MULTIPLICATIVE JORDAN DECOMPOSITION IN GROUP RINGS WITH A WEDDERBURN COMPONENT OF DEGREE 3

Chia-Hsin Liu[1]

Department of Mathematics,
National Taiwan Normal University,
Taipei, Taiwan, R.O.C.
chliu@math.ntnu.edu.tw

D. S. Passman[2]

Department of Mathematics,
University of Wisconsin-Madison,
Madison, Wisconsin 53706, USA
passman@math.wisc.edu

Abstract

If G is a finite group whose integral group ring $\mathbb{Z}[G]$ has the multiplicative Jordan decomposition property, then it is known that all Wedderburn components of the rational group ring $\mathbb{Q}[G]$ have degree at most 3. While degree 3 components can occur, we prove here that if they do, then certain central units in $\mathbb{Z}[G]$ cannot exist. With this, we are able to greatly simplify the argument that characterizes those 3-groups with integral group ring having MJD. Furthermore, we show that if G is a nonabelian semidirect product of the form $C_p \rtimes C_{3^k}$, with prime $p > 7$ and with the cyclic 3-group acting like a group of order 3, then $\mathbb{Z}[G]$ does not have MJD.

Keywords: integral group ring, multiplicative Jordan decomposition, 3-group, Z-group, Wedderburn component, central unit.
2000 MSC: 16S34, 20D15.

1. Introduction

Let $\mathbb{Q}[G]$ denote the rational group algebra of the finite group G. Since $\mathbb{Q}$ is a perfect field, every element a of $\mathbb{Q}[G]$ has a unique additive Jordan decomposition $a = a_s + a_n$, where a_s is a semisimple element and where a_n commutes with a_s and is nilpotent. If a is a unit, then a_s is also invertible

[1]Research supported in part by an NSC grant.
[2]Research supported in part by an NSA grant.

and $a = a_s(1 + a_s^{-1}a_n)$ is a product of a semisimple unit a_s and a commuting unipotent unit $a_u = 1 + a_s^{-1}a_n$. This is the unique multiplicative Jordan decomposition of a. Following [AHP] and [HPW], we say that $\mathbb{Z}[G]$ has the multiplicative Jordan decomposition property (MJD) if for every unit a of $\mathbb{Z}[G]$, its semisimple and unipotent parts are both contained in $\mathbb{Z}[G]$. For simplicity, we say that G satisfies MJD if its integral group ring $\mathbb{Z}[G]$ has that property.

More generally, let F be an algebraic number field and let $R = \mathcal{O}_F$ be its ring of algebraic integers. As above, we say that $R[G]$ has the multiplicative Jordan decomposition property if for every unit $a \in R[G]$, its unique semisimple part a_s and unipotent part a_u, constructed in $F[G]$, are contained in $R[G]$.

If G is abelian, then every element of $F[G]$ is semisimple and hence $R[G]$ has MJD. If G is a Hamiltonian 2-group, then every element of $\mathbb{Q}[G]$ is semisimple and hence $\mathbb{Z}[G]$ has MJD.

In the non-Dedekind case, it appears that the MJD property is relatively rare. Indeed, the papers [AHP] and [HPW] have shown that $R[G]$ and $F[G]$ must be quite restrictive. For example, we have the following, with part (i) from [AHP, Theorem 4.1] and part (ii) from [HPW, Corollary 9]. Actually, part (ii) is only stated for $\mathbb{Z}$ and $\mathbb{Q}$, but the proof for R and F is identical.

Theorem 1.1. *Let R be the ring of integers in the algebraic number field F and assume that $R[G]$ has the multiplicative Jordan decomposition property.*

i. If the matrix ring $\mathbf{M}_n(D)$ over the F-division algebra D is a Wedderburn component of $F[G]$, then $n \leq 3$.

ii. If z is a nilpotent element of $R[G]$ and e is a central idempotent of $F[G]$, then $ze \in R[G]$.

Furthermore, using numerous clever arguments, paper [HPW] was able to determine all nonabelian 2-groups that satisfy MJD. Specifically, these are the two nonabelian groups of order 8, five groups of order 16, four groups of order 32, and only the Hamiltonian groups of larger order. Building on this work, and using variants of many of the same arguments, [LP1], [LP2] and [LP3] determined all nonabelian 3-groups satisfying MJD. These turn out to be just the two groups of order 27.

In particular, there exist groups G with MJD such that $\mathbb{Q}[G]$ has Wedderburn components of degree 3. Besides the two nonabelian groups of order 27, there is also the nonabelian semidirect product $G = C_7 \rtimes C_3$, as was shown in [A], and of course there may be others. On the other hand, the main result of this paper shows that the existence of such a component does somewhat restrict the possibility that $R[G]$ has MJD. Specifically, we prove

Theorem 1.2. *Let F be an algebraic number field, write $R = \mathcal{O}_F$, and suppose that the group algebra $F[G]$ has a Wedderburn component $W = \mathbf{M}_3(D)$ for some F-division algebra D. If $R[G]$ has a central unit whose projection to W has infinite multiplicative order, then $R[G]$ does not have MJD.*

As a consequence, we first obtain an extremely efficient proof of the characterization of 3-groups with MJD based on the approach of [L]. Next, we show that if G is 3-group and if $R[G]$ has MJD with $F \neq \mathbb{Q}$, then G must be abelian. Finally, we prove that if G is the semidirect product $C_p \rtimes C_{3^k}$, where the cyclic group C_{3^k} acts on C_p as a group of order 3, and if the prime p is not 7, then G does not have MJD. The latter is one of the few remaining families listed in [HPW, Theorem 29] whose MJD properties had been in doubt.

We close this introduction with the obvious

Lemma 1.3. *Let R and F be as above and let G be a finite group. If $R[G]$ has MJD, then $\mathbb{Z}[G]$ also has MJD.*

Proof. If a is a unit of $\mathbb{Z}[G]$, the a_s and a_u belong to $\mathbb{Q}[G]$. On the other hand, a is also a unit of $R[G]$, a ring with MJD, so a_s and a_u belong to $R[G]$. Since $R \cap \mathbb{Q} = \mathbb{Z}$, it follows that $a_s, a_u \in \mathbb{Q}[G] \cap R[G] = \mathbb{Z}[G]$. □

2. Wedderburn Components of Degree 3

The goal of this section is to prove Theorem 1.2. To this end, let $R = \mathcal{O}_F$ be the ring of integers in the algebraic number field F. We assume that the group algebra $F[G]$ has a Wedderburn component $W \cong \mathbf{M}_3(D)$, where D is an F-division algebra. We fix a concrete realization of this isomorphism and write $W = \mathbf{M}_3(D)$. Then $F[G]$ is the internal direct sum $F[G] = W \oplus W' = \mathbf{M}_3(D) \oplus W'$ and we let $\theta\colon F[G] \to \mathbf{M}_3(D)$ denote the natural projection. If K is the center of D, then K is a field containing F. Indeed, since $\dim_{\mathbb{Q}} F[G]$ is finite, we have $|K : \mathbb{Q}| < \infty$, so K is also an algebraic number field.

Now $\mathbf{M}_3(D) \supseteq \mathbf{M}_3(K)$ and we let $F[G;W] = \mathbf{M}_3(K) \oplus W' \subseteq F[G]$ be the complete inverse image of $\mathbf{M}_3(K)$ under the projection map θ. Of course, $F[G;W]$ is a semisimple F-subalgebra of $F[G]$. Moreover, we write $R[G;W] = F[G;W] \cap R[G]$. Note that, if $D = K$ is commutative, then $F[G;W] = F[G]$ and $R[G;W] = R[G]$. Furthermore, since $K \supseteq F$, we have $\mathcal{O}_K \supseteq \mathcal{O}_F = R$.

Lemma 2.1. *With the above notation, we have*

i. $R[G]$ and $R[G;W]$ are finitely generated free $\mathbb{Z}$-modules.

ii. If a is an element of $F[G;W]$, then there exists a positive integer $n \in \mathbb{Z}$ with $na \in R[G;W]$.

iii. There exists a positive integer $\tilde{r} \in \mathbb{Z}$ such that if $\widetilde{R} = \mathcal{O}_K[1/\tilde{r}] \subseteq K$, then $\theta(R[G;W]) \subseteq \mathbf{M}_3(\widetilde{R})$.

Proof. (i) We know that R is a finitely generated free $\mathbb{Z}$-module and hence so is $R[G]$. Since $R[G;W]$ is a $\mathbb{Z}$-submodule of $R[G]$, it follows that $R[G;W]$ inherits these properties.

(ii) If $a \in F[G;W] \subseteq F[G]$, then there exists a positive integer n with $na \in R[G]$. Thus $na \in F[G;W] \cap R[G] = R[G;W]$.

(iii) Let T be the subring of K generated over $\mathbb{Z}$ by the matrix entries $\theta(x)_{i,j}$ for all x in the finite generating set for $R[G;W]$ given by (i). Then T is a finitely generated ring and $\theta(R[G;W]) \subseteq \mathbf{M}_3(T)$. Furthermore, for each generator t of T there exists a positive integer $n_t \in \mathbb{Z}$ with $n_t t \in \mathcal{O}_K$. In particular, if $\tilde{r}$ is the least common multiple of the finitely many n_t's, then $\tilde{r}t \in \mathcal{O}_K$, so $t \in \widetilde{R} = \mathcal{O}_K[1/\tilde{r}]$ for all such t. Hence T is contained in the ring $\widetilde{R}$. □

Note that $\widetilde{R}$ is the set of all elements of K of the form $\alpha/\tilde{r}^i$ for some $\alpha \in \mathcal{O}_K$ and nonnegative integer i.

We now define two key elements in $\mathbf{M}_3(K) \subseteq F[G;W]$ in terms of the matrix units $e_{i,j}$. Specifically, e is the idempotent $e_{1,1}$ and $s = e_{1,2} + e_{2,3}$. It is trivial to observe the following relations.

Lemma 2.2. *If e and s are as above, then $se = 0$, $es = e_{1,2}$, $s^2 = e_{1,3}$, $es^2 = s^2$ and $s^3 = 0$.*

In view of the above formula for s^2, we define the projection $\pi\colon F[G;W] \to K$ by $\pi(a) = \theta(a)_{1,3}$ for all $a \in F[G;W]$. In other words, π picks off the $1,3$-entry of the matrix $\theta(a)$. Furthermore, since $e, s \in F[G;W]$, part (ii) of the previous lemma implies that there exist positive integers $\tilde{e}, \tilde{s} \in \mathbb{Z}$ such that $\tilde{e}e \in R[G;W]$ and $\tilde{s}s \in R[G;W]$.

Now let b be any element of $F[G;W]$ such that $\theta(b)$ is central in $\mathbf{M}_3(K)$ and define $u = u(b) \in F[G;W]$ by

$$u = 1 + (b-1)e + \tilde{s}s.$$

Lemma 2.3. *If b, u and π are as above, then b commutes with e, s and u, and we have*

i. $(u-1)^2(u-b) = 0$.

ii. $\pi((u-1)^2) = \pi((u-1)(u-b)) = \pi((\tilde{s}s)^2) = \tilde{s}^2 \neq 0$.

Proof. Since $e, s \in \mathbf{M}_3(K)$ and $\theta(b)$ is central in $\mathbf{M}_3(K)$, it is clear that b commutes with both e and s. Hence b commutes with u and therefore all the factors in the displayed polynomial expressions commute. Furthermore, $u - 1 = (b-1)e + \tilde{s}s$ and $u - b = (b-1)(e-1) + \tilde{s}s$. Of course, $e(e-1) = 0$.

(i) We have

$$\begin{aligned}
(u-1)^2(u-b) &= [(b-1)e + \tilde{s}s]^2[(b-1)(e-1) + \tilde{s}s] \\
&= (b-1)^3e^2(e-1) + (b-1)^2\tilde{s}[e^2s + (es+se)(e-1)] \\
&\qquad + (b-1)\tilde{s}^2[(es+se)s + s^2(e-1)] + \tilde{s}^3s^3 \\
&= (b-1)^2\tilde{s}[ese] + (b-1)\tilde{s}^2[(es^2 + ses + s^2e) - s^2] + \tilde{s}^3s^3 \\
&= 0
\end{aligned}$$

since each of the coefficients of $(b-1)^i\tilde{s}^{3-i}$ is zero by the preceding lemma.

(ii) Note that

$$(u-1)^2 = (b-1)^2e^2 + (b-1)\tilde{s}(es+se) + \tilde{s}^2s^2$$

and

$$(u-1)(u-b) = (b-1)^2e(e-1) + (b-1)\tilde{s}[es + s(e-1)] + \tilde{s}^2s^2.$$

Since $\theta(b)$ is central in $\mathbf{M}_3(K)$, $\theta(b-1)$ and $\theta((b-1)^2)$ are both scalar matrices in the ring. With this, it follows easily from Lemma 2.2 that the $(b-1)^2$ and $(b-1)\tilde{s}$ terms in the above two polynomial expressions map to 0 under the linear map π. Thus

$$\pi((u-1)^2) = \pi((u-1)(u-b)) = \pi((\tilde{s}s)^2)$$

and, of course the latter is equal to $\tilde{s}^2 \neq 0$. □

At this point, it is appropriate to introduce additional assumptions on the element $b \in F[G;W]$ related to $R[G]$.

Lemma 2.4. *Let $q \in \mathbb{Z}$ be a prime not dividing either $\tilde{r}$ or $\tilde{s}$. Suppose b is a unit of $R[G]$ with $1 \neq \theta(b)$ central in W and with*

$$b \equiv 1 \bmod \tilde{e}q\, R[G].$$

Then $u = u(b)$ is a unit in $R[G]$ whose semisimple part is not in $R[G]$.

Proof. Since $\theta(b)$ is central in $W = \mathbf{M}_3(D)$, we see that $\theta(b)$ is a scalar matrix with scalar in K. In particular, $b \in F[G;W] \cap R[G] = R[G;W]$. Of course, the same is true of b^{-1}, so we have $b^{-1} \in R[G;W]$ and therefore b is a unit in this ring.

By the above displayed equation $b = 1 + \tilde{e}qc$ for some $c \in R[G]$. Clearly $\theta(c)$ is also central in W, so $c \in R[G;W]$ and c commutes with e, s and u. Since $\tilde{e}e$ and $\tilde{s}s$ are both in $R[G;W]$, it follows that

$$u = 1 + (b-1)e + \tilde{s}s = 1 + qc(\tilde{e}e) + \tilde{s}s \in R[G;W].$$

Furthermore, by the preceding lemma, $(u-1)^2(u-b) = 0$ so

$$u[u^2 - (2+b)u + (1+2b)] = b.$$

In particular, since b is a unit in $R[G;W]$,

$$u^{-1} = [u^2 - (2+b)u + (1+2b)]b^{-1} \in R[G;W]$$

and u is indeed a unit in $R[G;W]$. Hence u is a unit in the larger ring $R[G]$.

As we mentioned above, $\theta(b)$ and $\theta(c)$ are central in $W = \mathbf{M}_3(D)$ and hence they are scalar matrices with scalar in K. Say $\theta(b) = \beta I$. We consider $\theta(c)$ later. By assumption, $\theta(b)$ is not the identity I, so $\beta \neq 1$.

Next, since $(u-1)^2(u-b)=0$, by part (i) of the previous lemma, applying θ yields $(\theta(u)-I)^2(\theta(u)-\beta I)=0$. Also, by that lemma, and the fact that π factors through θ, it follows that $(u-1)^2$ and $(u-1)(u-b)$ do not map to 0 under θ. Therefore we have $(\theta(u)-I)^2\neq 0$ and $(\theta(u)-I)(\theta(u)-\beta I)\neq 0$. It follows that the minimal polynomial over K of the 3×3 matrix $\theta(u)\in \mathbf{M}_3(K)$ is precisely $(\zeta-1)^2(\zeta-\beta)$, and therefore this must be the characteristic polynomial of $\theta(u)$. In particular, $\theta(u)$ has eigenvalue 1 with multiplicity two and eigenvalue $\beta\neq 1$ with multiplicity one.

Now let u_s be the semisimple part of the unit u in $F[G;W]$. Then $\theta(u_s)$ is the semisimple part of $\theta(u)\in \mathbf{M}_3(K)$. Note that $\theta(u)$ is similar to

$$\begin{pmatrix} 1 & * & 0 \\ 0 & 1 & 0 \\ 0 & 0 & \beta \end{pmatrix}$$

for some element $*\in K$ and that, under this same similarity, $\theta(u_s)$ becomes the diagonal matrix $\mathrm{diag}(1,1,\beta)$. In particular, we see that $(\beta-1)(\theta(u_s)-I)=(\theta(u)-I)^2$. Reading off the $1,3$-entries we obtain

$$\begin{aligned}(\beta-1)\pi(u_s-1) &= (\beta-1)(\theta(u_s)-I)_{1,3}\\ &= (\theta(u)-I)^2_{1,3}=\pi((u-1)^2)=\tilde{s}^2.\end{aligned}$$

Suppose, by way of contradiction, that $u_s-1\in R[G]$. Then $u_s-1\in F[G;W]\cap R[G]=R[G;W]$ and, by Lemma 2.1(iii), $\pi(u_s-1)=\alpha/\tilde{r}^i$ for some $\alpha\in\mathcal{O}_K$. Also $(\beta-1)I=\theta(b-1)=\tilde{e}q\theta(c)$ and $\theta(c)=(\gamma/\tilde{r}^j)I$ for some $\gamma\in\mathcal{O}_K$ since $c\in R[G;W]$. Thus the above displayed equation becomes

$$\tilde{e}q(\gamma/\tilde{r}^j)(\alpha/\tilde{r}^i)=\tilde{s}^2$$

and hence

$$\frac{\tilde{r}^{(i+j)}\tilde{s}^2}{q}=\tilde{e}\alpha\gamma\in\mathcal{O}_K.$$

But the left hand side is a rational number, so it must be contained in $\mathcal{O}_K\cap\mathbb{Q}=\mathbb{Z}$. It follows that the prime q divides either $\tilde{r}$ or $\tilde{s}$ in $\mathbb{Z}$, a contradiction, by assumption. Thus $u_s\notin R[G]$. □

It is now a simple matter to prove

Theorem 2.5. *Let R be the ring of algebraic integers in the algebraic number field F and suppose that the group algebra $F[G]$ has a Wedderburn component $W=\mathbf{M}_3(D)$ for some F-division algebra D. If $R[G]$ has a unit whose projection to W is central and has infinite multiplicative order, then $R[G]$ does not satisfy the multiplicative Jordan decomposition property.*

Proof. We use all of the preceding notation and we choose a prime $q\in\mathbb{Z}$ that does not divide $\tilde{r}$ or $\tilde{s}$ in $\mathbb{Z}$. Let b_0 be the given unit of $R[G]$ and let $\varphi\colon R[G]\to(R/\tilde{e}qR)[G]$ denote the natural homomorphism. Then $\varphi(b_0)$ is a

unit in the finite ring $(R/\tilde{e}qR)[G]$ and hence it must have finite order, say n. If $b = b_0^n$, then b is also a unit of $R[G]$ and $\varphi(b) = \varphi(b_0)^n = 1$. In other words, $b \equiv 1 \bmod \tilde{e}qR[G]$. Furthermore, $\theta(b) = \theta(b_0)^n$ is central in W and not equal to 1, since by assumption, $\theta(b_0)$ is central in W and has infinite multiplicative order. We can now apply the preceding lemma to construct a unit $u = u(b)$ in $R[G]$ whose semisimple part is not contained in $R[G]$. Thus $R[G]$ does not have MJD, as required. □

Theorem 1.2 is now an immediate consequence since any central element of $R[G]$ will project to a central element of W. Of course, one way to find central units in $R[G]$ is to look for them in R. By doing this, we obtain

Corollary 2.6. *Let R be the ring of algebraic integers in the algebraic number field F and suppose that the group algebra $F[G]$ has a Wedderburn component $W = \mathbf{M}_3(D)$ for some F-division algebra D. If $F \neq \mathbb{Q}$ and if F is not an imaginary quadratic extension of $\mathbb{Q}$, then $R[G]$ does not have MJD.*

Proof. By the Dirichlet Unit Theorem (see [FT, Theorem 37]), the assumptions on F imply that R has a unit b of infinite multiplicative order, and b is surely central in $R[G]$. Since the projection map $F[G] \to W$ is one-to-one when restricted to F, the image of b has infinite multiplicative order in W. Theorem 1.2 now yields the result. □

We remark that the construction of the unit $u = u(b)$ in this section is based on the concrete example described in [LP3] for one specific group of order 81.

3. Applications to 3-groups

In this section, we first show how Theorem 1.2 and the approach of [L] greatly simplify the classification of those 3-groups with MJD. To start with, we need

Lemma 3.1. *Let C be a cyclic group of order 9. Then $\mathbb{Z}[C]$ has a unit b such that, for any $\mathbb{Q}$-algebra homomorphism $\varphi\colon \mathbb{Q}[C] \to W$ that is one-to-one on C, the element $\varphi(b)$ has infinite multiplicative order as a unit of W.*

Proof. Suppose $C = \langle z \rangle$. Following [AP], the element

$$b = 1 - 2(z + z^8) + (z^2 + z^7) + (z^4 + z^5)$$

is a unit in $\mathbb{Z}[C]$ with inverse

$$b^{-1} = -5 - (z + z^8) + 5(z^2 + z^7) + 3(z^3 + z^6) - 4(z^4 + z^5).$$

Also, b has infinite multiplicative order since, by [H], the units of finite order in the integral group ring of any abelian group are trivial, that is $\pm$ group elements. Furthermore, $b \equiv 1 \bmod (1 - z^3)\,\mathbb{Q}[C]$ since

$$b = 1 + (1 - z^3)(-2z + z^2 - z^4 + 2z^5).$$

If $C_3 = \langle z^3 \rangle$ is the subgroup of C of order 3, then we know that

$$\mathbb{Q}[C] = (1-e)\mathbb{Q}[C] + e\mathbb{Q}[C] \cong \mathbb{Q}[C/C_3] \oplus \mathbb{Q}[\varepsilon]$$

where e is a central idempotent and $\mathbb{Q}[\varepsilon]$ is the cyclotomic field generated over $\mathbb{Q}$ by ε, a primitive complex 9th root of unity. Since b maps to 1 in the first summand, it follows that the image of b in the second, namely eb, has infinite multiplicative order.

Finally, let $\varphi\colon \mathbb{Q}[C] \to W$ be a $\mathbb{Q}$-algebra homomorphism that is one-to-one on C. If $\varphi(e) = 0$, then φ factors through the natural map $\mathbb{Q}[C] \to \mathbb{Q}[C/C_3]$ and φ restricted to C is not one-to-one, a contradiction. Thus $\varphi(e) \neq 0$ and since $\mathbb{Q}[\varepsilon]$ is a field, φ restricted to $e\mathbb{Q}[C]$ is one-to-one. Hence

$$\varphi(b) = \varphi((1-e)b) + \varphi(eb)$$

has infinite multiplicative order. □

With this observation, we can obtain

Proposition 3.2. *Let G be a nonabelian 3-group. If G has a cyclic central subgroup of order 9, then G does not have MJD.*

Proof. Let C be the given cyclic central subgroup of G and let c_3 be an element of order 3 in C. Also let g' be a nonidentity element in the commutator subgroup G' of G. Note that $a = (1-c_3)(1-g')$ is a nonzero element of $\mathbb{Q}[G]$ since its identity coefficient is either 1 or 2. Thus, since $\mathbb{Q}[G]$ is semisimple, there exists a Wedderburn component W of $\mathbb{Q}[G]$ with corresponding projection map $\theta\colon \mathbb{Q}[G] \to W$, such that $\theta(a) \neq 0$. In particular, $\theta(g') \neq 1$ and $\theta(c_3) \neq 1$. Say $W = \mathbf{M}_n(D)$, the ring of $n \times n$ matrices over the division ring D.

Since G is a p-group for $p > 2$, the main result of [R] implies that D must be a commutative field and, to better appreciate this fact, we write $D = K$. Furthermore, since $\theta(g') \neq 1$ and $g' \in G'$, it follows that $W = \mathbf{M}_n(K)$ is noncommutative and hence $n > 1$. Of course, G is a 3-group, so n is a power of 3 and therefore $n \geq 3$. If $n > 3$, Theorem 1.1(i) implies that G does not have MJD. Thus it suffices to assume that $n = 3$ and $W = \mathbf{M}_3(K)$.

Finally, let b be the unit of the integral group ring $\mathbb{Z}[C]$ given by the previous lemma, so that b is a central unit of $\mathbb{Z}[G]$. Furthermore, if φ denotes the restriction of θ to $\mathbb{Q}[C]$, then $\varphi\colon \mathbb{Q}[C] \to W$ is a $\mathbb{Q}$-algebra homomorphism with $\varphi(c_3) = \theta(c_3) \neq 1$. In particular, φ is one-to-one on C. Thus, by Lemma 3.1, $\theta(b) = \varphi(b)$ has infinite multiplicative order as a unit in W. Theorem 1.2 now yields the result. □

As we will see, this result along with the new approach of [L] greatly simplifies the characterization of nonabelian 3-groups with MJD originally obtained in the sequence of papers [LP1], [LP2] and [LP3].

We start with notation from [L]. We say that a finite group G has property SN if for any subgroup Y of G and any normal subgroup N of G we have either $Y \supseteq N$ or $YN \triangleleft G$. Furthermore, G has property SSN if every subgroup of G has SN. Since the MJD property is inherited by subgroups, the following is [LP1, Proposition 2.5], an extension of [HPW, Corollary 10].

Lemma 3.3. *If G has MJD, then G satisfies SSN.*

The key new ingredient in [L] is a group-theoretic consequence of the SSN property. Indeed, the following is [L, Propositions 2.2 and 3.3].

Proposition 3.4. *If G is a finite p-group with property SSN, then all noncyclic subgroups of G are normal.*

It follows that if G is a p-group with MJD, then every noncyclic subgroup of G is normal. As it turns out, p-groups with this property had been previously classified. Modulo 2-groups of order $\leq 2^7$, this is [P, Proposition 2.9]. The complete classification was obtained in [BJ]. There are nine classes of p-groups and, following [L], these are labeled **BJ1** through **BJ9**. But only three of these classes, namely **BJ1**, **BJ2** and **BJ4**, can be 3-groups. Indeed, **BJ1** and **BJ2** occur for arbitrary p, while **BJ4** is a particular 3-group of order 3^4. The following is the 3-group corollary of [BJ]. We remark that in [P], the class **BJ4** is just listed as a nonregular group of order 3^4, but without additional details. Of course, if G is a p-group of order p^4 and $p > 3$, then G is necessarily regular.

Theorem 3.5. *Let G be a nonabelian 3-group with the property that every noncyclic subgroup is normal. Then G satisfies one of the following.*

BJ1. *G is a metacyclic minimal nonabelian group. Specifically,*

$$G = \langle x, y \mid x^{3^m} = y^{3^n} = 1,\, x^y = x^{1+3^{m-1}} \rangle$$

where $m \geq 2$, $n \geq 1$ and $|G| = 3^{m+n}$.

BJ2. *$G = Z * G_0$ is the central product of a nonabelian group G_0 of order 3^3 with a cyclic group Z. Here $Z \cap G_0 = \mathfrak{Z}(G_0)$, the center of G_0.*

BJ4. *G is a group of order 3^4 and maximal class, with $\Omega_1(G) = G' \cong C_3 \times C_3$.*

In other words, by the above, if G is a nonabelian 3-group with MJD, then G is a group in **BJ1**, **BJ2** or **BJ4**. We consider these three families in turn.

Lemma 3.6. *Let G be a 3-group with MJD. If*

$$G = \langle x, y \mid x^{3^m} = y^{3^n} = 1,\, x^y = x^{1+3^{m-1}} \rangle$$

is in **BJ1**, *then $m = 2$, $n = 1$ and G is a nonabelian group of order 27.*

Proof. If $m \geq 3$, then $\langle x^3 \rangle$ is a cyclic central subgroup of G of order ≥ 9 and this contradicts Proposition 3.2. Thus $m = 2$. Similarly if $n \geq 3$, then $\langle y^3 \rangle$ is a cyclic central subgroup of G of order ≥ 9, again a contradiction. Thus $n = 1$ or 2 and $|G| = 27$ or 81. In the latter case, $m = 2$, $n = 2$ and [LP2, Lemma 2.2] implies that this group does not have MJD. Thus $m = 2$, $n = 1$ and $|G| = 27$. □

Next, we have

Lemma 3.7. *Let G be a 3-group in* **BJ2**, *so that $G = Z * G_0$ is a central product with Z cyclic and with G_0 nonabelian of order 27. If G has MJD, then $G = G_0$ is itself a nonabelian group of order 27.*

Proof. Obviously Z is a cyclic central subgroup of G. Thus by Proposition 3.2 we must have $|Z| = 3$ and $G = Z * G_0 = G_0$. □

Finally,

Lemma 3.8. *Let G be a group in* **BJ4**. *Then G does not satisfy MJD.*

Proof. Since $|G| = 81$ and G has maximal class, we know that $A = \mathfrak{Z}(G)$ has order 3 and that G/G' is abelian of type $(3, 3)$. Furthermore, every nonidentity normal subgroup of G meets A and hence contains A. Now $B = \Omega_1(G) = G'$ is given to be abelian of type $(3, 3)$, so B is not central in G and $G \neq C = \mathfrak{C}_G(B) \supseteq B$. Since G/C acts faithfully on B and since 9 does not divide $|\mathrm{Aut}(B)|$, we conclude that $|G : C| = 3$ and hence $|C : B| = 3$. The latter implies that C is abelian and, since $B = \Omega_1(G)$, we see that C is in fact abelian of type $(9, 3)$. Note that B/A is central in G/A, so $[B, G] = A$. Furthermore, C/A is not central in G/A, so $[C, G] \not\subseteq A$ and hence $[C, G] = B = G'$.

Let x be an element of C of order 9. Then $\langle x^3\rangle$ is a characteristic subgroup of C and hence normal in G. Thus $1 \neq x^3$ generates the center A. Next, choose $z \in G \setminus C$. Then $z^3 \in C$, so $\mathfrak{C}_G(z^3) \supseteq \langle C, z\rangle = G$. In other words, $z^3 \in \mathfrak{Z}(G)$ and $z^3 \neq 1$ since $B = \Omega_1(G)$. Thus $z^3 = x^3$ or x^{-3} and, by replacing z by z^{-1} if necessary, we can assume that $z^3 = x^3$. Furthermore, since $[C, z] = [C, G] = B$ and $[B, z] = [B, G] = A$, we see that $y = [x, z] \in B \setminus A$. Thus y has order 3, $C = \langle x\rangle \times \langle y\rangle$ and $x^z = xy$. Of course, $y \in B$ is a noncentral element of G, so $[y, z]$ is a nonidentity element of A. In other words, $y^z = yx^3$ or yx^{-3}.

Suppose, $y^z = yx^3$. Then $x^{z^2} = (xy)^z = (xy)(yx^3)$ and hence

$$\begin{aligned}(zx)^3 = (zx)(zx)(zx) &= z^3(z^{-2}xz^2)(z^{-1}xz)x\\ &= (x^3)(xy^2x^3)(xy)x = x^9y^3 = 1.\end{aligned}$$

Thus $zx \in \Omega_1(G) \subseteq C$ and $z \in C$, a contradiction. It follows that $y^z = yx^{-3}$, so G is precisely the group considered in [LP2, Lemma 2.1]. That lemma now implies that G does not have MJD. □

In view of our previous discussion, it now follows from Lemmas 3.6, 3.7 and 3.8 that if G is a nonabelian 3-group with MJD, then $|G| = 27$. Conversely, if $|G| = 27$, then [LP1, Theorem 3.5] implies that G satisfies MJD. With this, we have obtained a much simpler proof of

Theorem 3.9. *Let G be a finite nonabelian 3-group. Then $\mathbb{Z}[G]$ has the MJD property if and only if G has order $3^3 = 27$.*

Our goal now is to consider the MJD property for group rings $R[G]$ with $R = \mathcal{O}_F$ and with G a 3-group. For this we need the following two lemmas. Recall that if H is a subgroup of G, then we let $\widehat{H}$ denote the sum of the group elements of H in the integral group algebra $\mathbb{Z}[G]$. As is well known, $(1 - h)\widehat{H} = \widehat{H}(1 - h) = 0$ for all $h \in H$, and $(\widehat{H})^2 = |H|\,\widehat{H}$.

Lemma 3.10. *Let G be a finite p-group and suppose that A is an abelian subgroup of G of type (p,p).*

i. For each of the $p+1$ subgroups A_i of A of order p with $i = 0, 1, \ldots, p$, let $a_i \in A_i$. Then in $\mathbb{Z}[A]$ we have $\prod_{i=0}^{p}(1-a_i) = 0$.

ii. Write $A = \langle z, x\rangle$ and suppose that $y \in G$ normalizes A and satisfies $z^y = z$ and $x^y = xz$. Then $\alpha = (1-z)(1-x)y^{-1}$ is a nilpotent element of $\mathbb{Z}[G]$.

Proof. (i) Set $\beta = \prod_i (1-a_i) \in \mathbb{Z}[A]$. Since $(1-a_i)$ is a factor of β, we have $\beta\widehat{A_i} = 0$ and also $\beta\widehat{A} = 0$. Furthermore, the $p+1$ subgroups A_i of A form a partition of A, so it follows that $\sum_i \widehat{A_i} - \widehat{A} = p$. Hence $\beta p = 0$ and $\beta = 0$.

(ii) We have

$$\begin{aligned}\alpha^p &= [(1-z)(1-x)y^{-1}]^p \\ &= (1-z)^p(1-x)(1-x)^y(1-x)^{y^2}\cdots(1-x)^{y^{p-1}}y^{-p} \\ &= (1-z)^p(1-x)(1-xz)(1-xz^2)\cdots(1-xz^{p-1})y^{-p} \\ &= 0\end{aligned}$$

by part (i), since the elements $z, x, xz, xz^2, \ldots, xz^{p-1}$ belong to the $p+1$ different subgroups of A of order p. □

Since the above results are identities in $\mathbb{Z}[G]$, they hold in the group ring of G over any ring of any characteristic. As an alternative proof of (i), we can embed $\mathbb{Z}[A]$ into the complex group algebra $\mathbb{C}[A]$ and show that $\lambda(\beta) = 0$ for all linear characters $\lambda\colon \mathbb{C}[A] \to \mathbb{C}$. To this end, let λ be given. Then $\lambda(A)$ is a finite multiplicative subgroup of $\mathbb{C}^\bullet$, so it must be cyclic. In particular, the kernel of the group homomorphism $\lambda\colon A \to \mathbb{C}^\bullet$ necessarily contains A_i for some i. But $(1-a_i)$ is a factor of β and $\lambda(1-a_i) = 0$, so the result follows.

Next, we need an analog of Lemma 3.1.

Lemma 3.11. *Let C be a cyclic group of order 3, let F be an imaginary quadratic extension of $\mathbb{Q}$, and let $R = \mathcal{O}_F$. Assume that F does not contain ω, a primitive complex cube root of 1. Then $R[C]$ has a unit b such that, for any F-algebra homomorphism $\varphi\colon F[C] \to W$ that is one-to-one on C, the element $\varphi(b)$ has infinite multiplicative order as a unit of W.*

Proof. Write $C = \langle x\rangle$. Since $\omega \notin F$, the polynomial $1 + \zeta + \zeta^2$ is irreducible in $F[\zeta]$ and therefore $|F[\omega] : F| = 2$. Moreover the F-algebra homomorphism $\theta\colon F[C] \to F[\omega]$ given by $x \mapsto \omega$ is onto. By dimension considerations and the fact that $F[C]$ is commutative and semisimple, we conclude that $F[C] = F \oplus F[\omega]$. Clearly the second projection $\theta'\colon F[C] \to F$ is the augmentation map determined by $x \mapsto 1$.

Since F is an imaginary quadratic extension of $\mathbb{Q}$, we can assume that $F = \mathbb{Q}[\sqrt{-d}]$ where d is a square-free positive integer. Furthermore, since $\omega \notin F$, we have $d \neq 3$. It follows that $3d$ is not a perfect square. In particular, by [NZ, Corollary 7.23], Pell's equation $a^2 - 3dc^2 = 1$ has infinitely many integer

solutions (a, c). Fix such a solution with $a \neq 0, \pm 1$. Since $a^2 \equiv 1 \bmod 3$, we have $a \equiv \pm 1 \bmod 3$. Replacing a by $-a$ if necessary, we can assume that $a \equiv 1 \bmod 3$. Similarly, replacing c by $-c$ if necessary, we can assume that a and c have the same sign.

Note that $R \supseteq \mathbb{Z}[\sqrt{-d}]$ and $\omega = (-1 + \sqrt{-3})/2$, so $\sqrt{-3} = 2\omega + 1$ and

$$R[\omega] \supseteq \mathbb{Z}[\sqrt{-d}, \sqrt{-3}] \supseteq \mathbb{Z}[\sqrt{3d}].$$

In the latter ring, Pell's equation yields $(a + c\sqrt{3d})(a - c\sqrt{3d}) = 1$, so $a + c\sqrt{3d}$ is a unit with inverse $a - c\sqrt{3d}$. Furthermore, since a and c have the same sign, $a + c\sqrt{3d}$ is a real number of absolute value > 1, so this unit has infinite multiplicative order.

Set $\beta = a + c\sqrt{-d}(2x+1) \in R[C]$ and $\beta' = a - c\sqrt{-d}(2x+1) \in R[C]$, where again $C = \langle x \rangle$. Since $\operatorname{aug}(2x + 1) = 3$, we have $\operatorname{aug} \beta \equiv a \equiv 1 \bmod 3R$ and $\operatorname{aug} \beta' \equiv a \equiv 1 \bmod 3R$. Thus there exist elements $r, r' \in R$ such that $b = \beta + r\widehat{C}$ and $b' = \beta' + r'\widehat{C}$ both have augmentation 1. In particular, $\theta'(b) = \theta'(b') = 1$, so $\theta'(bb') = 1$.

Furthermore, since $\theta(\widehat{C}) = 1 + \omega + \omega^2 = 0$ and $\theta(2x + 1) = 2\omega + 1 = \sqrt{-3}$, we have $\theta(b) = a + c\sqrt{3d}$ and $\theta(b') = a - c\sqrt{3d}$. Thus $\theta(bb') = \theta(b)\theta(b') = 1$. We conclude from this and the above that $bb' = 1$. In other words, b is a unit in $R[C]$ and $\theta(b)$ has infinite multiplicative order as a unit in $R[\omega]$.

Finally, let $\varphi\colon F[C] \to W$ be an F-algebra homomorphism that is one-to-one on C. If $e = \widehat{C}/3$ is the central idempotent in $F[C]$ corresponding to the augmentation map, and if $\varphi(1-e) = 0$, then φ factors through the natural map $F[C] \to F[C/C] = F$ and φ restricted to C is not one-to-one, a contradiction. Thus $\varphi(1 - e) \neq 0$ and since $F[\omega]$ is a field, φ restricted to $(1 - e)F[C] \cong F[\omega]$ is one-to-one. Hence

$$\varphi(b) = \varphi(eb) + \varphi((1 - e)b)$$

has infinite multiplicative order. □

With this, we can prove

Theorem 3.12. *Let $F \neq \mathbb{Q}$ be an algebraic number field and set $R = \mathcal{O}_F$. If G is a 3-group and $R[G]$ has MJD, then G is abelian.*

Proof. Suppose, by way of contradiction, that G is nonabelian. Since $R[G]$ has MJD, it follows from Lemma 1.3 that $\mathbb{Z}[G]$ has MJD. Thus, by Theorem 3.9, G is one of the two nonabelian groups of order 27. With this, and the main result of [R], it is clear that all noncommutative Wedderburn components of $F[G]$ are isomorphic to $\mathbf{M}_3(K)$ for suitable field extensions K of F. Corollary 2.6 now implies that F must be an imaginary quadratic field extension of $\mathbb{Q}$. In particular, we can assume that $F = \mathbb{Q}[\sqrt{-d}]$ where $d \in \mathbb{Z}$ is a square-free positive integer.

Suppose first that $d = 3$ so that $R = \mathcal{O}_F$ contains $\omega = (-1 + \sqrt{-3})/2$, a primitive complex cube root of unity. Observe that both possible groups G have a normal abelian subgroup $A = \langle z, x \rangle$ of type $(3, 3)$ and an element

$y \in G \setminus A$ with $z^y = z$ and $x^y = xz$. Thus, by Lemma 3.10(ii), we see that $\alpha = (1-z)(1-x)y^{-1}$ is a nilpotent element of $R[G]$. Furthermore, z is central in G, so $e = (1+\omega z+\omega^2 z^2)/3$ is a central idempotent in $F[G]$. Theorem 1.1(ii) now implies that $e\alpha \in R[G]$. But observe that $e(\omega z) = e$, so $ez = e\omega^2$ and hence $e\alpha = e(1-\omega^2)(1-x)y^{-1}$. In particular, the coefficient of y^{-1} in this product is $(1-\omega^2)/3$. But the latter element is not contained in R since its Galois norm is $[(1-\omega^2)/3]\cdot[(1-\omega)/3] = 1/3 \notin \mathbb{Z}$. Thus d cannot equal 3.

On the other hand if $d \neq 3$, write $C = \mathfrak{Z}(G) = G'$ so that $|C| = 3$ and let $b \in R[C]$ be the unit given by Lemma 3.11. Then b is a central unit of $R[G]$. Furthermore, if $C = \langle c \rangle$, then there exists a Wedderburn component W of $F[G]$, with corresponding projection map $\theta\colon F[G] \to W$, such that $\theta(c) \neq 1$. Since $c \in G'$, W must be noncommutative and hence $W \cong \mathbf{M}_3(K)$ for some field K. On the other hand, since $C = \langle c \rangle$ is cyclic of order 3, $\theta(c) \neq 1$ implies that θ is one-to-one when restricted to C. Thus, by Lemma 3.11, $\theta(b)$ is a unit of infinite multiplicative order in W. Theorem 1.2 now implies that $R[G]$ does not have MJD. With this final contradiction, the result follows. □

4. Application to $\{3, p\}$-groups

There are still a number of families to be considered to complete the classification of all nonabelian MJD groups. According to [HPW, Theorem 29] one such family consists of the semidirect products $C_p \rtimes C_{3^k}$, where C_p is cyclic of prime order p, $C_{3^k} = \langle g \rangle$ is cyclic of order 3^k, and g^3 acts trivially on C_p. In particular, C_p admits an automorphism of order 3, so $p \equiv 1 \bmod 3$ and hence $p \geq 7$. In this section, we use Theorem 1.2 to show that these groups do not have MJD at least when $p > 7$. The difficulty with $p = 7$ is that the appropriate unit b we need does not exist at least in $\mathbb{Z}[C_p]$.

On the other hand, for $p > 7$ we have the following result which we prove from first principles using particular Bass cyclic units (see [B]).

Lemma 4.1. *Let $C = \langle z \rangle$ be a cyclic group of prime order $p > 7$ and suppose that C admits an automorphism σ of order 3. Then $\mathbb{Z}[C]$ has a unit b of infinite multiplicative order that is centralized by σ. Indeed, if $\varphi\colon \mathbb{Z}[C] \to \mathbb{Z}[\varepsilon]$ is the natural homomorphism sending z to ε, a primitive complex pth root of unity, then $\varphi(b)$ is a unit of $\mathbb{Z}[\varepsilon]$ of infinite multiplicative order.*

Proof. Let $\mathrm{aug}\colon \mathbb{Z}[C] \to \mathbb{Z}$ denote the augmentation homomorphism and let $\widehat{C}$, as usual, denote the sum of the elements of C in $\mathbb{Z}[C]$. Then $\widehat{C}\mathbb{Z}[C] = \widehat{C}\mathbb{Z}$ is an ideal of $\mathbb{Z}[C]$ and $\mathrm{aug}(\widehat{C}) = p$. In particular, if $\alpha \in \mathbb{Z}[C]$ then there is at most one $\tilde{a} \in \mathbb{Z}$ with $\mathrm{aug}(\alpha + \tilde{a}\widehat{C}) = 1$. With this, it is clear that if $\alpha + \tilde{a}\widehat{C}$ and $\beta + \tilde{b}\widehat{C}$ are elements of $\mathbb{Z}[C]$ of augmentation 1, then

$$(\alpha + \tilde{a}\widehat{C})(\beta + \tilde{b}\widehat{C}) = \alpha\beta + \tilde{d}\widehat{C}$$

where $\tilde{d} \in \mathbb{Z}$ is the unique integer with $\mathrm{aug}(\alpha\beta + \tilde{d}\widehat{C}) = 1$.

Since $\tilde{n}^{p-1} \equiv 1 \bmod p$ for all integers $\tilde{n}$ prime to p and since p is odd, it follows that there exist integers $\tilde{a}, \tilde{b} \in \mathbb{Z}$ such that

$$u = (1+z)^{p-1} + \tilde{a}\widehat{C}, \quad \text{and}$$
$$v = (1+z^2+z^4+\cdots+z^{p-1})^{p-1} + \tilde{b}\widehat{C}$$

both have augmentation 1. Furthermore, since

$$(1+z)(1+z^2+z^4+\cdots+z^{p-1}) = (1+z+z^2+z^3+\cdots+z^p) = 1+\widehat{C},$$

we see that

$$uv \equiv (1+\widehat{C})^{p-1} \equiv 1 \bmod \widehat{C}\mathbb{Z}.$$

But $\operatorname{aug}(uv) = 1$ and therefore $uv = 1$. In other words, both u and v are units in $\mathbb{Z}[C]$.

Now let σ be the given automorphism of C of order 3 with say $\sigma(z) = z^i$ and $\sigma^2(z) = z^j$. Then clearly $b = u{\cdot}\sigma(u){\cdot}\sigma^2(u)$ is a unit of $\mathbb{Z}[C]$ centralized by σ and, by the above we have

$$b = [(1+z)(1+z^i)(1+z^j)]^{p-1} + \tilde{d}\widehat{C}$$

for some integer $\tilde{d}$.

Finally, let $\varphi\colon \mathbb{Z}[C] \to \mathbb{Z}[\varepsilon]$ be the given epimorphism. Since $\varphi(\widehat{C}) = 0$, we see that

$$\varphi(b) = [(1+\varepsilon)(1+\varepsilon^i)(1+\varepsilon^j)]^{p-1}.$$

In particular, if $\varphi(b)$ is a unit of finite order, then so is $(1+\varepsilon)(1+\varepsilon^i)(1+\varepsilon^j)$. But the only units in $\mathbb{Z}[\varepsilon]$ of finite order are of the form $\pm\varepsilon^k$ for some k. Thus

$$(1+\varepsilon)(1+\varepsilon^i)(1+\varepsilon^j) = \pm\varepsilon^k$$

and therefore ε is a root of the polynomial

$$f(\zeta) = (1+\zeta)(1+\zeta^i)(1+\zeta^j) \mp \zeta^k \in \mathbb{Z}[\zeta].$$

On the other hand, the minimal polynomial of ε is $g(\zeta) = 1+\zeta+\zeta^2+\cdots+\zeta^{p-1}$ and this is a monic integral polynomial. Thus $g(\zeta)$ divides $f(\zeta)$ in $\mathbb{Z}[\zeta]$. In particular, evaluating at 1, we see that $p = g(1)$ divides $f(1) = 2^3 \mp 1$ in $\mathbb{Z}$, and this is a contradiction since $p > 7$. Thus $\varphi(b)$ and hence b have infinite multiplicative order. □

We note that the above result is false for $p = 7$ because $\varphi(b)$ is a unit of $\mathbb{Z}[\varepsilon]^{\langle\sigma\rangle} \subseteq \mathbb{Q}[\varepsilon]^{\langle\sigma\rangle}$, where $\langle\sigma\rangle$ is a group of field automorphisms of order 3. But then $\mathbb{Q}[\varepsilon]^{\langle\sigma\rangle}$ is an imaginary quadratic extension of $\mathbb{Q}$ and therefore $\mathbb{Z}[\varepsilon]^{\langle\sigma\rangle}$ has only units of finite order.

As a consequence, we have

Theorem 4.2. *Let G be the noncommutative semidirect product $G = C_p \rtimes C_{3^k}$ where C_p is cyclic of prime order p, $C_{3^k} = \langle g\rangle$ is cyclic of order 3^k and g^3 centralizes C_p. If $p \neq 7$, then G does not have MJD.*

Proof. As we noted previously, $p \equiv 1 \bmod 3$. In particular, if $F = \mathbb{Q}[\varepsilon]$ is the cyclotomic field where ε is a primitive complex pth root of unity, then F admits a field automorphism τ of order 3. Using τ, we can form the skew group ring FH, where $H = \langle h \rangle$ is cyclic of order 3, and where $h^{-1} f h = \tau(f)$ for all $f \in F$. By definition, every element of FH is uniquely writable as $f_0 + f_1 h + f_2 h^2$ with $f_i \in F$. We quickly observe some well-known properties of FH.

First, since τ and τ^2 act nontrivially on F, it follows that $\mathfrak{C}_{FH}(F) = F$ and thus $\mathfrak{Z}(FH) = K$ is the fixed field of F under the action of $\langle \tau \rangle$. In particular, $|F : K| = 3$ and $\dim_K FH = 9$. Next, FH is easily seen to be simple. Indeed, if I is a nonzero ideal of the skew group ring, choose $0 \neq a = f_0 + f_1 h + f_2 h^2 \in I$ with the smallest number of nonzero f_i. Multiplying a by a power of h, if necessary, we can assume that $f_0 \neq 0$. But then $fa - af \in I$ for all $f \in F$, and these elements have smaller support than a. By the minimal nature of a, it follows that $fa - af = 0$ and hence that $0 \neq a \in \mathfrak{C}_{FH}(F) = F$. In particular, a is a unit and $I = FH$.

Since $\dim_K FH = 9$, it follows that FH is either a division ring or isomorphic to $\mathbf{M}_3(K)$. But $(1 + h + h^2)(1 - h) = 1 - h^3 = 0$, so FH has zero divisors and hence $FH \cong M_3(K)$. Now write $C_p = \langle z \rangle$ and let σ denote the automorphism of C_p of order 3 corresponding to conjugation by g. Then $\theta \colon \mathbb{Q}[G] \to FH$ given by $\theta(z) = \varepsilon$ and $\theta(g) = h$ is an epimorphism if τ is chosen to correspond to σ. With this, it follows that $\mathbb{Q}[G]$ has a Wedderburn component $W \cong FH \cong \mathbf{M}_3(K)$ with $\theta \colon \mathbb{Q}[G] \to \mathbf{M}_3(K)$ corresponding to the natural projection.

Finally $p > 7$, so we can let b be the unit of $\mathbb{Z}[C_p]$ given by the previous lemma. Then b is a unit of $\mathbb{Z}[G]$ that commutes with both z and g, so b is central in $\mathbb{Z}[G]$. Since $\theta(z) = \varepsilon$, it follows from Lemma 4.1 that $\theta(b)$ is a unit of W of infinite multiplicative order. Theorem 1.2 now yields the result. □

Thus only the case $p = 7$ remains. If $k = 1$, then by [A, Proposition 5.1] the group $G = C_7 \rtimes C_3$ has MJD. On the other hand, if $k \geq 3$, then $G = C_7 \rtimes C_{3^k}$ has a cyclic central subgroup Z of order ≥ 9 and it is tempting to try to use units obtained from $\mathbb{Z}[Z]$ in Theorem 1.2. Unfortunately this does not work since the Wedderburn components of $\mathbb{Q}[G]$ needed for these units turn out to be division rings and not 3×3 matrix rings. This can be verified using the deep results of Amitsur in his celebrated paper [Am]. Indeed, the various groups $G = C_7 \rtimes C_{3^k}$ with $k \geq 2$ form an infinite family of nonabelian groups that are all embeddable in division rings.

We sketch a proof of the latter facts below. For convenience, we replace k by $c + 1$ and write

$$G_c = C_7 \rtimes C_{3^{c+1}}$$

for all $c \geq 0$. To be consistent with the notation of [Am] we consider group conjugation with the inverse factor on the right.

Lemma 4.3. *If $c \geq 0$ and G_c is as above, then*

$$G_c = \langle a, b \mid a^m = 1,\, b^n = a^t,\, bab^{-1} = a^r \rangle,$$

where $m = 7 \cdot 3^c$, $n = 3$, $t = 7$, $r \equiv 1 \bmod 3^c$ and $r \equiv 2 \bmod 7$.

Proof. Write $G_c = X \rtimes B$, where $X = \langle x \rangle$ is cyclic of order 7 and $B = \langle b \rangle$ is cyclic of order 3^{c+1}. Then $bxb^{-1} = x^2$ or x^4, and by replacing b by b^{-1} if necessary, we can assume that $bxb^{-1} = x^2$. Obviously, b^3 is central in G_c and has order 3^c. Now choose an integer v with $7v \equiv 1 \bmod 3^c$. Since v is prime to 3, we have $\langle b^{3v} \rangle = \langle b^3 \rangle$ and hence $a = xb^{3v}$ is an element of G of order $7{\cdot}3^c$. Furthermore, $a^7 = x^7 b^{3v \cdot 7} = b^3$ since $x^7 = 1$ and $7v \equiv 1 \bmod 3^c$.

It follows that $G_c = \langle a, b \rangle$ and that

$$a^m = 1,\ b^n = a^t, \quad \text{and} \quad bab^{-1} = a^r,$$

where $m = 7{\cdot}3^c$, $n = 3$, $t = 7$ and r is a suitable integer. Furthermore, since b centralizes $b^n = a^t$, we have $a^{rt} = ba^t b^{-1} = a^t$, so $rt \equiv t \bmod 7{\cdot}3^c$ and hence $r \equiv 1 \bmod 3^c$. In the same way, since a^{3^c} has order 7, we see that $a^{3^c r} = ba^{3^c} b^{-1} = a^{2 \cdot 3^c}$, so $r \equiv 2 \bmod 7$. In particular, we can take $r = (15)^c + 1$.

Finally, note that the group G having the above generators and relations is a cyclic extension and hence has order $mn = 7{\cdot}3^{c+1} = |G_c|$. Since there is an epimorphism from G to G_c, it follows that $G \cong G_c$. In other words, G_c is the group determined by the two generators a and b and the three relations. □

Using the parameters of the preceding lemma, we now describe a particular cyclic algebra $\mathfrak{A}_c = F{*}H$. To start with, let ε be a complex primitive mth root of unity and let F be the cyclotomic field $F = \mathbb{Q}[\varepsilon]$. Then F admits a field automorphism τ of order 3 determined by $\tau(\varepsilon) = \varepsilon^r$, and $r \equiv 1 \bmod 3^c$ implies that τ fixes ε^7. With this, we can construct the crossed product $F{*}H$ where $H = \langle h \rangle$ is cyclic of order 3, $\bar{h} f \bar{h}^{-1} = \tau(f)$ for all $f \in F$ and $\bar{h}^3 = \varepsilon^7$. By definition, every element of $\mathfrak{A}_c = F{*}H$ is uniquely writable as $f_0 + f_1\bar{h} + f_2\bar{h}^2$ with $f_0, f_1, f_2 \in F$. Since H is a cyclic group, the crossed product $\mathfrak{A}_c$ is of course a cyclic algebra.

Lemma 4.4. *With the above notation, $\mathfrak{A}_c$ is a simple algebra with center $K = F^\tau$, the fixed field of τ, and there exists an epimorphism $\theta_c\colon \mathbb{Q}[G_c] \to \mathfrak{A}_c$ that embeds G_c as a subgroup of $\mathfrak{A}_c^\bullet$. Furthermore, $\mathfrak{A}_0 \cong \mathbf{M}_3(K)$, $\dim_{\mathbb{Q}} \mathfrak{A}_0 = 18$ and $\dim_{\mathbb{Q}} \mathfrak{A}_c = 4{\cdot}3^{c+1}$ for all $c \geq 1$.*

Proof. The skew group ring argument in the proof of Theorem 4.2 also applies here to show that $\mathfrak{C}_{\mathfrak{A}_c}(F) = \mathfrak{Z}(\mathfrak{A}_c) = K = F^\tau$ and that $\mathfrak{A}_c$ is a simple noncommutative ring. Furthermore, $\dim_{\mathbb{Q}} \mathfrak{A}_c = 3{\cdot}|F : \mathbb{Q}| = 3{\cdot}\varphi(7{\cdot}3^c)$ and hence $\dim_{\mathbb{Q}} \mathfrak{A}_0 = 18$ while $\dim_{\mathbb{Q}} \mathfrak{A}_c = 4{\cdot}3^{c+1}$ for all $c \geq 1$. Since each $\mathfrak{A}_c$ has dimension 9 over its center, we see that $\mathfrak{A}_c$ is either a division ring or isomorphic to $\mathbf{M}_3(K)$. But in $\mathfrak{A}_0$ we have $\bar{h}^3 = 1$, so $(1 - \bar{h})(1 + \bar{h} + \bar{h}^2) = 1 - \bar{h}^3 = 0$ and this ring has zero divisors. Thus $\mathfrak{A}_0 \cong \mathbf{M}_3(K)$.

Finally, using the description of G_c in Lemma 4.3 via generators and relations, it follows easily that there is a group homomorphism $\theta_c\colon G_c \to \mathfrak{A}_c^\bullet$ given by $a \mapsto \varepsilon$ and $b \mapsto \bar{h}$. Clearly θ_c is a one-to-one map on G_c that extends to an algebra epimorphism $\theta_c\colon \mathbb{Q}[G_c] \to \mathfrak{A}_c$. □

As a consequence, we obtain

Lemma 4.5. *For all $c \geq 0$, we have*

$$\mathbb{Q}[G_c] \cong \mathfrak{A}_0 \oplus \mathfrak{A}_1 \oplus \cdots \oplus \mathfrak{A}_c \oplus \mathbb{Q}[G_c/G_c'].$$

In particular, $\mathfrak{A}_0, \mathfrak{A}_1, \ldots, \mathfrak{A}_c$ are the noncommutative Wedderburn components of the group algebra $\mathbb{Q}[G_c]$.

Proof. Since $G_c = C_7 \rtimes C_{3^{c+1}}$, there exists a group epimorphism $G_c \to G_d$ for all $d \leq c$. In particular, there exists an algebra epimorphism $\mathbb{Q}[G_c] \to \mathbb{Q}[G_d]$ and, by composing this with θ_d, we obtain an epimorphism $\mathbb{Q}[G_c] \to \mathfrak{A}_d$. But $\mathfrak{A}_d$ is simple, so this implies that $\mathbb{Q}[G_c]$ has a noncommutative Wedderburn component isomorphic to $\mathfrak{A}_d$. Furthermore, note that the various $\mathfrak{A}_d$'s are not isomorphic since they have different dimensions over $\mathbb{Q}$. With this, it follows that $\mathbb{Q}[G_c]$ has a ring direct summand isomorphic to $\mathfrak{A}_0 \oplus \mathfrak{A}_1 \oplus \cdots \oplus \mathfrak{A}_c$.

On the other hand, $\mathbb{Q}[G_c]$ has a ring direct summand isomorphic to the group algebra $\mathbb{Q}[G_c/G_c'] \cong \mathbb{Q}[C_{3^{c+1}}]$ and this gives rise to all the commutative Wedderburn components of $\mathbb{Q}[G_c]$. In particular, $\mathfrak{A}_0 \oplus \mathfrak{A}_1 \oplus \cdots \oplus \mathfrak{A}_c \oplus \mathbb{Q}[G_c/G_c']$ is a ring direct summand of $\mathbb{Q}[G_c]$ having $\mathbb{Q}$-dimension

$$18 + \sum_{d=1}^{c} 4{\cdot}3^{d+1} + 3^{c+1} = 7{\cdot}3^{c+1} = \dim_{\mathbb{Q}} \mathbb{Q}[G_c].$$

Thus we conclude that $\mathbb{Q}[G_c] \cong \mathfrak{A}_0 \oplus \mathfrak{A}_1 \oplus \cdots \oplus \mathfrak{A}_c \oplus \mathbb{Q}[G_c/G_c']$. □

Finally, we need

Lemma 4.6. *We have the following simple arithmetic facts.*

i. For all $i \geq 0$, we have

$$7^{3^i} \equiv 1 - 3^{i+1} \bmod 3^{i+2}.$$

ii. If $c \geq 1$ and if δ is the order of 7 modulo 3^c, then $\delta = 3^{c-1}$ and the integer quotient $(7^\delta - 1)/3^c$ is relatively prime to 3.

Proof. (i) We proceed by induction on i, the case $i = 0$ being trivial to verify. Now suppose the result holds for some $i \geq 0$ and write $7^{3^i} = 1 + 3^{i+1}b$ where $b = -1 + 3a$ for some integer a. Then

$$\begin{aligned} 7^{3^{i+1}} &= (1 + 3^{i+1}b)^3 = 1 + 3^{i+2}b + 3^{2i+3}b^2 + 3^{3i+3}b^3 \\ &\equiv 1 + 3^{i+2}b \equiv 1 - 3^{i+2} + 3^{i+3}a \equiv 1 - 3^{i+2} \bmod 3^{i+3}, \end{aligned}$$

as required.

(ii) Since $c \geq 1$, we can set $i = c - 1$ in equation (i) to obtain

$$\begin{aligned} 7^{3^{c-1}} &\equiv 1 - 3^c \bmod 3^{c+1} \\ &\equiv 1 \bmod 3^c. \end{aligned}$$

Thus δ, the order of 7 modulo 3^c, divides 3^{c-1}. If $c = 1$, then clearly $\delta = 3^{c-1}$. If $c \geq 2$, we can set $i = c - 2$ in equation (i) to obtain

$$7^{3^{c-2}} \equiv 1 - 3^{c-1} \not\equiv 1 \bmod 3^c.$$

Thus δ does not divide 3^{c-2} and hence $\delta = 3^{c-1}$ in all cases. Finally, by (i) again,

$$7^\delta = 7^{3^{c-1}} \equiv 1 - 3^c \bmod 3^{c+1}$$

so $(7^\delta - 1)/3^c \equiv -1 \bmod 3$ and therefore the latter integer quotient is relatively prime to 3. □

With this, we can now prove

Proposition 4.7. *The cyclic algebras $\mathfrak{A}_c$ are division rings for all $c \geq 1$. In particular, the corresponding nonabelian groups $G_c = C_7 \rtimes C_{3^{c+1}}$ are all embeddable in division rings.*

Proof. By Lemma 4.3, the group G_c has the structure of [Am, (3B)] with the appropriate parameters m, n, t and r, and [Am, (3A)] holds since

$$s = \gcd(r - 1, m) = 3^c, \quad \text{and} \quad t = m/s = 7.$$

Furthermore, [Am, (3C)] is satisfied since we have $\gcd(n, t) = \gcd(3, 7) = 1$ and $\gcd(s, t) = \gcd(3^c, 7) = 1$. Now our algebra $\mathfrak{A}_c$ is identical to the cyclic algebra $\mathfrak{A}_{m,r}$ defined by [Am, page 364 (6)], so we can use [Am, Theorem 4(2)(a)] to prove that $\mathfrak{A}_c$ is a division ring. For this, we have to consider all prime factors q of n. But $n = 3$, so we need only deal with $q = 3$. Furthermore, we require a second prime p that divides m and satisfies certain additional properties. Obviously, we can only take $p = 7$.

Using $q = 3$ and $p = 7$, we compute certain quantities that are listed on [Am, page 365]. To start with, p^α is the highest power of p dividing m, so $\alpha = \alpha_p = 1$ and hence $m/p^\alpha = 3^c$. Next, n_p is the minimal positive integer satisfying $r^{n_p} \equiv 1 \bmod m/p^\alpha$ or equivalently $r^{n_p} \equiv 1 \bmod 3^c$. But we know that $r \equiv 1 \bmod 3^c$, so $n_p = 1$. In particular, $q \nmid n_p$. Similarly, μ_p is the minimal positive integer such that $r^{\mu_p} \equiv p^{\mu'} \bmod 3^c$ for some $\mu' \geq 0$ and again $r \equiv 1 \bmod 3^c$ implies that $\mu_p = 1$. Since $n_p = \mu_p = 1$, [Am, Lemma 9(1)] implies that $\delta' = \mu_p \delta_p / n_p = \delta_p$.

By definition, δ_p is the minimal positive integer with $p^{\delta_p} \equiv 1 \bmod m/p^\alpha$ or equivalently $7^{\delta_p} \equiv 1 \bmod 3^c$. Since $c \geq 1$, the preceding lemma implies that $\delta_p = 3^{c-1}$. Thus, by Lemma 4.6(ii) again, we see that $(p^{\delta'} - 1)/s = (7^{\delta_p} - 1)/3^c$ is relatively prime to $q = 3$. With this observation, [Am, Theorem 4(2)(a)] clearly yields the result. □

In view of Lemma 4.5 and Proposition 4.7, almost all of the Wedderburn components of $\mathbb{Q}[G_c]$ are division rings. Indeed, only $\mathfrak{A}_0 \cong \mathbf{M}_3(K)$ is not a division ring, and under the corresponding representation $\mathbb{Q}[G_c] \to \mathbb{Q}[G_0] \to \mathfrak{A}_0$, we see that $\mathfrak{Z}(G_c)$ maps to $\langle 1 \rangle$. In particular, the group of units of $\mathbb{Z}[\mathfrak{Z}(G_c)]$ maps to $\{\pm 1\}$ in this representation and hence these units cannot be used when one tries to apply Theorem 1.2 to the integral group ring $\mathbb{Z}[G_c]$.

References

[AP] R. Zh. Aleev and G. A. Panina, *The units of cyclic groups of orders 7 and 9*, (Russian) Izv. Vyssh. Uchebn. Zaved. Mat. **1999**, no. 11, 81–84; translation in Russian Math. (Iz. VUZ) **43** (1999), no. 11, 80-83 (2000).

[Am] S. A. Amitsur, *Finite subgroups of division rings*, Trans. AMS **80** (1955), 361-386.

[A] S. R. Arora, *A study of the Jordan decomposition in group rings*, Doctoral Thesis, Panjab University, Chandigarh, India, 1994.

[AHP] S. R. Arora, A. W. Hales and I. B. S. Passi, *The multiplicative Jordan decomposition in group rings*, J. Algebra **209** (1998), 533–542.

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

[BJ] Z. Božikov and Z. Janko, *A complete classification of finite p-groups all of whose noncyclic subgroups are normal*, Glas. Mat. Ser. III **44 (64)** (2009), 177-185.

[FT] A. Fröhlich and M. J. Taylor, *Algebraic Number Theory*, Cambridge Studies in Adv. Math. **27**, Cambridge Univ. Press, Cambridge, 1993.

[HPW] A. W. Hales, I. B. S. Passi and L. E. Wilson, *The multiplicative Jordan decomposition in group rings, II*, J. Algebra **316** (2007), 109–132; *Corrigendum*, J. Algebra **371** (2012), 665–666.

[H] G. Higman, *The units of group rings*, Proc. London Math. Soc. (2) **46** (1940), 231–248.

[L] Chia-Hsin Liu, *Multiplicative Jordan decomposition in group rings and p-groups with all noncyclic subgroups normal*, J. Algebra **371** (2012), 300–313.

[LP1] Chia-Hsin Liu and D. S. Passman, *Multiplicative Jordan decomposition in group rings of* 3*-groups*, J. Algebra and Applications **8** (2009), 505–519.

[LP2] Chia-Hsin Liu and D. S. Passman, *Multiplicative Jordan decomposition in group rings of* $2, 3$*-groups*, J. Algebra and Applications **9** (2010), 483–492.

[LP3] Chia-Hsin Liu and D. S. Passman, *Multiplicative Jordan decomposition in group rings of* 3*-groups, II*, Commun. Algebra, to appear.

[NZ] I. Niven and H. S. Zuckerman, *An Introduction to the Theory of Numbers*, Third edition, John Wiley & Sons, New York, 1972.

[P] D. S. Passman, *Nonnormal subgroups of p-groups*, J. Algebra **15** (1970), 352–370.

[R] P. Roquette, *Realisierung von Darstellungen endlicher nilpotenter Gruppen*, Arch. Math. **9** (1958), 241–250.