bigm| ca = ac,\ cb = bc,\ a^2 = b^2 = c^4 = 1,\ ba = c^2ab\bigr\rangle;\\
\mathcal{D}^+ &= \bigl\langle a, b, c \bigm| ca = ac,\ cb = bc,\ a^4 = b^2 = c^4 = 1,\ ba = ca^3b\bigr\rangle.
\end{aligned}$$

We also need the central product $D_8 Y Q_{2^n}$ of D_8 and Q_{2^n}, i.e. $D_8 Y Q_{2^n} = (D_8 \times Q_{2^n})/\langle (z_1, z_2)\rangle$, where z_1 and z_2 are generators of the center of D_8 and Q_{2^n} respectively. Recall that a non-abelian group G is said to be Hamiltonian if every subgroup of G is normal in G. The finite Hamiltonian groups are the groups of the form $Q_8 \times C_2^n \times A$ with A a finite abelian group of odd order [25, 5.3.7].

If F is a field and a, b are non-zero elements of F then $(\frac{a,b}{F})$ denotes the quaternion algebra $F[i, j \mid i^2 = a,\ j^2 = b,\ ji = -ij]$. The Hamiltonian quaternion algebra $(\frac{-1,-1}{F})$ is denoted by $\mathbb{H}(F)$. Recall that a quaternion algebra $(\frac{a,b}{F})$ over a number field F is totally definite if F is a totally real field such that a, b are totally negative (i.e. $\sigma(F) \subseteq \mathbb{R}$ and $\sigma(a)$ and $\sigma(b)$ are negative for every homomorphism $\sigma : F \to \mathbb{C}$).

Let A be a finite dimensional semisimple rational algebra and R an order in A. Hence $A \cong A_1 \times \cdots \times A_n$ with $A_1, \ldots, A_n$ simple algebras. Such an expression is called the Wedderburn decomposition of A and the factors A_i are called the simple components of A. The following Wedderburn decompositions can be found in [6, pp. 161–163], [29, Lemma 20.4] or [12]:

$$\begin{aligned}
\mathbb{Q}C_n &\cong \bigoplus_{d|n} \mathbb{Q}(\zeta_d),\\
\mathbb{Q}D_{2n} &\cong 2\mathbb{Q}\big(D_{2n}/D_{2n}'\big) \oplus \bigoplus_{2<d|n} M_2\big(\mathbb{Q}\big(\zeta_d+\zeta_d^{-1}\big)\big),\\
\mathbb{Q}Q_{2^n} &\cong \mathbb{Q}D_{2^{n-1}} \oplus \mathbb{H}\big(\mathbb{Q}\big(\zeta_{2^{n-1}}+\zeta_{2^{n-1}}^{-1}\big)\big),\\
\mathbb{Q}D_{16}^{-} &\cong 4\mathbb{Q} \oplus M_2(\mathbb{Q}) \oplus M_2\big(\mathbb{Q}(\sqrt{-2})\big),\\
\mathbb{Q}D_{16}^{+} &\cong 4\mathbb{Q} \oplus 2\mathbb{Q}(i) \oplus M_2\big(\mathbb{Q}(i)\big),\\
\mathbb{Q}\mathcal{D} &\cong 8\mathbb{Q} \oplus M_2\big(\mathbb{Q}(i)\big),\\
\mathbb{Q}\mathcal{D}^{+} &\cong 4\mathbb{Q} \oplus 2\mathbb{Q}(i) \oplus 2M_2(\mathbb{Q}) \oplus 2M_2\big(\mathbb{Q}(i)\big),\\
\mathbb{Q}(D_8 Y Q_8) &\cong 16\mathbb{Q} \oplus M_2\big(\mathbb{H}(\mathbb{Q})\big).
\end{aligned} \tag{1}$$

By an order in A we mean a $\mathbb{Z}$-order in A, i.e. a subring of A with finitely generated underlying additive group and containing a basis of A over $\mathbb{Q}$. It is well known that if R and S are orders in A then $R^* \cap S^*$ has finite index in both R^* and S^* (see e.g. [29, Lemmas 4.2 and 4.6]).

We say that A is *virtually central* (*VC*) if the center of R^*, for R an order in A, has finite index in R^*. This definition does not depend on the choice of the order. If A is simple then A is VC if and only if it is either a field or a totally definite quaternion algebra [29, Lemma 21.3]. Therefore, in general, A is VC if and only if all its simple components are fields or totally definite quaternion algebras.

We now recall some elementary properties of subgroup separability. It is easy to see that abelian groups are subgroup separable and that the class of subgroup separable groups is closed for subgroups. Moreover, if Λ is a subgroup of finite index in Γ and Λ is subgroup separable then Γ is subgroup separable. This implies that if R and S are orders in a finite dimensional semisimple rational algebra then R^* is subgroup separable if and only if so is S^*. If Γ is a subgroup separable group and Ω is a finitely generated abelian group then it is known that $\Gamma \times \Omega$ is subgroup separable (see e.g. [21, Lemma 4]). However, subgroup separability fails to be preserved by many natural operations. For instance, if F is a non-abelian free group then, by a well-known result of K.A. Mikhailova [20], $F \times F$ contains a finitely generated subgroup that have undecidable membership problem (see [19, Theorem IV.4.3]). Hence $F \times F$ is not subgroup separable. So the class of subgroup separable groups is not closed under direct products.

The following proposition links subgroup separability of $\mathbb{Z}G^*$ with the Wedderburn decomposition of $\mathbb{Q}G$.

Proposition 1. *Let G be a finite group. Then $\mathbb{Z}G^*$ is subgroup separable if and only if one of the following conditions holds*:

1. *$\mathbb{Q}G$ is VC.*
2. *$\mathbb{Q}G$ has exactly one non-VC simple component A and if R is an* (*any*) *order in A then R^* is subgroup separable.*

Proof. Let $\mathbb{Q}G = A_1 \times \cdots \times A_n$ be the Wedderburn decomposition of $\mathbb{Q}G$ and let R_i be an order in A_i. As both $\mathbb{Z}G$ and $R = R_1 \times \cdots \times R_n$ are orders in $\mathbb{Q}G$, it follows that $\mathbb{Z}G^*$ is subgroup separable if and only if so is R^*.

If condition 1 holds then R^* contains a finitely generated abelian subgroup of finite index. If condition 2 holds and A_1 is the only non-VC simple component of $\mathbb{Q}G$ then R_1^* is subgroup separable and $R_2^* \times \cdots \times R_n^*$ has a finitely generated abelian subgroup H of finite index. Thus $R_1^* \times H$ is a subgroup separable subgroup of finite index in R^*. In both cases R^* is subgroup separable and hence so is $\mathbb{Z}G^*$.

Conversely, assume that $\mathbb{Z}G^*$ is subgroup separable. Then R^* is subgroup separable and hence so is each R_i^*. By Tits Alternative each R_i^* is either virtually solvable or contains a non-abelian free group.

Since the direct product of two non-abelian free groups is not subgroup separable, the number of R_i^*'s which are not virtually solvable is at most 1. If R_i^* is virtually solvable then A_i is VC [15, Theorem 2]. Therefore $\mathbb{Q}G$ has at most one non-VC simple component. □

Observe that the class of finite groups G such that $\mathbb{Z}G^*$ is subgroup separable is closed under subgroups and epimorphic images. The first is an obvious consequence of the fact that the class of subgroup separable groups is closed under subgroups and the second is a consequence of Proposition 1. We will use this throughout without specific mention.

Let $A = M_n(D)$ with D a finite dimensional division rational algebra and R an order in D. Then the group of units of an order in A is subgroup separable if and only if so is $\mathrm{GL}_n(R)$. Moreover, $\mathrm{GL}_n(R)$ contains a subgroup of finite index of the form $H \times K$ where H is a subgroup of finite index in the center of R^* and K is a subgroup of finite index in $\mathrm{SL}_n(R)$. Therefore $\mathrm{GL}_n(R)$ is subgroup separable if and only if so is $\mathrm{SL}_n(R)$. This and Proposition 1 imply that it is relevant to consider the problem of when $\mathrm{SL}_n(R)$ is subgroup separable for R an order in a finite dimensional rational division algebra D. This is, in general, a difficult problem with many known negative results and few positive ones. Most of the negative results follow from the fact that if $\mathrm{SL}_n(R)$ is subgroup separable then it does not have the Congruence Subgroup Property. In particular, if $\mathrm{SL}_n(R)$ is subgroup separable then $n \leqslant 2$ and if $n = 2$ then D is either $\mathbb{Q}$, an imaginary quadratic extension of the $\mathbb{Q}$ or a totally definite quaternion algebra over $\mathbb{Q}$ (see the Main Theorem on page 74 in [24] and also 5.6 of [23] for a short proof written for fields that is valid for division algebras as well). This proves the following lemma.

Lemma 2. *Let G be a finite group such that $\mathbb{Z}G^*$ is subgroup separable and A a non-VC simple component of $\mathbb{Q}G$. Then A is either a division algebra or isomorphic to $M_2(D)$ with D either $\mathbb{Q}$, an imaginary quadratic extension of $\mathbb{Q}$ or a totally definite quaternion algebra over $\mathbb{Q}$.*

We say that a group G is decomposable if it is the direct product of two non-trivial subgroups. Otherwise we say that G is indecomposable. Proposition 1 and Lemma 2 imply strong conditions for finite decomposable groups G such that $\mathbb{Z}G^*$ is subgroup separable.

Lemma 3. *If G is a finite non-abelian decomposable group such that $\mathbb{Z}G^*$ is subgroup separable then one of the following conditions holds*:

1. $G \cong Q_8 \times C_2^k$ *for some* $k \geqslant 1$.
2. $G \cong Q_8 \times C_n$, *with n either* 3, 4 *or prime satisfying* $n \equiv -1 \bmod (8)$.

Proof. Assume that $G = H \times K$ with H non-trivial and K non-abelian. We claim that K is Hamiltonian. Otherwise one of the simple components of $\mathbb{Q}K$ is not a division algebra and so, by Lemma 2, it is of the form $M_2(D)$ for D a division algebra. As $\mathbb{Q}H$ has at least two simple components, $\mathbb{Q}G$ has at least two simple components which are not division algebras, and hence they are not VC. This contradicts Proposition 1 and finishes the proof of the claim.

If H is non-abelian then it is also Hamiltonian, by the previous paragraph. Then G contains a subgroup isomorphic to $Q_8 \times Q_8$. As $\mathbb{Q}(Q_8 \times Q_8)$ has a simple component isomorphic to $\mathbb{H}(\mathbb{Q}) \otimes_{\mathbb{Q}} \mathbb{H}(\mathbb{Q}) \cong M_4(\mathbb{Q})$, the group $\mathbb{Z}(Q_8 \times Q_8)^*$ is not subgroup separable, by Lemma 2. This yields a contradiction. Therefore H is abelian.

Let $n > 1$. Then $\mathbb{Q}(Q_8 \times C_n)$ has a simple component isomorphic to $\mathbb{H}(\mathbb{Q}(\zeta_d))$, for every divisor d of n. This algebra is VC if and only if $d = 1$ or 2. Therefore, if $\mathbb{Z}(Q_8 \times C_n)^*$ is subgroup separable then n has at most one divisor different from 1 or 2 and hence n is either 4 or prime. The same argument shows that if $\mathbb{Z}(\mathbb{Q}_8 \times C_n \times C_m)^*$ is subgroup separable with n and m different of 1 then $n = m = 2$.

This implies that $K \cong Q_8 \times A$ with A an elementary abelian 2-group, and H is either elementary abelian 2-group or cyclic of order 4 or prime. Moreover, if $A \neq 1$ then H is elementary abelian 2-group. Thus either G satisfies condition 2 or $G = Q_8 \times C_n$ with $n = 4$ or an odd prime. Assume that $G = Q_8 \times C_n$ with n odd prime. Then one of the simple components of $\mathbb{Q}G$ is isomorphic to $\mathbb{H}(\mathbb{Q}(\zeta_n))$. If moreover $n \not\equiv -1 \bmod (8)$ then $\mathbb{H}(\mathbb{Q}(\zeta_n)) \cong M_2(\mathbb{Q}(\zeta_n))$ (see e.g. the paragraph below [16, Proposition 2.11]). By Lemma 2, $n - 1 = [\mathbb{Q}(\zeta_n) : \mathbb{Q}] \leqslant 2$ and hence $n = 3$. This finishes the proof. □

By Lemma 2, if $\mathbb{Z}G^*$ is subgroup separable then every simple component of $\mathbb{Q}G$ is either a division algebra or a two-by-two matrix ring over a division algebra. The simple components of this form, for G a nilpotent group, have been classified in [12]. We will use this in our next lemma.

Lemma 4. *Let G be a non-abelian nilpotent finite group. Let e be a primitive central idempotent of $\mathbb{Q}G$ such that $(\mathbb{Q}G)e$ is not abelian. If $\mathbb{Z}G^*$ is subgroup separable then one of the following facts holds*:

1. $Ge \cong Q_8 \times C_3$ *and* $(\mathbb{Q}G)e = M_2(\mathbb{Q}(\sqrt{-3}))$.
2. $Ge \cong Q_8 \times C_p$ *with p prime satisfying* $p \equiv -1 \mod (8)$ *and* $(\mathbb{Q}G)e = \mathbb{H}(\mathbb{Q}(\zeta_p))$.
3. $Ge \cong D_8$ *and* $(\mathbb{Q}G)e = M_2(\mathbb{Q})$.
4. $Ge \cong Q_8$ *and* $(\mathbb{Q}G)e = \mathbb{H}(\mathbb{Q})$.
5. $Ge \cong Q_{16}$ *and* $(\mathbb{Q}G)e = \mathbb{H}(\mathbb{Q}(\sqrt{2}))$.
6. $Ge \cong D_{16}^+$ *and* $(\mathbb{Q}G)e = M_2(\mathbb{Q}(i))$.
7. $Ge \cong \mathcal{D}$ *and* $(\mathbb{Q}G)e = M_2(\mathbb{Q}(i))$.
8. $Ge \cong D_8 Y Q_8$ *and* $(\mathbb{Q}G)e = M_2(\mathbb{H}(\mathbb{Q}))$.

Proof. As Ge is an epimorphic image of G, $\mathbb{Z}(Ge)^*$ is subgroup separable and $(\mathbb{Q}G)e$ is a simple component of $\mathbb{Q}G$ isomorphic to a simple component of $\mathbb{Q}(Ge)$. We separate cases depending on whether Ge is a p-group or not. The p-group case is the most involved and it is split depending on whether $\mathbb{Q}Ge$ is a division algebra, a matrix algebra over a field or a matrix algebra over a non-commutative division algebra.

If Ge is not a p-group, for some p then, by Lemma 3, $Ge \cong Q_8 \times C_p$ with p prime and either $p = 3$ or $p \equiv -1 \mod (8)$. In the first case $(\mathbb{Q}G)e \cong M_2(\mathbb{Q}(\sqrt{-3}))$ and in the second case $(\mathbb{Q}G)e \cong \mathbb{H}(\mathbb{Q}(\zeta_p))$. Therefore if Ge is not a p-group then either condition 1 or 2 holds.

Assume otherwise that Ge is a p-group for some prime p. If p is odd then, by a well-known result of Roquette [27], $(\mathbb{Q}G)e$ is an $n \times n$ matrix algebra over a field, for n a power of p, contradicting Lemma 2. Thus Ge is a 2-group and, by Lemma 2, $(\mathbb{Q}G)e$ is either a division algebra or a two-by-two matrix algebra over a division algebra. Then Ge and $(\mathbb{Q}G)e$ satisfy one of the conditions of [12, Theorem 2.2].

If $(\mathbb{Q}G)e$ is a division algebra then Ge is isomorphic to Q_{2^n} and $(\mathbb{Q}G)e = \mathbb{H}(\mathbb{Q}(\zeta_{2^{n-1}} + \zeta_{2^{n-1}}^{-1}))$. Then $D_{2^{n-1}}$ is an epimorphic image of Ge. Hence $\mathbb{Q}G$ has a simple component isomorphic to $M_2(\mathbb{Q}(\zeta_{2^{n-1}} + \zeta_{2^{n-1}}^{-1}))$. (See Wedderburn decomposition in (1).) By Lemma 2 it follows that $\mathbb{Q}(\zeta_{2^{n-1}} + \zeta_{2^{n-1}}^{-1}) = \mathbb{Q}$ and thus $n \leqslant 4$. Therefore, in this case either condition 4 or 5 holds.

Assume that $(\mathbb{Q}G)e \cong M_2(F)$ with F a field. By [12, Theorem 2.2], Ge is isomorphic to one of the following groups: D_8, D_{16}, D_{16}^+, D_{16}^-, $\mathcal{D}$ or $\mathcal{D}^+$. By inspection of the Wedderburn decomposition of these groups (1) we observe that $\mathbb{Q}D_{16}$, $\mathbb{Q}D_{16}^-$, $\mathbb{Q}\mathcal{D}$ and $\mathbb{Q}\mathcal{D}^+$ have at least two non-VC simple components, yielding a contradiction with Proposition 1. We conclude that Ge is either D_8, D_{16}^+ or $\mathcal{D}$. Then either condition 3, 6 or 7 holds.

It remains to consider the case when $(\mathbb{Q}G)e \cong M_2(D)$ with D a non-commutative division algebra. By [12, Theorem 2.2], $D \cong \mathbb{H}(\mathbb{Q}(\zeta_{2^{n-1}} + \zeta_{2^{n-1}}^{-1}))$ and $G = \langle H, g\rangle$, with H a subgroup of index 2 in G, and H contains a non-trivial normal subgroup N such that $N \cap N^g = 1$ and $H/N \cong Q_{2^n}$. (Observe that case (3.a) in [12] is in fact contained in case (3.b) because if $D_8 = \langle a, b\rangle$, with a of order 4, $H = \langle b, Q_{2^n}\rangle$ and $N = \langle b\rangle$ then H and N satisfy condition (3.b) for $Ge = D_8 Y Q_{2^n}$.) By Lemma 2, $\mathbb{Q}(\zeta_{2^{n-1}} + \zeta_{2^{n-1}}^{-1}) = \mathbb{Q}$ and hence $n = 3$. Since $N \cap N^g = \{1\}$ and N is a normal subgroup of H, $\langle N, N^g\rangle = N \times N^g \subseteq H$ and $(N \times N^g)/N$ is a non-trivial subgroup of $H/N \cong Q_8$. Thus N is isomorphic to a subgroup of Q_8 and therefore its order is either 2, 4 or 8. If $|N| = 8$ then $N \times N^g$ is isomorphic to $Q_8 \times Q_8$ and its rational group algebra contains a simple component isomorphic to $M_4(\mathbb{Q})$ yielding a contradiction with Lemma 1. Thus N has order 2 or 4. We claim that N has order 2. Otherwise N is generated by an element of order 4, since so is every subgroup of order 4 of Q_8. Then $H = \langle x, a, b\rangle$ with $N = \langle x\rangle_4$, $a = x^g$, $b^2N = a^2N$ and $a^bN = a^{-1}N$. As N is normal in H and a is not central in H we have $x^b = x^{-1}$ and $a^b = a^{-1}$. Moreover $b^2 = a^2x^i$, with $i = 0, 1, 2$ or 3. As a^2 and b^2 are central in H and x is not, necessarily $i = 0$ or 2. In both cases $H/\langle b^2\rangle$ is isomorphic to $D_8 \times C_2$. This yields a contradiction with Lemma 3.

Thus $N = \langle x\rangle_2$, $|H| = 16$, $H/N \cong Q_8$ and $G = \langle H, g\rangle$ with $x^g \neq x$. This implies that H is isomorphic to either $Q_8 \times C_2$ or $\langle c\rangle_4 \rtimes \langle d\rangle_4$, with $dc = c^3 d$. Assume that H is as in the second case. Then H has 3 elements of order 2, namely c^2, d^2 and c^2d^2. Notice that c^2 is the only element of order 2 in $H' = \langle c^2\rangle$ and c^2d^2 is the only non-square element of order 2 of H. This proves that c^2, d^2 and c^2d_2 are invariant by any automorphism of H. As x is an element of order 2 of H it follows that $x^g = x$, a contradiction. Therefore $H \cong Q_8 \times C_2$. This implies that for every $a, b \in H$ with $(a, b) \neq 1$ we have $H = \langle a, b\rangle \times \langle x\rangle$, $\langle a, b\rangle \cong Q_8$ and $x^g = a^2 x$.

In the remainder of the proof we will use that D_8 is not an epimorphic image of G. Otherwise $M_2(\mathbb{Q})$ is a simple quotient of $\mathbb{Q}G$ and by assumption $M_2(\mathbb{H}(\mathbb{Q}))$ is another simple quotient of $\mathbb{Q}G$ yielding a contradiction with Proposition 1.

We claim that the order of g is either 2 or 4 and in fact we may assume that it is 4. If g is of order 8 then we may assume that $g^2 = a$. Thus, $x^g = g^4 x$ and therefore $\langle g, x\rangle$ is a normal subgroup of G isomorphic to D_{16}^+. Then $g^b = g^i x^j$ with $i = \pm 1$ or ± 3 and $j = 0$ or 1. Also $g^{-2} = a^{-1} = a^b = (g^2)^b = (g^i x^j)^2$. If $j = 0$ then $g^{-2} = g^{2i}$. Therefore $i \equiv -1 \bmod 4$ and thus $G/\langle a^2, x\rangle$ is isomorphic to D_8, a contradiction. So $j = 1$ and $g^{-2} = g^{6i}$. Therefore $i = 1$ or -3. In this case $G/\langle xg^2\rangle$ is isomorphic to D_8, again a contradiction. Then the order of g is 2 or 4. If the order of g is 2 then gx has order 4. Hence, we may assume that g has order 4 as desired.

Thus in the remainder of the proof we assume that g has order 4. Then g^2 is an element of order 2 of H which commutes with g and hence $g^2 = a^2$. The group H has three abelian subgroups of order 8, namely, $\langle a, x\rangle$, $\langle b, x\rangle$ and $\langle ab, x\rangle$. If any of these groups is not fixed by the action of g then we may assume that $a^g = b$ (changing b by a^g if needed). Then $(g, a) = b^{-1}a = ab$ and thus the quotient $G/\langle a^2, x\rangle$ is a non-abelian group of order 8 generated by two elements of order 2. Hence $G/\langle a^2, x\rangle \cong D_8$, a contradiction. So the action of g fixes the three subgroups of order 8 in H. If $\langle a\rangle$ is not normal in G then $a^g = ax$ or $a^g = a^{-1}x$. Then $a = (a^g)^g$ is equal to either $(ax)^g = axa^2x = a^{-1}$ or $(a^{-1}x)^g = axa^2x = a^{-1}$, a contradiction. This proves that every cyclic subgroup of order 4 of H is normal in G. Therefore, if $(a, g) \neq 1$ then $a^g = a^{-1}$ and hence $(ax)^g = ax$. Thus replacing a by ax if needed we may assume that $(g, a) = 1$ and similarly, one may assume that $(g, b) = 1$. Hence $G = \langle g, x\rangle Y \langle a, b\rangle = D_8 Y Q_8$ which finishes the proof of the lemma. □

Theorem 5. *Let G be a non-abelian finite group such that $\mathbb{Z}G^*$ is subgroup separable. Then G is either abelian or isomorphic to one of the following groups*:

$$D_6,\quad D_8,\quad Q_{12},\quad C_4 \rtimes C_4,\quad \mathcal{D},\quad D_{16}^+,\quad Q_{16},\quad Q_8 \times C_3,\quad Q_8 \times C_4,\quad D_8 Y Q_8,$$

$$Q_8 \times C_2^n \quad \textit{with } n \geqslant 0, \quad \textit{or}$$

$$Q_8 \times C_p \quad \textit{with p prime and } p \equiv -1 \bmod (8).$$

Proof. If G is decomposable then, by Lemma 3, G is isomorphic to either $Q_8 \times C_2^n$ (with $n \geqslant 1$), $Q_8 \times C_3$, $Q_8 \times C_4$ or $Q_8 \times C_p$ with p prime and $p \equiv -1 \bmod 8$. So in the remainder of the proof we assume that G is indecomposable. We consider cases depending on whether G is nilpotent or not.

Assume that G is nilpotent. Then, G is a p-group, because it is indecomposable and, by Lemma 4, G is a 2-group. Moreover, for every primitive central idempotent e of $\mathbb{Q}G$ such that Ge is not abelian, one of the conditions 3–8 of Lemma 4 holds. If G is Hamiltonian then G is isomorphic to Q_8. Assume that G is not Hamiltonian. If Q_{16} is not an epimorphic image of G then, by Lemma 4, every noncommutative simple quotient of $\mathbb{Q}G$ is isomorphic to either $M_2(\mathbb{Q})$, $\mathbb{H}(\mathbb{Q})$, $M_2(\mathbb{Q}(i))$ or $M_2(\mathbb{H}(\mathbb{Q}))$ and only one simple component is not a division algebra, by Proposition 1. The non-abelian finite groups G satisfying this condition have been classified in [13, Theorem 1]. Using this result we deduce that G is isomorphic to either D_8, $C_4 \rtimes C_4$, $\mathcal{D}$, D_{16}^+ or $D_8 Y Q_8$.

Assume otherwise that Q_{16} is an epimorphic image of G. Then D_8 is also an epimorphic image of G and therefore $M_2(\mathbb{Q})$ is isomorphic to a simple component of $\mathbb{Q}G$. Then the remaining simple components of $\mathbb{Q}G$ are division algebras, by Proposition 1. By Lemma 4, every simple quotient of $\mathbb{Q}G$ is isomorphic to either $M_2(\mathbb{Q})$, $\mathbb{H}(\mathbb{Q})$ or $\mathbb{H}(\mathbb{Q}(\sqrt{2}))$. Then G satisfies condition (3) of [14, Theorem 1.3]. Thus G is one of the groups (a)–(g) listed in that result, because G is non-abelian indecomposable 2-group and the groups (h) and (i) in the list are not 2-groups. The groups (a)–(f) have exponent 4, while the exponent of G is at least 8 because Q_{16} is an epimorphic image of G. Thus G is isomorphic to the group H_n given by the presentation $\langle x, y_1, \dots, y_n \mid x^4 = x^2 y_i^4 = y_i^2 [x, y_i] = [y_i, y_j] = 1\rangle$ for some $n \geqslant 1$. As $H_n/\langle y_2^2, \dots, y_n^2\rangle \cong Q_{16} \times C_2^{n-1}$ does not satisfy the conditions of Lemma 3 if $n > 1$, we deduce that $n = 1$. We conclude that $G \cong Q_{16}$. This finishes the proof for the nilpotent case.

Assume that G is non-nilpotent. By Proposition 1, every simple component of $\mathbb{Q}G$ is either a division algebra or a two-by-two matrix ring over a division algebra. In other words the reduced degree over $\mathbb{Q}$ of each irreducible character of G is either 1 or 2. This implies that G contains a nilpotent subgroup of index 2, by [7,8]. Hence $G = N_{2'} \rtimes G_2$ where $N_{2'}$ is a nilpotent $2'$-group and G_2 is a 2-group such that $N_2 = \mathrm{Cen}_{G_2}(N_{2'})$ has index 2 in G_2. Therefore, there is a non-trivial automorphism σ of $N_{2'}$ of order 2, such that for every $x \in G_2$, the action φ_x of x on $N_{2'}$ by conjugation is trivial if $x \in N_2$ and otherwise $\varphi_x = \sigma$.

We claim that G_2 is cyclic. Assume first that G_2 is abelian and write $G_2 = \langle x_1\rangle_{n_1} \times \cdots \times \langle x_k\rangle_{n_k}$ with $2 \leqslant n_1 \leqslant n_2 \leqslant \cdots \leqslant n_k$. Let i be minimum with $x_i \notin N_2$. By replacing, x_j by $x_j x_i$, for each $j > i$ such that $x_j \notin N$, we may assume that $x_j \in N_2$ for every $j \neq i$. Then $G = (N_{2'} \rtimes \langle x_i\rangle) \times \prod_{j \neq i} \langle x_j\rangle$. As, by assumption, G is indecomposable we deduce that $k = 1$, as wanted. Assume otherwise that G_2 is non-abelian. By the nilpotent case G_2 is one of the 2-groups listed in the theorem. On the other hand G_2' is a normal subgroup of G and $G/G_2' \cong N_{2'} \rtimes (G_2/G_2')$. By the abelian case, G_2/G_2' is cyclic. This yields a contradiction, since none of the 2-groups listed in the theorem satisfies this condition.

Hence $G_2 = \langle x\rangle$ for some x, of order 2^n, say. Now we claim that every subgroup of $N_{2'}$ is normal in G. Otherwise there is $a \in N_{2'}$ of order q, an odd prime power, such that $b = a^x \notin \langle a\rangle$. This implies that $\langle ab, x^2\rangle$ is contained in the center of G and $\langle a, b, x\rangle/\langle ab, x^2\rangle$ is isomorphic to D_{2q_1}, for q_1 a divisor of q different than 1. However $\mathbb{Q}D_{2q_1}$ has a simple component isomorphic to $M_2(\mathbb{Q}(\zeta_{q_1} + \zeta_{q_1}^{-1}))$. This implies that $\mathbb{Q}(\zeta_{q_1} + \zeta_{q_1}^{-1}) = \mathbb{Q}$ and hence $q_1 = 3$. Thus $a^3 = (ab)^i = a^i b^i$ for some integer i. Therefore $b^i = a^{3-i}$. As $b \notin \langle a\rangle$, we have $i = 3m$ for some m. Then $a^{3(1-m)} = b^{3m}$. As a and b have the same order, m is coprime with 3. Thus $b^3 \in \langle a^3\rangle$. This implies that $\langle a^3, x^2\rangle$ is normal in G and $H = \langle a, b, x\rangle/\langle a^3, x^2\rangle \cong (\langle \bar{a}\rangle_3 \times \langle \bar{b}\rangle_3) \rtimes \langle \bar{x}\rangle_2$. The Wedderburn decomposition of $\mathbb{Q}H$ is

$$\mathbb{Q}H = 2\mathbb{Q} \oplus 2\mathbb{Q}(\sqrt{-3}) \oplus M_2(\mathbb{Q}) \oplus M_2\big(\mathbb{Q}(\sqrt{-3})\big).$$

By Proposition 1, $\mathbb{Z}H^*$ is not subgroup separable, a contradiction. This finishes the proof of the claim.

Thus every subgroup of $N_{2'}$ is normal in G. Therefore, if $a \in N_{2'}$ is an element of order q non-commuting with x, then $\langle a, x\rangle/\langle x^2\rangle \cong D_{2q}$. As in the previous paragraph this implies that $q = 3$. Using that G is indecomposable it is now easy to prove that $N_{2'} = C_3$. Therefore $G = C_3 \rtimes C_{2^n}$ with $a^x = a^{-1}$. If $n \geqslant 3$ then $K = C_3 \rtimes C_8$ is isomorphic to an epimorphic image of G. The Wedderburn decomposition of $\mathbb{Q}K$ is

$$\mathbb{Q}K = 2\mathbb{Q} \oplus \mathbb{Q}(i) \oplus \mathbb{Q}(\zeta_8) \oplus M_2(\mathbb{Q}) \oplus \left(\frac{-1, -3}{\mathbb{Q}}\right) \oplus \left(\frac{i, -3}{\mathbb{Q}(i)}\right).$$

By Proposition 1, $\mathbb{Z}K^*$ is not subgroup separable, a contradiction. Therefore G is isomorphic to either $C_3 \rtimes C_2 \cong D_6$ or $C_3 \rtimes C_4 = Q_{12}$ which finishes the proof of the theorem. □

To obtain a complete classification of the finite groups G such that $\mathbb{Z}G^*$ is subgroup separable one should decide which of the groups appearing in Theorem 5 satisfy the conditions of Proposition 1. If $G = Q_8 \times C_2^n$, with $n \geqslant 0$, then $\mathbb{Z}G^*$ is finite and hence $\mathbb{Z}G^*$ is subgroup separable. For the remaining groups in Theorem 5, $\mathbb{Q}G$ has precisely one non-VC component. The following table classifies the groups appearing in Theorem 5, other than $Q_8 \times C_2$, according to the non-VC component A. The third column contains an order R in the non-VC component.

G	A	R
D_6, D_8, $C_4 \rtimes C_4$, Q_{16}	$M_2(\mathbb{Q})$	$M_2(\mathbb{Z})$
$Q_8 \times C_3$	$M_2(\mathbb{Q}(\sqrt{-3}))$	$M_2(\mathbb{Z}[\sqrt{-3}])$
$Q_8 \times C_4$, $\mathcal{D}$, D_{16}^+	$M_2(\mathbb{Q}(i))$	$M_2(\mathbb{Z}[i])$
$D_8 Y Q_8$	$M_2(\mathbb{H}(\mathbb{Q}))$	$M_2(\mathbb{H}(\mathbb{Z}))$
$Q_8 \times C_p$, with p prime and $p \equiv -1 \bmod (8)$	$\mathbb{H}(\mathbb{Q}(\zeta_p))$	$\mathbb{H}(\mathbb{Z}[\zeta_p])$

Let G be one of the groups in the previous table and let R be the order displayed in the third column of the table. By Proposition 1, $\mathbb{Z}G^*$ is subgroup separable if and only if R^* is subgroup separable. This has been settled for the groups in the first three rows. Indeed, it is well known that $\mathrm{GL}_2(\mathbb{Z})$ contains a non-abelian free subgroup of finite index and it has been proved recently that $\mathrm{GL}_2(\mathbb{Z}[\sqrt{-3}])$ and $\mathrm{GL}_2(\mathbb{Z}[i])$ are subgroup separable (see [18, Theorem 3.4]). So we have the following positive result.

Theorem 6. *If G is one of the following groups*

$$D_6, \quad D_8, \quad Q_{12}, \quad C_4 \rtimes C_4, \quad \mathcal{D}, \quad D_{16}^+, \quad Q_{16}, \quad Q_8 \times C_3, \quad Q_8 \times C_4 \quad \textit{or}$$
$$Q_8 \times C_2^n \quad (\textit{with } n \geqslant 0)$$

then $\mathbb{Z}G^*$ is subgroup separable.

To decide whether $\mathbb{Z}G^*$ is subgroup separable or not, for G one of the groups in the last two rows of the table, one should decide whether R^* is subgroup separable. Thus to complete the classification of finite groups G with $\mathbb{Z}G^*$ subgroup separable it remains to decide if $\mathrm{GL}_2(\mathbb{H}(\mathbb{Z}))$ is subgroup separable and for which prime integers p with $p \equiv -1 \bmod (8)$, the group of units of $\mathbb{H}(\mathbb{Z}[\zeta_p])$ is subgroup separable. In fact $\mathrm{GL}_2(\mathbb{H}(\mathbb{Z}))$ is subgroup separable if and only if so is $\mathrm{SL}_2(\mathbb{H}(\mathbb{Z}))$. Similarly, $\mathbb{H}(\mathbb{Z}[\zeta_p])^*$ is subgroup separable if and only if so is $\mathrm{SL}_1(\mathbb{H}(\mathbb{Z}[\zeta_p]))$.

A presentation by generators and relations for $\mathrm{SL}_2(\mathbb{H}(\mathbb{Z}))$ has been obtained in [1]. Unfortunately the subgroup separability question for this groups does not seem to follow from the presentation. Note that $\mathrm{SL}_2(\mathbb{H}(\mathbb{Z}))$ does not posses the congruence subgroup property, since it contains a subgroup of finite index that maps onto a free non-abelian group. However, it is not known whether failure of the congruence subgroup property implies subgroup separability for arithmetic groups (virtually indecomposable in direct products).

In the remaining cases, $\mathrm{SL}_1(\mathbb{H}(\mathbb{Z}[\zeta_p]))$ with p prime with $p \equiv -1 \bmod (8)$, the congruence subgroup property is unknown and the structure of the group not-understood.

References

[1] S.I. Adian, I.G. Lysionok, J.G. Mennicke, Defining relations and the algebraic structure of the group SL_2 over integral Hamilton quaternions, Internat. J. Algebra Comput. 7 (1) (1997) 1–24.

[2] I. Agol, Criteria for virtual fibering, J. Topol. 1 (2) (2008) 269–284.

[3] I. Agol, I.D.D. Long, A.W. Reid, The Bianchi groups are separable on geometrically finite subgroups, Ann. of Math. (2) 153 (3) (2001) 599–621.

[4] O. Broche Cristo, A. Konovalov, A. Olivieri, G. Olteanu, Á. del Río, Wedderga – Wedderburn Decomposition of Group Algebras, Version 4.0, http://www.um.es/adelrio/wedderga.htm, 2006.

[5] R.G. Burns, On finitely generated subgroups of free products, J. Aust. Math. Soc. 12 (1971) 358–364.

[6] C.W. Curtis, I. Reiner, Methods of Representation Theory, vol. 1, Interscience, New York, 1981.

[7] R. Gow, B. Huppert, Degree problems of representation theory over arbitrary fields of characteristic 0, J. Reine Angew. Math. 381 (1987) 136–147.

[8] R. Gow, B. Huppert, Degree problems of representation theory over arbitrary fields of characteristic 0. Part 2: Groups which have only two reduced degrees, J. Reine Angew. Math. 389 (1988) 122–132.

[9] The GAP Group, GAP – Groups, Algorithms, and Programming, Version 4.4, http://www.gap-system.org, 2006.

[10] M. Hall Jr., Subgroups of finite index in free groups, Canad. J. Math. 1 (1949) 187–190.

[11] J. Hempel, 3-Manifolds, Ann. of Math. Stud., vol. 86, Princeton University Press, 1976.

[12] E. Jespers, G. Leal, Degree 1 and 2 representations of nilpotent groups and applications to units of group rings, Manuscripta Math. 86 (4) (1995) 479–498.

[13] E. Jespers, G. Leal, Free products of abelian groups in the unit group of integral group rings, Proc. Amer. Math. Soc. 126 (5) (1998) 1257–1265.
[14] E. Jespers, Á. del Río, A structure theorem for the unit group of the integral group ring of some finite groups, J. Reine Angew. Math. 521 (2000) 99–117.
[15] E. Kleinert, Two theorems on units of orders, Abh. Math. Semin. Univ. Hambg. 70 (2000) 355–358.
[16] T.Y. Lam, The Algebraic Theory of Quadratic Forms, Benjamin/Cumming, 1980.
[17] D.D. Long, A.W. Reid, On subgroup separability in hyperbolic Coxeter groups, Geom. Dedicata 87 (2001) 245–260.
[18] D.D. Long, A.W. Reid, Subgroup separability and virtual retractions of groups, Topology 47 (3) (2008) 137–159.
[19] R.C. Lyndon, P.E. Schupp, Combinatorial Group Theory, Springer-Verlag, Berlin, 1977.
[20] K.A. Mikhailova, The occurrence problem for direct products of groups, Dokl. Akad. Nauk SSSR 119 (1958) 1103–1105.
[21] V. Metaftsis, E. Raptis, On the profinite topology of right-angled Artin groups, J. Algebra 320 (3) (2008) 1174–1181.
[22] A. Olivieri, Á. del Río, J.J. Simón, On monomial characters and central idempotents of rational group algebras, Comm. Algebra 32 (4) (2004) 1531–1550.
[23] G. Prasad, A.S. Rapinchuk, Developments on the congruence subgroup problem after the work of Bass, Milnor and Serre, in: H. Bass, T.Y. Lam (Eds.), Collected Papers of J. Milnor, vol. 5, Amer. Math. Soc., 2010, pp. 307–325.
[24] M.S. Raghunathan, On the congruence subgroup problem II, Invent. Math. 85 (1) (1986) 73–117.
[25] D.J.S. Robinson, A Course in the Theory of Groups, Springer-Verlag, 1982.
[26] N.S. Romanovskii, On the residual finiteness of free products with respect to subgroups, Izv. Akad. Nauk SSSR Ser. Mat. 33 (1969) 1324–1329.
[27] P. Roquette, Realisierung von Darstellungen endlicher nilpotenter Gruppen, Arch. Math. (1958) 241–250.
[28] P. Scott, Subgroups of surface groups are almost geometric, J. London Math. Soc. (2) 17 (1978) 555–565.
[29] S.K. Sehgal, Units in Integral Group Rings, Longman Scientific and Technical, Essex, 1993.
[30] J.R. Stallings, Topology of finite graphs, Invent. Math. 71 (1983) 551–565.