Proceedings of the Royal Society of Edinburgh: Section A Mathematics, 1–61, *2025*
DOI:10.1017/prm.2025.10013

On integral decomposition of unipotent elements in integral group rings

Leo Margolis,
Departamento de Matemáticas, Universidad Autónoma de Madrid, C/Francisco Tomás y Valiente 7, Madrid, Spain (leo.margolis@icmat.es)

Geoffrey Janssens
Institut de recherche en mathématique et physique, Université Catholique de Louvain, Chemin du Cyclotron 2, Louvain-la-Neuve, Belgium (geoffrey.janssens@uclouvain.be)

(Received 11 June 2024; revised 1 May 2025; accepted 6 May 2025)

Jespers and Sun conjectured in [27] that if a finite group G has the property ND, i.e. for every nilpotent element n in the integral group ring $\mathbb{Z}G$ and every primitive central idempotent $e \in \mathbb{Q}G$ one still has $ne \in \mathbb{Z}G$, then at most one of the simple components of the group algebra $\mathbb{Q}G$ has reduced degree bigger than 1. With the exception of one very special series of groups we are able to answer their conjecture, showing that it is true—up to exactly one exception. To do so, we first classify groups with the so-called SN property which was introduced by Liu and Passman in their investigation of the Multiplicative Jordan Decomposition for integral group rings.

The conjecture of Jespers and Sun can also be formulated in terms of a group $q(G)$ made from the group generated by the unipotent units, which is trivial if and only if the ND property holds for the group ring. We answer two more open questions about $q(G)$ and notice that this notion allows to interpret the studied properties in the general context of linear semisimple algebraic groups. Here we show that $q(G)$ is finite for lattices of big rank but can contain elements of infinite order in small rank cases.

We then study further two properties which appeared naturally in these investigations. A first which shows that property ND has a representation theoretical interpretation, while the other can be regarded as indicating that it might be hard to decide ND. Among others we show these two notions are equivalent for groups with SN.

Keywords: unipotent units; group ring; integral decompositions; SN groups; representation theory

2020 *Mathematics Subject Classification:* 16S34; 20C10; 20E99; 16U99

© The Author(s), 2025. Published by Cambridge University Press on behalf of The Royal Society of Edinburgh. This is an Open Access article, distributed under the terms of the Creative Commons Attribution licence (http://creativecommons.org/licenses/by/4.0), which permits unrestricted re-use, distribution and reproduction, provided the original article is properly cited.

https://doi.org/10.1017/prm.2025.10013 Published online by Cambridge University Press

1. Introduction

Already in the 1860s Weierstrass and Jordan introduced what students today learn to call the Jordan normal form of a matrix, cf. [18] for a historic overview. Reformulating this theory in a more general context for A an algebra over a field F every invertible element $a \in A$ can be uniquely decomposed as $a = a_u a_s$ such that a_u is unipotent, a_s is semisimple and $a_u a_s = a_s a_u$. When A contains a substructure B of interest, e.g. when F is a number field and B an order in A, one could ask, if for every invertible $b \in B$ one can still achieve this Jordan decomposition in B, i.e. whether $b_n, b_s \in B$ holds. Motivated by the study of units in integral group rings Hales, Luthar, and Passi asked when the above will happen for $A = \mathbb{Q}G$ the rational group algebra of a finite group G and $B = \mathbb{Z}G$ the integral group ring therein. Namely they defined a finite group G to have *Multiplicative Jordan Decomposition*, if for every unit $u \in \mathbb{Z}G$ the elements u_n and u_s, which a priori are defined in $\mathbb{Q}G$, actually live in $\mathbb{Z}G$, and asked which groups satisfy this property. Though quite a lot of research has been developed to this, the problem remains open in general, see §5.3 for more details and references.

A major breakthrough in this investigation came when it was observed in [17] that a group which has Multiplicative Jordan Decomposition also has the *Nilpotent Decomposition* (*ND* for short). Namely, G is said to have ND, if for every nilpotent element $n \in \mathbb{Z}G$ and every central idempotent $e \in \mathbb{Q}G$, the product ne still lies in $\mathbb{Z}G$. This property can be reformulated in terms of the associated unipotent elements $1 + n$. More precisely, denote by $\mathcal{U}(\mathbb{Z}G)$ the unit group in $\mathbb{Z}G$ and let

$$\mathcal{U}(\mathbb{Z}G)_{un} := \{\alpha \in \mathcal{U}(\mathbb{Z}G) \mid \alpha \text{ is unipotent } \}$$

be the set of unipotent elements in $\mathcal{U}(\mathbb{Z}G)$. Furthermore, for e a primitive central idempotent of $\mathbb{Q}G$ consider the set $\mathcal{E}_G(e) := \{\alpha \in \mathcal{U}(\mathbb{Z}G)_{un} \mid (\alpha - 1)e = \alpha - 1\}$ of unipotent elements projecting trivially to all components except the eth one. Denote by $\mathrm{PCI}(\mathbb{Q}G)$ the set of all the central primitive idempotents in $\mathbb{Q}G$. Now, by considering the group $q(G) := \langle \mathcal{U}(\mathbb{Z}G)_{un} \rangle / \langle \mathcal{E}_G(e) \mid e \in \mathrm{PCI}(\mathbb{Q}G) \rangle$ one obtains the alternative characterization:

$$q(G) = 1 \text{ if and only if } G \text{ has ND.} \tag{1}$$

Looking on the Wedderburn–Artin decomposition

$$\mathbb{Q}G = M_{n_1}(D_1) \oplus \cdots \oplus M_{n_\ell}(D_\ell), \tag{2}$$

where $M_{n_i}(D_i)$ denotes the $n_i \times n_i$-matrix ring over a division algebra D_i, one sees that property ND will hold if at most one of the n_i is bigger than 1, as the only unipotent element in a division algebra is the trivial one. This observation during the search for groups having ND led Jespers and Sun to define a group G as having *at most one matrix component*, if at most one of the n_i in (2) is bigger than 1 [27].

https://doi.org/10.1017/prm.2025.10013 Published online by Cambridge University Press

Their investigations even made them conjecture that these properties are in fact equivalent:

CONJECTURE 1.1 (Jespers–Sun, [27 Conjecture 1]). *A finite group* G *has ND if and only if* $\mathbb{Q}G$ *has at most one matrix component.*

Using the perspective of $q(G)$ in (1) and work of Kleinert-del Río [28], conjecture 1.1 can be elegantly reformulated in terms of unipotent elements. Namely, *it conjectures that* $\langle \mathcal{U}(\mathbb{Z}G)_{un} \rangle$ *is indecomposable.* From this point of view, their conjecture is even more surprising.

Note that the indecomposability statement of the group generated by all unipotent elements is of interest for arithmetic subgroups of arbitrary semisimple algebraic groups. In §4.2, we expand on this generality. In [27, Section 6] also the questions of when $q(G)$ is finite and whether there is a connection between the structure of $q(G)$ and the simple components of $\mathbb{Q}G$ were asked. The aim of this article is to answer all the problems above.

The latter two questions will be answered in §4. The study of property ND, with the solution of the conjecture above as the ending point, is done in §3. This, however, will require to classify in §2 the so-called SN groups, which is a problem of independent interest. Finally, in §5, we show that property ND has also a representation theoretical interpretation and yields concrete structural information when considered for specific subsets of all nilpotent elements. We will now explain the main results of this article in more detail.

1.1. Jespers–Sun conjecture and SN groups

Conjecture 1.1 has been the starting point for the investigations presented here. To describe our result on it, define a finite group G to be an *SSN group of unfaithful type*, if there exist primes p and q such that $G = P \rtimes Q$ for P a cyclic group of order p and Q a cyclic group of q-power order which acts non-trivially, but also not faithfully on P (the reason for the name will become clear later). Then our main result, obtained in Theorem 3.1, states:

THEOREM A. *Let* G *be a finite group which is not an SSN group of unfaithful type. Then* G *has ND if and only if either* $\mathbb{Q}G$ *has at most one matrix component or* $G = \langle a, b \mid a^4 = b^8 = 1, a^b = a^{-1} \rangle \cong C_4 \rtimes C_8$.

Hence we show that though the conjecture of Jespers and Sun is not correct in general, we know only about one counterexample and all the other potential counterexamples lie in a very specific family of groups. Interpreting the conjecture as a statement on how far the rational group algebra $\mathbb{Q}G$ determines properties of G and its integral group ring, this allows still to show a strong implication:

COROLLARY B. *Let* G *and* H *be groups such that* $\mathbb{Q}G \cong \mathbb{Q}H$ *and* G *has ND. Then* H *has* ND.

This result is obtained in corollary 3.2. Note, that there are many groups which have isomorphic rational group algebras [40, Theorem 14.1.11] and it is hence not

https://doi.org/10.1017/prm.2025.10013 Published online by Cambridge University Press

a typical situation that a property of G can be recovered from its group algebra over $\mathbb{Q}$.

A concept which turns out to be crucial to reduce our studies to certain classes of groups is that of *groups with SN*. Namely, G is said to have SN, if for every normal subgroup $N \trianglelefteq G$ and subgroup $Y \leq G$ one has $N \leq Y$ or $NY \trianglelefteq G$. This property was introduced by Liu and Passman to restrict the group-theoretical structure of those groups which have ND [31] (the name was later coined in [30]), so that a group which does not have SN will not have ND. Liu and Passman obtained some properties of groups with SN [33], but they were more interested in *groups with SSN*, which are those in which every subgroup has SN, as this property is a consequence of the Multiplicative Jordan Decomposition. They were able to achieve quite explicit descriptions of all the groups having SSN and we generalize their findings in some sense, giving restrictions on the structure of groups with SN. Recall that a group is said to be *Dedekind*, if all its subgroups are normal.

THEOREM C. *Let* G *be a finite group. Then* G *is a group with SN if and only if it is one of the following types:*

(i) *a group with SSN,*
(ii) $G \cong P \rtimes H$ *with* P *an elementary abelian Sylow* p*-subgroup and* H *a* p′*-Hall subgroup which is Dedekind with cyclic or generalized quaternion Sylow subgroups such that the action of* H *on* P *is irreducible and faithful,*
(iii) G *has a unique minimal normal subgroup* S *and* S *is not solvable and* G/S *Dedekind,*
(iv) $\mathbb{Q}G$ *has one matrix component.*

As remarked before, groups with SSN have been classified in [33], so that we have a precise group-theoretical descriptions for those groups with SN which do not have one matrix component.

Theorem C is proven in §2 by dividing it into three separate subcases: nilpotent groups (which are handled in Proposition 2.8), solvable non-nilpotent groups (Proposition 2.17), and non-solvable groups (Proposition 2.18). The classification of nilpotent groups with SN turns out to be the hardest of those. With those preparations, we then prove Theorem A and corollary B in §3, where the former is obtained by dividing in the same cases.

1.2. A general perspective on the obstruction to have ND

In §4, we investigate the group $q(G)$ which by (1) measures how far a given group G is from having ND or in other words it as an obstruction to have ND. Jespers and Sun [27, Section 6] formulated the following two problems about $q(G)$:

(1) Classify the finite groups G such that $q(G)$ is finite. ([27] Problem 1, §6)
(2) Find a connection between the structure of $q(G)$ and the simple components of $\mathbb{Q}G$. ([27] Problem 2, §6)

https://doi.org/10.1017/prm.2025.10013 Published online by Cambridge University Press

In §4.1, we give answers to both questions. More precisely, Proposition 4.1 and the proof of Theorem 4.2 will show that for unipotent elements to have an integral decomposition is not truly connected to the simple components of $\mathbb{Q}G$. The relationship is rather a combination of the congruence level of $\mathbb{Z}G$ in the maximal order of $\mathbb{Q}G$ on the one hand and the rank of the simple matrix components of $\mathbb{Q}G$ on the other hand.

Besides, the second problem fits in a more general context of semisimple algebraic groups. More precisely, let F be a number field and S a non-empty finite set of places of F containing the Archimedean places. Furthermore, let $\mathbf{G}$ be a simply connected semisimple algebraic group. In particular, $\mathbf{G}$ is a direct product of simply connected almost-simple algebraic F-subgroups [41, Theorem 2.6], say $\mathbf{G} = \prod_{i=1}^{m} \mathbf{G}_i$. Finally let Γ be an S-arithmetic subgroup of $\mathbf{G}(F)$. In Proposition 4.7, we obtain the following:

Proposition D. *Consider the notations above and suppose S-rank$(\mathbf{G}_i(F)) \geq 2$ for all anisotropic $\mathbf{G}_i(F)$. Then, $|q(\Gamma)| < \infty$. In particular, in this case, finiteness of $q(\Gamma)$ does not depend on the chosen* S*-arithmetic subgroup Γ.*

In the case that $F = \mathbb{Q}, \mathbf{G}(F) = \mathrm{SL}_1(\mathbb{Q}G)$, and $\Gamma = \mathrm{SL}_1(\mathbb{Z}G)$, we give in Proposition 4.1 a precise and down-to-earth upper bound. Our arguments heavily rely on solutions of the Congruence Subgroup Problem.

Next, recall that a finite dimensional simple algebra is called *exceptional of type II* if it is $\mathrm{M}_2(D)$ with D either $\mathbb{Q}$, an imaginary quadratic extension of $\mathbb{Q}$ or a totally definite quaternion algebra with centre $\mathbb{Q}$.

In Theorem 4.2, we show the Theorem below, saying that the finiteness of $q(G)$ depends on the presence of exceptional components. For instance, if $3 \nmid |G|$ and $\mathbb{Q}G$ has a simple component isomorphic to $M_2(\mathbb{Q})$, then by [3, Remark 6.17] G is an extension of D_8. In §4.1, we formulate some condition on the exponent of the preimage of D_8 in G, called $(\star)$, which, in turn, we prove to have an impact on the size of $q(G)$.

Theorem E. *Let* G *be a finite group. Then the following hold:*

(i) *If $\mathbb{Q}G$ has no exceptional components of type II, then* q*(*G*) is finite.*
(ii) *If* G *has order at most* 16*, then* q*(*G*) is finite.*
(iii) *If* G *has order bigger than* 16*, maps onto* D_8 *and this surjection satisfies $(\star)$, then* q*(*G*) is an infinite non-torsion group.*

Interestingly the group $C_4 \rtimes C_8$ in Theorem A is the smallest group fitting in none of the cases covered by Theorem E.

1.3. A representation theoretical and local look at ND

In §5, we will introduce two more properties which appeared in our investigations of the nilpotent decomposition. The first is a purely representation-theoretical property, called DK, namely that any two non-equivalent irreducible $\mathbb{Q}$-representations have different kernels. We show in Theorem 5.2 that this is the case for groups with at most one matrix component, but also other interesting classes of groups are show

https://doi.org/10.1017/prm.2025.10013 Published online by Cambridge University Press

in §5.1 to have that property. We then study in §5.2 what one could call a partial nilpotent decomposition, namely that the nilpotent decomposition does hold for those nilpotent elements of $\mathbb{Z}G$ which are the easiest to construct and which we call bicyclic nilpotent. When a decomposition does hold for all such elements, we call a group bicyclic resistant. The reason for the definition of the SN property is essentially that a group which does not have SN is also not bicyclic resistant. We will show, however, that the class of not bicyclic resistant groups is bigger than the class of groups with SN, though it does not incorporate some classes relevant in the study of the ND property. Finally, we connect these two new notions by showing:

THEOREM F. *Let* G *be a finite group with SN. Then the following are equivalent:*

(1) G *is bicyclic resistant.*
(2) G *is supersolvable or* $\mathbb{Q}G$ *has one matrix component.*
(3) G *has DK.*

This result is proven in Theorem 5.16.

1.4. Conventions and notations

G will always denote a finite group. If $\mathbb{Q}G \cong \prod_i \mathrm{M}_{n_i}(D_i)$ is the Wedderburn–Artin decomposition of the semisimple algebra $\mathbb{Q}G$, then we call the factors $\mathrm{M}_{n_i}(D_i)$ *simple components* of $\mathbb{Q}G$. Recall that n is called the *reduced degree* of the simple component $M_n(D)$. If a component has reduced degree 2 or more we will speak of a *matrix component*. The set $\mathrm{PCI}(G)$ denotes the primitive central idempotents of $\mathbb{Q}G$.

Moreover, we use standard group-theoretical notation: for a group G, we denote by G' the derived subgroup of G, by $\mathcal{Z}(G)$ the centre of G, by $\Phi(G)$ the Frattini subgroup of G, by g^G the conjugacy class of an element $g \in G$ in G, and by $\mathrm{Soc}(G)$ the socle of G. Moreover for $g, h \in G$, we set $g^h = h^{-1}gh$ and $[g,h] = g^{-1}h^{-1}gh = g^{-1}g^h$. A cyclic group of order n is denoted C_n, a dihedral group of order $2n$ by D_{2n}, an alternating group of degree n by A_n and Q_{2^n} denotes the generalized quaternion group of order 2^n, i.e.

$$Q_{2^n} = \langle a, b \mid a^{2^{n-1}} = b^4 = 1,\ b^2 = a^{2^{n-2}},\ a^b = a^{-1} \rangle.$$

When speaking about generalized quaternion groups, we assume them to be non-abelian, i.e. at least of order 8.

If H is a subgroup of G we denote two elements in the rational group algebra $\mathbb{Q}G$ as

$$\widetilde{H} = \sum_{h \in H} h \quad \text{and} \quad \widehat{H} = \frac{1}{|H|} \sum_{h \in H} h.$$

2. Description of groups with SN

Recall that a group G has the *SN property* if for every normal subgroup N of G and every subgroup $Y \leq G$ either $N \subseteq Y$ or $NY \trianglelefteq G$. The main goal of this

https://doi.org/10.1017/prm.2025.10013 Published online by Cambridge University Press

section is to prove Theorem C. We separate this in essentially three steps: the nilpotent groups with SN (which are handled in Proposition 2.8), the solvable non-nilpotent groups with SN (Proposition 2.17), and the non-solvable groups with SN (Proposition 2.18). The combination of these cases then gives exactly Theorem C.

Recall that the group G *has SSN* if every subgroup has SN. Such groups have been classified in [33]. In fact, we will give a precise classification of groups with SN in case G is non-nilpotent. Namely, in Theorem C, the non-nilpotent groups with SN are exactly those from (iii) and solvable non-nilpotent groups with SN. As proven in Proposition 2.17, the latter come in two families with one having SSN and the other being the groups from (ii). Though we have made no attempt to classify groups with one matrix component, some restrictions can be filtered out of our proofs.

2.1. Background results on groups with SN

If every subgroup of G is normal, then G obviously has SN. Recall that these groups are called *Dedekind groups* and have been classified by Baer and Dedekind:

THEOREM 2.1 ([37, Theorem 1.8.5.]). G *is a Dedekind group if and only if it is abelian or* $G \cong Q_8 \times C_2^n \times A$ *for some* $n \in \mathbb{N}_0$ *and* A *an abelian group of odd order.*

Many basic properties of group with SN and SSN have been studied by Liu and Passman and we will use several of their results. For the convenience of the reader, we collect them here as well as some other results we will need.

LEMMA 2.2 ([33, Lemma 2.1]). *Let* G *be a group with SN and* N *a non-trivial normal subgroup of* G. *If* N *is not cyclic, then* G/N *is a Dedekind group. Moreover, if* H *is a subgroup of* G *such that* $H \cap N = 1$, *then* $NH \trianglelefteq G$ *and* H *is a Dedekind group.*

For the description of solvable groups with SN, the following lemma will be key.

LEMMA 2.3 ([33, Lemma 2.4]). *Let* G *be a group with SN,* $P \in Syl_p(G)$ *such that* $P \trianglelefteq G$ *and* $G = P \rtimes H$ *for a* p′*-group* H *which acts non-trivially on* P. *Then* P *is elementary abelian and* H *acts irreducibly on* P. *Moreover, if* H *acts non-faithfully, then* G *is an SSN group of unfaithful type.*

The following is [33, Lemma 2.5. (1)] where it was stated for groups with SSN. However, its proof only uses properties of groups with SN, so that we restate it in this form. The moreover part has been added and follows directly by using lemma 2.2.

LEMMA 2.4. *Let* G *be a group with SN with non-trivial normal* p*-subgroup* P_0, *say contained in the Sylow* p*-subgroup* P *of* G. *Then* G *contains a nilpotent* p*-complement* H, *we have* $P_0H \trianglelefteq G$ *and* $G = PH$. *In particular* G *is solvable. Moreover, if* P_0 *is not cyclic then* H *is Dedekind and* $P \trianglelefteq G$.

Proof. Suppose P_0 is not cyclic. Then lemma 2.2 implies that G/P_0 is Dedekind. Therefore $P/P_0 \trianglelefteq G/P_0$, which implies that $P \trianglelefteq G$. The proof of the rest of the statement is completely as the proof of [33, Lemma 2.5. (1)]. □

https://doi.org/10.1017/prm.2025.10013 Published online by Cambridge University Press

We will also need a particular way to construct primitive central idempotents of $\mathbb{Q}G$. For this, we will use the theory of strong Shoda pairs. For now, we give definitions that are sufficient for this section and refer the reader to §3.1 and [24, Chapter 3] for more details. Suppose G is metabelian. Then all the irreducible $\mathbb{Q}$-representations of G are monomial, i.e. they all arise as the induced representations λ^G of a linear representation λ of some subgroup H of G. In that case, one considers $K = \ker(\lambda)$ and denotes by $e(G, H, K)$ the associated primitive central idempotent of $\mathbb{Q}G$.

LEMMA 2.5. *[24, Theorem 3.5.12 and Exercise 3.4.4] Assume* G *is a metabelian group and* A *a maximal abelian subgroup of* G *containing* G′. *Then the primitive central idempotents of* $\mathbb{Q}G$ *are the elements* $e(G, H, K)$ *where* H *and* K *are subgroups of* G *such that* H *is a maximal element of the set* $\{B \leq G \mid A \leq B \text{ and } B' \leq K \leq B\}$ *and* H/K *is cyclic. Moreover* $e(G, H, K_1) = e(G, H, K_2)$ *if and only if* K_1 *and* K_2 *are conjugate in* G.

As the construction of central idempotents from normal subgroups or Shoda pairs is not always possible or practical, we will sometimes need to work with the central idempotents coming from characters instead. We recall their construction:

THEOREM 2.6 *[34, Theorem 2.1.6] Let* F *be a field of characteristic* 0 *and* χ *the character of a simple* FG*-module* L *with* $D = End_{FG}(L)$. *Then the primitive central idempotent of the Wedderburn component of* FG *corresponding to* χ *is*

$$\frac{\chi(1)}{[D : F]|G|} \sum_{g \in G} \chi(g^{-1})g.$$

In practice, we will use the following lemma.

LEMMA 2.7. *Let* $M_k(D)$ *be a simple component of the group algebra* FG, *for* F *a field of characteristic* 0, *with character* χ *and corresponding primitive central idempotent* e. *Moreover, let* $n = \sum_{g \in G} \alpha(g)g$ *be a generic element in* FG. *Then the coefficient of* ne *at* g *can be expressed in the two forms*

$$\frac{k}{|G|} \sum_{h \in G} \alpha(gh^{-1})\chi(h^{-1}) = \frac{k}{|G|} \sum_{h \in G} \alpha(h)\chi(g^{-1}h).$$

Proof. Note that $\dim_F(eFG) = k^2[D : F]$ and $\chi(1) = k[D : F]$. So the primitive central idempotent e corresponding to this component by Theorem 2.6 has the form

$$e = \frac{\chi(1)}{[D : F]|G|} \sum_{g \in G} \chi(g^{-1})g = \frac{k}{|G|} \sum_{g \in G} \chi(g^{-1})g.$$

https://doi.org/10.1017/prm.2025.10013 Published online by Cambridge University Press

Hence for the product we have

$$ne = \frac{k}{|G|}\sum_{g\in G}\sum_{h\in G}\alpha(g)\chi(h^{-1})gh$$
$$= \frac{k}{|G|}\sum_{g\in G}\left(\sum_{h\in G}\alpha(gh^{-1})\chi(h^{-1})\right)g = \frac{k}{|G|}\sum_{g\in G}\left(\sum_{h\in G}\alpha(h)\chi(g^{-1}h)\right)g.$$

So the coefficient of ne at g is

$$\frac{k}{|G|}\sum_{h\in G}\alpha(gh^{-1})\chi(h^{-1}) = \frac{k}{|G|}\sum_{h\in G}\alpha(h)\chi(g^{-1}h).$$

□

2.2. Nilpotent groups

The goal of this subsection is to describe nilpotent groups with SN:

THEOREM 2.8. *Let* G *be a nilpotent group with SN. Then it has property SSN or* $\mathbb{Q}G$ *has at most one matrix component.*

To start, one can quickly reduce to studying p-groups.

LEMMA 2.9. *Let* G *be a nilpotent group with SN which is not a Dedekind group. Then* G *is a* p*-group.*

Proof. Assume P and Q are a non-cyclic p-Sylow and a q-Sylow subgroup of G respectively. Then $P \trianglelefteq G$ and so by lemma 2.2 we know that Q is a Dedekind group. But as this argument applies to every prime, this means that G is Dedekind, contradicting the assumption. □

Recall that it was shown by Liu and Passman that p-groups with SSN coincide with the so-called NCN groups.

LEMMA 2.10. *[33, Proposition 2.2] Let* G *be a* p*-group. Then* G *has SSN if and only if every non-cyclic subgroup of* G *is normal.*

Now, the advantage of this is that non-normal subgroups of p-groups with SN are very restricted as the following result shows. This is a variation of [30, Lemma 3.2] which includes 2-groups.

LEMMA 2.11. *Let* G *be a group with SN and* Q *a subgroup of* G *which is not normal.*

(a) *If there exists* $N \leq Q$ *such that* $N \trianglelefteq G$*, then* N *is cyclic.*
(b) *Now assume* G *is a* p*-group. Then* Q *is cyclic, elementary abelian or isomorphic to a quaternion group of order* 8*. If moreover,* $N \leq Q$ *such that* $N \trianglelefteq G$ *and* $\mathrm{N} \neq 1$*, then* Q *is cyclic or isomorphic to* Q_8*.*

https://doi.org/10.1017/prm.2025.10013 Published online by Cambridge University Press

We will need the following well-known classical result.

LEMMA 2.12. *[20, III, Satz 8.2] Let* G *be a* p*-group which contains exactly one cyclic subgroup of order* p*. Then* G *is cyclic or a generalized quaternion group.*

Proof of lemma 2.11. Assume N is a normal subgroup of G contained in Q. If N is not cyclic, then G/N is Dedekind by lemma 2.2, so that $Q/N \trianglelefteq G/N$, which implies the contradiction $Q \trianglelefteq G$. So part (a) follows.

The proof of part (b) is by two 'iterations'. First assume N with the described properties exists. Then Q is cyclic or a generalized quaternion group: indeed, if $n \in N$ has order p and $q \in Q$ is an element of order p not lying in $\langle n \rangle$, then $\langle n \rangle \langle q \rangle \trianglelefteq G$, as G is a group with SN. But this contradicts part (a) as $\langle n \rangle \langle q \rangle$ is not cyclic. So Q contains exactly one subgroup of order p, implying Q is cyclic or generalized quaternion by lemma 2.12. Next we claim that, independently from the existence of N, the group Q is cyclic, elementary abelian or generalized quaternion. For this assume Q is maximal non-normal and let M be a subgroup of G containing Q such that $[M : Q] = p$. By the maximality of Q, we get $M \trianglelefteq G$ and so $\Phi(M) \trianglelefteq G$, where $\Phi(M)$ denotes the Frattini subgroup of M. As Q is a maximal subgroup of M, it contains $\Phi(M)$ and so $\Phi(M)$ is cyclic by part (a). If $\Phi(M) = 1$, then Q is elementary abelian. If $\Phi(M) \neq 1$, then Q is cyclic or generalized quaternion by the first claim proved in this paragraph.

It remains to show that in the two claims proven in the previous paragraph we can replace generalized quaternion groups by quaternion groups of order 8. Assume first N exists and Q is a generalized quaternion with $n \in Q$ the unique involution. Then $Q/\langle n \rangle$ is a dihedral group of order $|Q|/2$. If $|Q|/2 \geq 8$, this implies, by the claim proven in the previous paragraph and the fact that the SN property is inherited by quotients, that $Q/\langle n \rangle \trianglelefteq G/\langle n \rangle$. This would imply $Q \trianglelefteq G$. So $|Q|/2 \leq 4$ which means that Q is the quaternion group of order 8. Now again ignore the existence of N, let Q be again maximal non-normal, M a normal subgroup of G containing Q such that $[M : Q] = p$ and assume that Q is generalized quaternion. Then as before $\Phi(M) \trianglelefteq G$ and $\Phi(M) \neq 1$, as Q is not elementary abelian. It follows that the unique involution of Q is central in G and so the same argument as before can be used to show $|Q| = 8$. □

With these preparations, we are ready to show that groups with SN but without SSN necessarily have one matrix component. We will separate two cases.

PROPOSITION 2.13. *Let* G *be a* p*-groups which has SN, but not SSN. Assume that either* p *is odd, or* p = 2 *and* G *contains an elementary abelian subgroup* Q *which is not normal. Then* G *has at most one matrix component.*

Proof. If $p = 2$ let Q be the elementary abelian subgroup of G which is not normal. When p is odd, by lemma 2.10, G contains a non-cyclic subgroup Q which is not normal in G. Then Q is elementary abelian by lemma 2.11. We choose Q maximal with these properties, in particular for $Q \lneq M \leq G$ we have $M \trianglelefteq G$. By lemma 2.11, if Q contains a subgroup N which is normal in G, then $N = 1$ (note that this is trivial if $|Q| = 2$). In particular, we have $\mathcal{Z}(G) \cap Q = 1$.

Claim 1: $\mathcal{Z}(G)$ is cyclic.

https://doi.org/10.1017/prm.2025.10013 Published online by Cambridge University Press

Assume first that $\mathcal{Z}(G)$ contains an elementary abelian subgroup $\langle z_1\rangle \times \langle z_2\rangle$. Then, by our choice of Q and the fact that $\mathcal{Z}(G) \cap Q = 1$, we have $Q\langle z_1\rangle \trianglelefteq G$ and $Q\langle z_2\rangle \trianglelefteq G$. This implies that $[G, Q] \leq Q\langle z_1\rangle$ and $[G, Q] \leq Q\langle z_2\rangle$, respectively. So $[G, Q] \leq Q\langle z_1\rangle \cap Q\langle z_2\rangle = Q$, which would imply that $Q \trianglelefteq G$. Hence $\mathcal{Z}(G)$ contains at most one subgroup of order p. As $\mathcal{Z}(G)$ cannot be generalized quaternion, because such a group is not abelian, the claim follows from lemma 2.12.

We denote an element of order p in $\mathcal{Z}(G)$ by z.

Claim 2: $G' = \langle z\rangle$. Moreover, if $g \in G$ such that $z \notin \langle g\rangle$, then $g^p = 1$.

Let $g, h \in G$ such that $[g, h] \neq 1$. Assume first that $z \notin \langle g\rangle$. Note that we can assume this without changing the value of $[g, h]$ when p is odd. As G is a group with SN, this implies $\langle g, z\rangle = \langle g\rangle \times \langle z\rangle \trianglelefteq G$. As z is central and G is a p-group we hence get $[G, g] \subseteq \langle g^p\rangle \times \langle z\rangle$. If $g^p \neq 1$, then we have $[G, g^p] \subseteq \langle g^{p^2}\rangle$, $[G, g^{p^2}] \subseteq \langle g^{p^3}\rangle$, …,$[G, g^{\circ(g)/p}] = 1$, implying $g^{\circ(g)/p} \subseteq \mathcal{Z}(G)$ which contradicts Claim 1, as $z \notin \langle g\rangle$ by assumption. Hence $g^p = 1$ and $[G, g] \subseteq \langle z\rangle$, in particular $[g, h] \in \langle z\rangle$. Now suppose that z lies in every non-trivial subgroup of $\langle g, h\rangle$, i.e. $\langle g, h\rangle$ is a generalized quaternion group. If $\langle g, h\rangle$ has order 8, then $[g, h] = z$ and there is nothing more to prove. So assume $\langle g, h\rangle \cong Q_{2^m}$ for some $m \geq 4$. Say $g^{2^{m-1}} = h^4 = 1$ and $g^h = g^{-1}$. Note that $h^g = hg^2$. As Q is elementary abelian and maximal non-normal, we get $\langle Q, h\rangle \trianglelefteq G$. As also $Q \times \langle z\rangle \trianglelefteq G$, we have that $[h, q]$ has order at most 2 and so hq has order at most 4 for every $q \in Q$. Note for this that $h^2 = z$ is central in G. But as $h^g = hg^2 \in \langle Q, h\rangle$, we have $g^2 \in \langle Q, h\rangle$, a contradiction, since g^2 has order at least 8.

In particular Claim 2 implies that G is metabelian. Moreover, there exists a cyclic subgroup C of G containing z such that $A = C \times Q$ is a maximal abelian subgroup of G. We are now finally ready to prove that G has at most one matrix component by applying lemma 2.5. So assume $\mathbb{Q}e(G, H, K)$ is a non-commutative component of $\mathbb{Q}G$. As K lies in the kernel of a representation corresponding to this component, we have $G' \not\leq K$, i.e. $z \notin K$ by Claim 2. Hence, again by Claim 2, the unique maximal element of $\{B \leq G \mid A \leq B \text{ and } B' \leq K \leq B\}$ is A and $e(G, H, K) = e(G, A, K)$ with A/K a cyclic group. By lemma 2.5, it is thus sufficient to prove that all subgroups of A which do not contain z and have cyclic quotients are conjugate. We call such subgroups 'good'. Note that good subgroups are elementary abelian, so contained in $\langle z\rangle \times Q$. A good subgroup U is determined by $(\langle z\rangle \times Q)/U$ and these quotients are exactly the images of the groups $\langle zq\rangle$, where q runs through the elements of Q. Hence there are $|Q|$ good subgroups. It is clear that Q itself is a good subgroup. So we need to prove that Q has $|Q|$ conjugates in G, i.e. $[G : N_G(Q)] = |Q|$. By the maximality of Q, and since $z \in N_G(Q)$, we have $N_G(Q) \trianglelefteq G$. As G' is a central subgroup of order p, the group $G/N_G(Q)$ is elementary abelian. So we can view $V = Q \times G/N_G(Q)$ as an $\mathbb{F}_p$-vector space of dimension $|Q| + |G/N_G(Q)|$. We define a non-degenerate symplectic bilinear form

$$V \times V \to \langle z\rangle, \quad (v, w) \mapsto [v, w].$$

As no element of $G/N_G(Q)$ leaves all elements of Q fixed under conjugation, Q and $N_G(Q)$ are maximal isotropic subspaces of V, so that each of them has dimension $\frac{1}{2} \cdot (|Q| + |G/N_G(Q)|)$ by [20, II, Satz 9.11], i.e. $|G/N_G(Q)| = |Q|$. □

https://doi.org/10.1017/prm.2025.10013 Published online by Cambridge University Press

By lemma 2.11, it hence remains to study the case that G is a 2-group and all the non-normal subgroups of G are isomorphic to a quaternion group of order 8. This turns out to be surprisingly hard. We would be very interested in an easier proof.

LEMMA 2.14. *Let* G *be a* 2*-group which has SN, but not SSN. Then every involution of* G *is central if and only if* $G \cong Q_8 \times Q_8$.

Proof. Assume that every involution in G is central. We first note that G is not a generalized quaternion group. Indeed Q_8 and Q_{16} have SSN [30, Theorem 2.3, BJ6] and if $G = \langle g, h \mid g^{2^n} = h^4 = 1,\ g^{2^{n-1}} = h^2,\ g^h = g^{-1}\rangle$ for some $n \geq 4$, then G does not have SN. This can be observed by taking $N = \langle g^4\rangle$, $Y = \langle h\rangle$, so that $N \not\subseteq Y$ and $NY \not\trianglelefteq G$ as $h^g = hg^2 \notin NY$. In particular, the centre of G is not cyclic.

By lemmas 2.10 and 2.11, we can assume G contains a non-normal subgroup Q isomorphic to Q_8. We fix $a, b \in Q$ as generators of Q and $c = a^2$. We will prove several small facts on G which will lead to the proof of the lemma.

(i) $\mathcal{Z}(G)$ has rank 2:
$\mathcal{Z}(G)$ is not cyclic, as G is not generalized quaternion. So assume the rank of $\mathcal{Z}(G)$ is bigger than 2. Say $z_1, z_2 \in \mathcal{Z}(G)$ are independent elements of order 2 such that $(\langle z_1\rangle \times \langle z_2\rangle) \cap Q = 1$. Then $Q \times \langle z_1\rangle$ and $Q \times \langle z_2\rangle$ are both normal subgroups of G. Hence $[G, Q] \leq Q\langle z_1\rangle \cap Q\langle z_2\rangle = Q$ which would imply $Q \trianglelefteq G$.

Convention: We let $z \in G$ be an involution not lying in Q, so $\langle c\rangle \times \langle z\rangle$ is the unique maximal elementary abelian subgroup of G.

(ii) $|G/\Phi(G)| \leq 16$, i.e. G is at most 4-generated:
This follows from (i) using [35, Four Generator Theorem].

(iii) The groups $\langle a\rangle$, $\langle b\rangle$, and $\langle ab\rangle$ are not normal in G:
Say $\langle a\rangle \trianglelefteq G$. As $\langle a\rangle \not\subseteq \langle b\rangle$ and G has SN this implies $\langle a\rangle\langle b\rangle = Q \trianglelefteq G$, a contradiction. Similarly $\langle b\rangle$ and $\langle ab\rangle$ are not normal in G.

(iv) $a^G = \{a, a^{-1}, az, a^{-1}z\}$, $b^G = \{b, b^{-1}, bz, b^{-1}z\}$, and $(ab)^G = \{ab, (ab)^{-1}, abz, (ab)^{-1}z\}$:
As G has SN we have $\langle a\rangle \times \langle z\rangle \trianglelefteq G$. So by (iii) there is $g \in G$ such that $a^g = az$ or $a^g = a^{-1}z$. As $a^b = a^{-1}$ and $(az)^b = a^{-1}z$ the claim for a^G follows. Similarly the conjugacy classes of b and ab follow from (iii).

(v) For $g \in G$, we have $g^2 \in C_G(Q)$:
By (iv) we have $[g, a] \in \{1, c, z, cz\}$, in any case a central element of order at most 2. So $[g^2, a] = [g, a]^g[g, a] = 1$. Of course for b and ab we similarly have $[g^2, b] = [g^2, ab] = 1$.

(vi) If $g \in C_G(Q)$ and $g \notin \langle c\rangle$, then $c \notin \langle g\rangle$:
This is clear if g has order 2. So assume the order of g is 2^n for $n \geq 2$ and such that $g^{2^{n-1}} = c$. Then $(g^{2^{n-2}}a)^2 = c \cdot c = 1$, so $g^{2^{n-2}}a$ is an involution. Here we used that $g \in C_G(Q)$. As $g^b = g$ we have $(g^{2^{n-2}}a)^b = g^{2^{n-2}}a^{-1}$, so this involution is not central, contradicting the assumptions on G.

https://doi.org/10.1017/prm.2025.10013 Published online by Cambridge University Press

(vii) If $g \notin N_G(Q)$, but g is centralizing a, b, or ab, then $c \notin \langle g \rangle$:
Say $g \in C_G(a)$, $\circ(g) = 2^n$ and assume $c \in \langle g \rangle$. As $g \notin N_G(Q)$, we must have $g \notin N_G(\langle b \rangle)$, so $b^g = b^{\pm 1}z$ by (iv). Note that $g^2 \in C_G(Q)$ by (v). So $g^{2^{n-2}}a$ is an involution with $(g^{2^{n-2}}a)^b = g^{2^{n-2}}ac$, if $n > 2$, or $(g^{2^{n-2}}a)^b \in \{gaz, gacz\}$, if $n = 2$. In any case we would have a non-central involution.

(viii) If $g \notin N_G(\langle a \rangle)$ and $g \notin N_G(\langle b \rangle)$, then $g \in N_G(\langle ab \rangle)$. The same holds for every permutation of a, b, and ab:
If $g \notin N_G(\langle a \rangle)$ and $g \notin N_G(\langle b \rangle)$, then $a^g = a^{\pm 1}z$ and $b^g = b^{\pm 1}z$, so that

$$(ab)^g = a^{\pm 1}b^{\pm 1}zz \in \{ab, a^{-1}b, ab^{-1}, a^{-1}b^{-1}\}.$$

Noting that $a^{-1}b = ab^{-1} = (ab)^{-1}$ and $a^{-1}b^{-1} = ab$, the claim follows.

(ix) $N_G(Q) \trianglelefteq G$ and $G/N_G(Q) \cong C_2 \times C_2$:
$N_G(Q) \trianglelefteq G$ follows, as $N_G(Q)$ contains z and is thus bigger than Q. By (v) the group $G/N_G(Q)$ is elementary abelian. If $G/N_G(Q) \cong C_2$ would hold, then by (viii) one of $\langle a \rangle$, $\langle b \rangle$, or $\langle ab \rangle$ would be normal in G, which would contradict (iii). On the other hand, if $g, h \notin N_G(\langle a \rangle)$, then $gh \in N_G(\langle a \rangle)$ by (iv). This implies that G has only three non-trivial ways to act on the cyclic subgroups of the normal subgroup $Q \times \langle z \rangle$, implying $|G/N_G(Q)| \leq 4$.

Convention: By (viii) and (ix), we can choose $x, y \in G$ such that $\circ(x) \geq \circ(y)$ and $x \notin N_G(\langle a \rangle)$, $x \in N_G(\langle b \rangle)$ as well as $y \in N_G(\langle a \rangle)$, $y \notin N_G(\langle b \rangle)$. To assure the condition $\circ(x) \geq \circ(y)$ we might have to rename the elements a and b.

(x) $C_G(Q) = \Phi(G)$ and $\{a, b, x, y\}$ is a minimal generating set of G:
First note that if $g \in G$, then $Q^g \leq Q\langle z \rangle$ by (iv). As z is central, this implies that for every $h \in C_G(Q)$, the element h is also centralizing Q^g. Hence $h^g \in C_G(Q)$, implying that $C_G(Q)$ is normal in G. Now, by the action of a, b, x, and y on $Q \times \langle z \rangle$, we see that no element of the form $a^\alpha b^\beta x^\gamma y^\delta$ with at least one of the α, β, γ, and δ odd is centralizing Q. Hence the images of a, b, x, and y in $G/C_G(Q)$ generate an elementary abelian subgroup of order 16. By (ii), this is a maximal elementary abelian quotient of G, so the well-known properties of Frattini subgroups of p-groups, as recorded for instance in [20, III, Section 3], imply the claim.

(xi) $G^2 = \Phi(G)$. Moreover for any $g, h \in G$ we have $[g, h]^g = [g, h]$ and $(gh)^2 = g^2h^2[h, g]$:
The equation $G^2 = \Phi(G)$ holds in every 2-group [20, III, Satz 3.14(b)]. Let $i \in G$ be an involution so that $i \notin \langle g \rangle$. Hence $\langle g \rangle \times \langle i \rangle \trianglelefteq G$ and so $[g, h] \in \langle g^2, i \rangle$, which implies $[g, h]^g = [g, h]$. Moreover, this gives $(gh)^2 = g^2h[h, g]h = g^2h^2[h, g]$.

(xii) For $g, h \in G$, we have $[g^2, h] = [g, h]^2$ and $[g^2, h] \in \langle g^4 \rangle \cap \langle h^4 \rangle$. Furthermore, $\langle g^2 \rangle \trianglelefteq G$:

https://doi.org/10.1017/prm.2025.10013 Published online by Cambridge University Press

In general $[g^2,h]=[g,h]^g[g,h]$, so $[g^2,h]=[g,h]^2$ holds by (xi). Moreover, if $i,j\in G$ are involutions such that $i\notin\langle g\rangle$ and $j\notin\langle h\rangle$, then $\langle g\rangle\times\langle i\rangle$ and $\langle h\rangle\times\langle j\rangle$ are normal subgroups of G, so that $[g,h]\in\langle g^2,i\rangle$ and $[g,h]\in\langle h^2,j\rangle$. So $[g^2,h]=[g,h]^2\in\langle g^4\rangle\cap\langle h^4\rangle$. Finally, as $\langle g\rangle\times\langle i\rangle\trianglelefteq G$ we have $[g,G]\subseteq\langle g^2,i\rangle$, so that $[g^2,G]\subseteq\langle g^4\rangle$ by the previous, implying that $\langle g^2\rangle\trianglelefteq G$.

(xiii) If $g,h\in C_G(Q)$ and both have order at least 4, then $\langle g\rangle\cap\langle h\rangle\neq 1$:

Say $\langle g\rangle\cap\langle h\rangle=1$. By (vi), we know that c is not contained in $\langle g\rangle$ or $\langle h\rangle$. So we can assume $z\in\langle g\rangle$ and $cz\in\langle h\rangle$. Assume first that $\circ(g)=2^n\geq 8$ and say $\circ(h)=2^m$. By (xii) and the assumption $\langle g\rangle\cap\langle h\rangle=1$, we have $[g^2,h]=1$, so that $(g^{2^{n-2}}h^{2^{m-2}})^2=zzc=c$. Hence $g^{2^{n-2}}h^{2^{m-2}}$ is an element of order 4 in $C_G(Q)$ squaring to c, contradicting (vi). Now assume g and h are both of order 4. As $g\in C_G(Q)$ and $G^2=\Phi(G)=C_G(Q)$ by (x) and (xi), there are $g_1,\dots,g_k\in G$ such that $g=g_1^2g_2^2\cdots g_k^2$. By the general commutator formulas and (xii), we get

$$[g,h]=[g_1^2\cdots g_k^2,h]=([g_1,h]^2)^{g_2^2\cdots g_k^2}([g_2,h]^2)^{g_3^2\cdots g_k^2}\cdots[g_k,h]^2.$$

As $[g_i,h]^2\in\langle h^4\rangle=1$ for all i by (xii) we get $[g,h]=1$ and so $(gh)^2=g^2h^2=zcz=c$, again contradicting (vi).

Convention: In case $C_G(Q)$ contains an element g of order 4, we set $z=g^2$. By (vi) and (xiii), this is well defined. If there is no such element, we just keep the z from before.

(xiv) There is $\tilde{z}\in C_G(Q)$ such that $z\in\langle\tilde{z}\rangle$ and $C_G(Q)=\langle c\rangle\times\langle\tilde{z}\rangle$:

Let $g,h\in C_G(Q)$. As $C_G(Q)=G^2$ by (x) and (xi) as in the proof of (xiii) we have $[g,h]\in\langle h^4\rangle$, where we also need that $\langle h^2\rangle\trianglelefteq G$ by (xii). Hence $[C_G(Q),C_G(Q)]\leq C_G(Q)^4$, so that $C_G(Q)$ is a *powerful* 2*-group* (cf. the definition in [13, I, Definition 2.1]). Hence $C_G(Q)^2=\{g^2\mid g\in C_G(Q)\}$ [13, I, Proposition 2.6]. By (vi), this implies $c\notin\Phi(C_G(Q))=C_G(Q)^2$, hence $\langle c\rangle$ is a direct factor of $C_G(Q)$ and we have $C_G(Q)=\langle c\rangle\times H$ for a subgroup H containing only the involution z. Then H is cyclic or generalized quaternion by lemma 2.12, but as quaternion groups are not powerful, H must be cyclic and the claim follows.

(xv) For $g,h\in G$, we have $[g^2,h^2]=1$:

By (v), we know $g^2,h^2\in C_G(Q)$ which is an abelian group by (xiv).

(xvi) Without breaking the conventions, we can assume that y has order 4, $a^y=a$ and $z\in\langle y\rangle$:

We first aim to replace y by an element of order 4. By (xiv) we know $x^4,y^4\in\langle\tilde{z}\rangle$, so, as by convention $\circ(x)\geq\circ(y)$, there is $\ell\in\mathbb{Z}$ such that $x^{4\ell}y^4=1$. If x has order 4, then also y. So assume x has order at least 8. Note that as $x^2,y^2\in\langle c\rangle\times\langle\tilde{z}\rangle$ by (v) and (xiv) we have $y^2\in\langle x^2,c\rangle$, so that $[x,y^2]=1$. Hence by (xi) and (xii)

$$(x^\ell y)^4=(x^{2\ell}y^2[y,x^\ell])^2=x^{4\ell}y^4[y^2,x^\ell]=x^{4\ell}y^4=1.$$

https://doi.org/10.1017/prm.2025.10013 Published online by Cambridge University Press

Note that by the defining properties of x and y we have $x^\ell y \notin N_G(\langle b\rangle)$, so $x^\ell y$ cannot be an involution. So, $x^\ell y$ has order 4 and we replace y by $x^\ell y$, where we replace a by ab if ℓ is odd, so that the convention is kept. In case with the new y, we have $a^y \neq a$, we replace y by by. Finally, if $z \notin \langle y\rangle$, then $cz \in \langle y\rangle$ as $c \in \langle y\rangle$ is impossible by (vii). Then ay satisfies all the conventions and moreover $(ay)^2 = a^2y^2 = ccz = z$, so that we choose ay as the new y.

Convention: We choose y as described in (xvi).

(xvii) $\circ(x) = 4$:

Assume $\circ(x) = 2^n > 4$. Then by (v) and (xiv) we have $x^4 \in \langle \tilde{z}\rangle$ and so $z \in \langle x^4\rangle$. As $[x^2, y] \in \langle y^4\rangle = 1$ by (xii) we then get $(x^{2^{n-2}}y)^2 = zz = 1$ and $x^{2^{n-2}}y$ is an involution. But as it is not centralizing b this gives a contradiction.

(xviii) $\tilde{z} = z$:

Assume $\circ(\tilde{z}) > 2$ holds. First note that as x and y have order 4 by (xvi) and (xvii), the defining properties of x and y then imply that $\tilde{z}$ is not a power of x or y. Moreover, again as x has order 4, we have $x^2 \in Z(G)$ and so $1 = [x^2, y] = [x, y]^2$ by (xii). In particular, $[x, y]$ has order at most 2, implying that it is an element of the maximal elementary abelian subgroup $\langle c\rangle \times \langle z\rangle$ which is contained in $\langle c\rangle \times \langle \tilde{z}^2\rangle$. So, $G/(\langle c\rangle \times \langle \tilde{z}^2\rangle)$ is an elementary abelian group where the images of a, b, x, y, and $\tilde{z}$ are independent elements. To see the this use again the fact that $\circ(x) = \circ(y) = 4$. But this cannot be true, as G is 4-generated by (x).

(xix) We can assume $b^x = b$ and $x^2 = z$ without breaking the conventions:

As $x \in N_G(\langle b\rangle)$, we have $b^x = b^{\pm 1}$. If $b^x = b^{-1}$, we can replace x by ax. Next, $x^2 = c$ is not possible by (vii). So if $x^2 \neq z$, we must have $x^2 = cz$ (note that $\circ(x) = 4$ by (xvii)). If this is the case, we replace x by bx noting that $(bx)^2 = ccz = z$.

Convention: We choose x as described in (xix).

(xx) $a^x = az$ and $b^y = bz$:

Assume $a^x \neq az$. Then $a^x = a^{-1}z$ by the properties of x and (iv). Then using (xi) we get $(ax)^2 = a^2x^2[x, a] = czcz = 1$, so that ax would be an involution not centralizing b. Similarly, if $b^y \neq bz$, then by would be an involution not centralizing a.

Relations: We summarize the obtained relations:

$$x^4 = y^4 = 1, \quad x^2 = y^2 = z,$$
$$a^x = az, \quad b^x = b, \quad a^y = a, \quad b^y = bz.$$

We also note $(ab)^x = abz$ and $(ab)^y = abz$.

(xxi) $\langle x, y\rangle$ and $\langle bx, ay\rangle$ are normal subgroups of G isomorphic to Q_8:

By the relations already obtained for x and y to show that $\langle x, y\rangle \cong Q_8$ it suffices to show $[x, y] = z$. As x and y have order 4 the commutator $[x, y]$ has order at most 2 by (xii) and the fact

https://doi.org/10.1017/prm.2025.10013 Published online by Cambridge University Press

that involutions are central. We consider the other possible values for $[x, y]$. If $[x, y] = 1$, then xy is an involution no centralizing b. If $[x, y] = cz$, then by (xi) we get $(axy)^2 = a^2(xy)^2[xy, a] = c(x^2y^2cz)z = 1$, so that axy would be an involution not centralizing a. Similarly, if $[x, y] = c$, then $abxy$ is an involution not centralizing a. Hence $[x, y] = z$ and $\langle x, y\rangle \cong Q_8$. We next observe $\langle bx, ay\rangle \cong Q_8$. This follows from calculating $(bx)^2 = (ay)^2 = cz$ as well as $(bx)^{ay} = bxcz = (bx)^{-1}$. It remains to show that both these subgroups are normal, but as $\{a, b, x, y\}$ is a generating set of G by (x), it is sufficient to consider their conjugates under these four elements. A direct calculation using the relations above then gives the claim.

(xxii) $G = \langle x, y\rangle \times \langle bx, ay\rangle \cong Q_8 \times Q_8$:
By (xxi), both groups $\langle x, y\rangle$ and $\langle bx, ay\rangle$ are normal subgroups of G and isomorphic to Q_8. As they have trivial intersection, $\langle x, y\rangle \times \langle bx, ay\rangle$ is a subgroup of G. This subgroup contains a, b, x, and y which is a generating set of G by (x).

Finally, we show that if $G \cong Q_8 \times Q_8$, then G has SN but not SSN using the notation for the elements of G as in the $Q_8 \times Q_8$ we just found. First, as $a^x = az$ the subgroup $\langle a, b\rangle$ is not normal in G and G does not have SSN by lemma 2.10. Next, note that every subgroup containing the three non-trivial involutions is normal in G, as $G' = \langle c\rangle \times \langle z\rangle$. Moreover, it is easy to see that a cyclic subgroup Y of order 4 is non-normal in G if and only if $Y^2 = \langle c\rangle$. Hence, a general subgroup Y is non-normal if and only if $\Phi(Y) = \langle c\rangle$ and Y is either cyclic of order 4 or a quaternion group of order 8. Hence, for every normal subgroup N and non-normal subgroup Y, the relation $N \not\leq Y$ implies that N contains an involution different from c, giving $NY \trianglelefteq G$. Overall, G has SN. □

The main result of this subsection now follows easily.

Proof of Proposition 2.8. Let G be a nilpotent group which has SN but not SSN. By lemma 2.9, G is a p-group. If p is odd, or $p = 2$ and G contains a non-central involution, then the result is contained in Proposition 2.13. Finally consider the case $p = 2$ and that all involutions of G are central which only applies to the group $Q_8 \times Q_8$ by lemma 2.14. As $\mathcal{Z}(G)$ is not cyclic, G has no faithful irreducible representations. It hence suffices to consider the components of the maximal quotients of G. Say c and z are the involutions of the direct factors. Then $G/\langle c\rangle$, $G/\langle z\rangle$, and $G/\langle cz\rangle$ are the maximal quotients. The first two of those are isomorphic to $Q_8 \times C_2 \times C_2$ which is a Hamiltonian group not contributing matrix components to $\mathbb{Q}G$. Finally, we show that the group $G/\langle cz\rangle$ has SN, but not SSN, and contains non-central involutions, so that the result then follows from Proposition 2.13. To see this say a is an element of order 4 in the first direct factor and x an element of order 4 in the second. Then $(ax)^2 = cz$, so that ax is mapped to a non-central involution when mapping to $G/\langle cz\rangle$. To see that this quotient does not have SSN consider the subgroup generated by the first direct factor and x: then $\langle x\rangle$ is mapped to a normal subgroup not contained in the image of $\langle a\rangle$, but $\langle a, x\rangle$ is not mapped to a normal subgroup. □

https://doi.org/10.1017/prm.2025.10013 Published online by Cambridge University Press

REMARK 2.15. An alternative proof of lemma 2.14 could be derived from the classification of 2-groups all of whose non-normal subgroups are cyclic, elementary abelian of rank 2 or quaternion of order 8 in [9, Section 175]. The group $Q_8 \times Q_8$ is one of those, but one would need to exclude the other groups appearing.

2.3. Non-nilpotent groups

We will start with the case that G is solvable. For this, we need to introduce the following class of groups which will in §3 distinguish themselves by being the only finite groups for which we cannot determine the equivalence between property ND and having at most one matrix component. Recall,

DEFINITION 2.16. *Let* G *be a group whose order is divisible by exactly two different primes* p *and* q *and let* $P \in Syl_p(G)$ *and* $Q \in Syl_q(G)$. *Assume* P *and* Q *are both cyclic,* P *has order* p *and* $G = P \rtimes Q$ *such that* Q *acts non-trivially but also non-faithfully on* Q. *Then we call* G *an* SSN group of unfaithful type.

We note that the name in the previous definition is justified by [33, Theorem 2.7].

When we speak of the *rank* of a p-group P we will mean the minimal number of generators of a maximal elementary abelian subgroup of G.

PROPOSITION 2.17. G *is a solvable non-nilpotent group with SN if and only if the following holds:* G *contains a normal elementary abelian Sylow* p*-subgroup* P *and a* p′*-Hall subgroup* H *which is Dedekind. Each Sylow subgroup of* H *has rank* 1 *and if* P *has rank* 1, *then* H *is cyclic. Moreover,*

(i) *either* G *is an SSN group of unfaithful type*
(ii) *or the action of* H *on* P *is irreducible and faithful. In this case also no non-trivial element of* H *is centralizing a non-trivial element of* P.

Proof. We first show that G being a solvable and non-nilpotent group with SN implies the described properties. Assume first that G contains a normal elementary abelian subgroup of rank at least 2 for some prime p. Then by lemma 2.4, we know that $P \trianglelefteq G$ for $P \in \mathrm{Syl}_p(G)$ and G contains a nilpotent p'-Hall subgroup H. By lemma 2.3, the action of H on P is irreducible and faithful and P is elementary abelian. It remains to show that the Sylow subgroups of H all have rank 1. The action of H on P corresponds to a faithful and irreducible representation of H over $\mathbb{F}_p$. Let χ be the character of this representation, M the $\mathbb{F}_pG$-module and F a field extension of $\mathbb{F}_p$ which is a splitting field for H. Then by [21, Theorem 9.21] the character of the module $F \otimes_{\mathbb{F}_p} M$ is a sum of certain Galois-conjugate characters of an irreducible F-character η of H. If H contains an elementary-abelian subgroup Q of rank at least 2, then by the structure of Dedekind groups, Q is central in H and η has a non-trivial kernel on Q. But this kernel is then also contained in the kernel of χ, contradicting the fact that the action of H on P is faithful. Note also that if D is a representation corresponding to η and $h \in H \setminus \{1\}$, then $D(h)$ has no eigenvalue 1. This follows again from the structure of Dedekind groups, as this is true for faithful characters of the quaternion group of order 8 and cyclic groups. Hence there is no $g \in P \setminus \{1\}$ such that $g^h = g$.

https://doi.org/10.1017/prm.2025.10013 Published online by Cambridge University Press

We can hence assume that every elementary abelian normal subgroup of G has rank 1. Let P_0 be such a normal p-subgroup, so P_0 is a cyclic group of order p, and let H be a nilpotent p'-Hall subgroup of G which exists by lemma 2.4. We first consider the case that some Sylow subgroup of H acts trivially on P_0. Let $Q \in \mathrm{Syl}_q(G)$ be a such a Sylow subgroup, i.e. $[P_0, Q] = 1$. Then $P_0 \times Q \trianglelefteq G$, as G has SN, and so $Q \trianglelefteq G$, as it is characteristic in $P_0 \times Q$. So by lemma 2.4, we have $G = QR$ for R a q'-Hall subgroup of G. Moreover, the action of R on Q is not faithful, as P_0 acts trivially on Q. We conclude by lemma 2.3 that G is an SSN group of unfaithful type.

So we can assume that every Sylow subgroup of H acts non-trivially on P_0. Let $Q \in \mathrm{Syl}_q(H)$. We first show that the rank of Q is 1. Assume it is not and that $\langle x \rangle \times \langle y \rangle$ is an elementary abelian group of rank 2 contained in Q. As $\mathrm{Aut}(P_0)$ is cyclic, some element of $\langle x \rangle \times \langle y \rangle$ must act trivially on P_0, say this is x. Then $P_0 \times \langle x \rangle \trianglelefteq G$, as G has SN and so $\langle x \rangle \trianglelefteq G$, as $\langle x \rangle$ is a characteristic subgroup of $P_0 \times \langle x \rangle$. Hence, again using the SN property of G, also $\langle x \rangle \times \langle y \rangle \trianglelefteq G$, but this contradicts our assumption that G contains no normal elementary abelian subgroup of rank at least 2. Hence Q has rank 1. So, every Sylow subgroup of H is cyclic or generalized quaternion by lemma 2.12.

We show that H contains no quaternion group. Indeed, assume $Q = \langle g, h \mid g^{2^n} = g^4 = 1, g^{2^{n-1}} = h^2, g^h = g^{-1} \rangle$ is a subgroup of H for some $n \geq 2$. As $\mathrm{Aut}(P_0)$ is cyclic, some element of order 4 in Q must act trivially on P_0. As in the previous paragraph, this element must generate a normal subgroup of G. When $n \geq 3$ the only normal subgroup of Q of order 4 is $\langle g^{2^{n-2}} \rangle$, so it must act trivially. When $n = 2$ we can assume this without loss of generality. Now $G/\langle g^{2^{n-2}}, h \rangle$ is a Dedekind group, so that the image of Q in this quotient acts trivially on the image of P_0. Hence g acts trivially on P_0 and h non-trivially. As before we get then $\langle g \rangle \trianglelefteq G$ and the SN property implies $\langle g \rangle \langle h \rangle = Q \trianglelefteq G$. But this cannot be as h acts non-trivially on P_0. We conclude that all the Sylow subgroups of H are cyclic.

We now show that under all the assumptions G has a normal Sylow p-subgroup. Let $\{q_1, q_2, \ldots, q_k\}$ be the prime divisors of $|H|$ with $q_1 < q_2 < \cdots < q_k$. Note that as a Sylow q_i-subgroup of H acts non-trivially on P_0 we have $q_i \mid (p-1)$ and so $q_i < p$ for each i. By successively applying the famous corollary of Burnside's p-complement Theorem on cyclic Sylow subgroups for minimal primes [20, IV, Satz 2.8], we obtain that G contains a normal q_1-complement H_1, which contains a normal q_2-complement H_2,..., which contains a normal q_k-complement P which must be a Sylow p-subgroup of G. Note that in each step the normal complement found is characteristic, so that all these groups are also normal in G, in particular P. So $G = P \rtimes H$. It follows from lemma 2.3 that the structure of G is as claimed. Moreover, as all the Sylow subgroups of G are cyclic and the action of each Sylow subgroup of H on P is now faithful we get $[g, h] \neq 1$ for all $h \in H \setminus \{1\}$ and $g \in P \setminus \{1\}$.

Finally, we also show that the described groups are groups with SN. This is clear for the SSN groups of unfaithful type, as these have even SSN by [33, Theorem 2.7]. So assume G is as described in (ii). As the action of H on P is irreducible and faithful, P is the unique minimal normal subgroup of G. So if $N \trianglelefteq G$ and $N \neq 1$, then $P \leq N$. Let moreover $Y \leq G$. If N is not a subgroup of Y, then $NY/N \trianglelefteq G/N$,

https://doi.org/10.1017/prm.2025.10013 Published online by Cambridge University Press

as G/N is a quotient of H and hence a Dedekind group. This implies $NY \trianglelefteq G$ and so G indeed has SN. □

Finally, using the methods from [33, Section 3], we readily classify the non-solvable groups with SN.

PROPOSITION 2.18. *Let* G *be a non-solvable group. Then* G *has SN if and only if* G *has a unique minimal normal subgroup* S *such that* S *is non-abelian and* G/S *Dedekind. Moreover in that case* $S = \mathrm{Soc}(G)$ *is a direct product of isomorphic finite simple groups and if* S *is simple, then* G *is an almost simple group.*

Proof. Let G be a non-solvable group with SN. Recall that minimal normal subgroups are direct products of isomorphic simple groups, see [2, (8.3)]. By lemma 2.4, we cannot have an abelian minimal normal subgroup. Hence every minimal normal subgroup is the direct product of non-abelian simple groups, the socle S of G is non-abelian and the Fitting subgroup trivial. In particular, S equals the generalized Fitting subgroup which is the unique largest normal semisimple subgroup.

Next, write S as the internal direct product $\prod_{i=1}^{n} A_i$ with A_i a minimal normal subgroup of G. Using lemma 2.2, we see that G/A_1 is Dedekind which is only possible if all $A_i = 1$ for $i \neq 1$. Thus S is the unique minimal normal subgroup. Moreover, S is the direct product of isomorphic non-abelian simple groups. Furthermore, as S is non-abelian, lemma 2.2 also yields that G/S is Dedekind.

Conversely, suppose $S \leq G$ is the unique minimal normal subgroup of G, that S is non-abelian and G/S is Dedekind. Now, every $N \trianglelefteq G$ contains the unique minimal normal subgroup S. Hence if $Y \leq G$, then $S \leq NY$ and so $NY/S \leq G/S$ is normal. Therefore, $NY \trianglelefteq G$ as needed.

Finally, suppose that G has SN and $S = \mathrm{Soc}(G)$ is simple. As S is also the generalized Fitting subgroup, it contains its own centralizer. In other words, $C_G(S) = \mathcal{Z}(S)$ is trivial and hence G acts faithfully on S. Thus one may identify G with a subgroup of $\mathrm{Aut}(S)$ with S simple, i.e. G is almost simple. □

3. Groups with the ND property and the Jespers–Sun conjecture

Let G be a finite group and $n \in \mathbb{Z}G$ nilpotent. Then G *has ND* if $ne \in \mathbb{Z}G$ for every n and every primitive central idempotent e of $\mathbb{Q}G$. In this section, we answer property ND for all finite groups which are not as in definition 2.16. In particular for such groups, we show that there is a unique counterexample to Jespers–Sun's conjecture 1.1.

THEOREM 3.1. *Let* G *be a finite group which is not an SSN group of unfaithful type. Then* G *has ND if and only if* $\mathbb{Q}G$ *has at most one matrix component or* $G \cong \langle a, b \mid a^4 = b^8 = 1, a^b = a^{-1} \rangle$.

Any group with ND is necessarily a group with SN. This follows almost directly from the definition and is recorded in [31, Proposition 2.5], where this follows from the proof, and more explicitly in [27, Proposition 3.4]. So to prove Theorem 3.1 we will use Theorem C. Furthermore, we will have to distinguish the case where G is nilpotent or not. In particular, the above result is the combination of Theorems 3.5 and 3.15.

https://doi.org/10.1017/prm.2025.10013 Published online by Cambridge University Press

One may now draw easily interesting consequences from Theorem A. For example, if G is not metacyclic, then Jespers–Sun's conjecture is actually correct. In the philosophy 'what does a group ring RG know about G?' we can give a positive answer to a variation of the Jespers–Sun conjecture:

COROLLARY 3.2. *Let* G *and* H *be groups such that* $\mathbb{Q}G \cong \mathbb{Q}H$ *and* G *has ND. Then* H *has* ND.

Proof. Assume first that G has at most one matrix component. Then $\mathbb{Q}G \cong \mathbb{Q}H$ implies, that so has H and so H has ND. By Theorem 3.1, it remains to consider the cases that G is the non-abelian group $C_4 \rtimes C_8$ or an SSN group of unfaithful type. Assume first that $G \cong C_4 \rtimes C_8$. Then $G/G' \cong C_8 \times C_2 \cong H/H'$ [15, Theorem 2.8]. It follows that if $\langle c \rangle = H'$, then either there is an element $h \in H$ of order 4 or 16 such that $c \in \langle h \rangle$ or there is no element at all squaring to c. As a generalized quaternion group of order 32 has derived subgroup of order 8, it follows that $\mathcal{Z}(G)$ has rank bigger than one and with the previous $H \cong G$ or it is one of the groups

$$H_1 = \langle a, b \mid a^{16} = b^2 = 1, a^b = a^9 \rangle,$$
$$H_2 = \langle a, b, c \mid a^8 = b^2 = c^2 = 1, a^b = ac, [a, c] = [b, c] = 1 \rangle.$$

None of these groups map onto a quaternion group, so both $\mathbb{Q}H_1$ and $\mathbb{Q}H_2$ do not have a simple component isomorphic to the rational quaternion algebra, while $\mathbb{Q}G$ does. We conclude $G \cong H$.

So assume G is an SSN group of unfaithful type, say $G \cong C_p \rtimes C_{q^k}$ for some primes p and q and a positive integer k. Then $\mathbb{Q}G \cong \mathbb{Q}H$ implies $|H| = p \cdot q^k$. Moreover, the maximal commutative direct summand of $\mathbb{Q}G$ is isomorphic to $\mathbb{Q}(G/G') \cong \mathbb{Q}C_{q^k}$. So $H/H' \cong C_{q^k}$, which implies also $H' \cong C_p$. Hence $H \cong C_p \rtimes C_{q^k}$. To show that $G \cong H$ it remains to show that the action on the derived subgroup has the same order or equivalently $\mathcal{Z}(G) \cong \mathcal{Z}(H)$. It is easy to calculate that the number of conjugacy classes of cyclic subgroups of G and H is the same if and only if $\mathcal{Z}(G) \cong \mathcal{Z}(H)$. As this number coincides with the number of simple components of a rational group algebra [24, Corollary 7.1.12], the result follows. □

3.1. Background on describing simple components via Shoda pairs

As could be expected from the content of conjecture 1.1, we need to recall some methods to construct primitive central idempotents of $\mathbb{Q}G$. These methods were introduced by Olivieri–del Río–Simón [39], see [24, Chapter 3] for a good introduction. To start, recall that if $H \trianglelefteq G$, then $\widehat{H}$ is a central idempotent in $\mathbb{Q}G$. Now, set $\epsilon(H, H) = \widehat{H}$ and for a strict normal subgroup K of H define

$$\epsilon(H, K) = \prod_{M/K \in \mathcal{M}(H/K)} (\widehat{K} - \widehat{M}) = \widehat{K} \prod_{M/K \in \mathcal{M}(H/K)} (1 - \widehat{M}), \tag{3}$$

where $\mathcal{M}(H/K)$ denotes the set of the non-trivial minimal normal subgroups of H/K. In both cases, the construction results in a central idempotent in $\mathbb{Q}H$. Next,

https://doi.org/10.1017/prm.2025.10013 Published online by Cambridge University Press

with $K \trianglelefteq H$, one associates the element

$$e(G,H,K) = \sum_{t\in\mathcal{T}} \epsilon(H,K)^t, \tag{4}$$

where $\mathcal{T}$ is a right transversal of $\mathrm{Cen}_G(\epsilon(H,K))$ in G. The element $e(G,H,K)$ is central in $\mathbb{Q}G$ and is a primitive idempotent when (H,K) is a *Strong Shoda pair* of G. A tuple (H,K) is called a strong Shoda pair when $K \leq H \trianglelefteq N_G(K)$, H/K is cyclic and a maximal abelian subgroup of $N_G(K)/K$, and the G-conjugates of $\epsilon(H,K)$ are orthogonal.

To a central idempotent e, we will also need the associated homomorphism

$$\varphi_e : G \to Ge, \quad g \mapsto ge. \tag{5}$$

The following is a combination of [24, Proposition 3.4.1, Theorems 3.4.2 & 3.5.5 and Problem 3.5.1].

THEOREM 3.3. ([39]). *With notations as above, $e(G,H,K)$ is a primitive central idempotent of $\mathbb{Q}G$ if (*H, K*) is a strong Shoda pair. Moreover, in that case* $\mathrm{Cen}_G(\epsilon(H,K)) \cong N_G(K)$ *and* $\ker(\varphi_{e(G,H,K)}) = core_G(K) = \bigcap_{g\in G} K^g$.

We also need the $\mathbb{Q}$-dimension of the simple algebra associated with a strong Shoda pair which directly follows from the known description of $\mathbb{Q}Ge(G,H,K)$.

LEMMA 3.4. *Let (*H, K*) be a strong Shoda pair of* G. *Then*

$$\dim_{\mathbb{Q}} \mathbb{Q}Ge(G,H,K) = [G:H][G:N_G(K)]\phi([H:K]),$$

where $\phi(\cdot)$ denotes the phi-Euler function.

Proof. Following [24, Theorem 3.5.5], $\mathbb{Q}Ge(G,H,K) \cong M_{[G:N_G(K)]}(\mathbb{Q}(\zeta_{[H:K]}) \star N_G(K)/H)$ for some crossing that can be made explicit (see [24, Remark 3.5.6]). Therefore, one has that

$$\begin{aligned} dim_{\mathbb{Q}}\mathbb{Q}Ge(G,H,K) &= [G:N_G(K)]^2\phi([H:K])[N_G(K):H] \\ &= [G:H][G:N_G(K)]\phi([H:K]). \end{aligned}$$

□

3.2. Nilpotent case

In this section, we completely solve conjecture 1.1 for nilpotent groups. It turns out that in this class the conjecture is almost true—there is exactly one counterexample. From the results of the previous section, we know that we need to consider the question only for nilpotent groups with SSN. For many of those Jespers and Sun did prove their conjecture [27, Corollary 4.12], but as it turns out, quite some work remains. Overall in this section, we get:

THEOREM 3.5. *Let* G *be a nilpotent group. Then* G *has ND if and only if either* G *has one matrix component or* $G \cong \langle a,b \mid a^4 = b^8 = 1, a^b = a^{-1}\rangle \cong C_4 \rtimes C_8$.

https://doi.org/10.1017/prm.2025.10013 Published online by Cambridge University Press

The identifier of the exception appearing in the theorem in the SmallGroupsLibrary [10] is [32, 12].

It turns out that from our results in the previous section and the previous work of others, mostly Liu and Jespers–Sun, there is one series of groups we need to address which we define now. For a prime p and positive integers $n \geq 1$ and $m \geq 2$ define the group

$$G(p,m,n) = \langle a, b \mid 1 = a^{p^m} = b^{p^n}, a^b = a^{1+p^{m-1}} \rangle. \tag{6}$$

Note that the centre of $G(p,m,n)$ is $\langle a^p \rangle \times \langle b^p \rangle$. When working with a group $G(p,m,n)$ we will always assume that it has generators and relations exactly as given in (6).

THEOREM 3.6. *The group $G(2,2,3)$ has (ND), but $\mathbb{Q}G(2,2,3)$ has more than one matrix component. Consequently, conjecture 1.1 is not correct.*

Before we proceed to prove the theorem, we record an easy property of nilpotent 2×2-matrices.

LEMMA 3.7. *Assume $A = \begin{pmatrix} x & y \\ z & w \end{pmatrix}$ is a 2×2-matrix over a commutative domain* R. *Then* A *is nilpotent if and only if $x = -w$, $x^2 = -yz$.*

Proof. As A is nilpotent, i.e. $A^n = 0$ for some n, the multiplicativity of the determinant gives $\det(A) = 0$, implying $xw = yz$. Hence,

$$A^2 = \begin{pmatrix} x^2 + yz & xy + yw \\ xz + zw & w^2 + yz \end{pmatrix} = \begin{pmatrix} x^2 + xw & y(x+w) \\ z(x+w) & w^2 + xw \end{pmatrix} = \operatorname{tr}(A)A.$$

So, $0 = \operatorname{tr}(A)^{n-1}A$, which gives $\operatorname{tr}(A) = 0$. Hence, $x = -w$ and from $xw = yz$ we also get $x^2 = -yz$. □

Proof of Theorem 3.6. Let

$$G(2,2,3) = G = \langle a, b \mid a^4 = b^8 = 1,\ a^b = a^{-1} \rangle.$$

We note that $G' = \langle a^2 \rangle$ and $\mathcal{Z}(G) = \langle a^2, b^2 \rangle$. Then $G/G' \cong C_2 \times C_8$, so the algebra $\mathbb{Q}G$ has a direct summand

$$\mathbb{Q}[C_2 \times C_8] \cong 4\mathbb{Q} \oplus 2\mathbb{Q}(i) \oplus \mathbb{Q}(\zeta_8).$$

Moreover, $G/\langle a^2b^2 \rangle \cong Q_8$ and $G/\langle b^2 \rangle \cong D_8$, so that $\mathbb{Q}G$ has also direct summands $\mathbb{H}_{\mathbb{Q}}$, the standard rational quaternions, and $M_2(\mathbb{Q})$. Moreover, $G/\langle a^2b^4 \rangle$ is a group of order 16 sometimes denoted by D_{16}^+. The rational group algebra of this group has one matrix component isomorphic to $M_2(\mathbb{Q}(i))$. We mention that it has been used in [5] to solve another problem on integral group rings. Overall

$$\mathbb{Q}G \cong 4\mathbb{Q} \oplus 2\mathbb{Q}(i) \oplus \mathbb{Q}(\zeta_8) \oplus \mathbb{H}_{\mathbb{Q}} \oplus M_2(\mathbb{Q}) \oplus M_2(\mathbb{Q}(i)).$$

This can also be easily checked using GAP [45] and the wedderga package therein [7].

https://doi.org/10.1017/prm.2025.10013 Published online by Cambridge University Press

Furthermore, the following representations correspond to the non-commutative components (in the order as above):

$$\begin{aligned} &G \to \mathbb{H}_{\mathbb{Q}}, \quad a \mapsto i, \quad b \mapsto j, \\ &G \to M_2(\mathbb{Q}), \quad a \mapsto \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \quad b \mapsto \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}, \\ &G \to M_2(\mathbb{Q}(i)), \quad a \mapsto \begin{pmatrix} -i & 0 \\ 0 & i \end{pmatrix}, \quad b \mapsto \begin{pmatrix} 0 & 1 \\ i & 0 \end{pmatrix}. \end{aligned} \tag{7}$$

Here we denote by i and j the standard generators of $\mathbb{H}_{\mathbb{Q}}$.

We first derive the properties which are equivalent to having a nilpotent element in $\mathbb{Z}G$. Let n be a generic nilpotent element in $\mathbb{Z}G$ and write

$$n = \sum_{g \in G} \alpha(g) g.$$

In the quotient G/G', the element n must map to 0 which is equivalent to the fact that for each $h \in G$ one has $\sum_{g \in G'} \alpha(hg) = 0$. This is, in turn, equivalent to

$$\alpha(g) = -\alpha(ga^2) \ \forall g \in G, \tag{8}$$

since $G' = \langle a^2 \rangle$. As in the three non-commutative components the element a^2 is always send to -1, this will always give a factor 2 in the considerations below and reduces the number of indeterminants by half. So we will always replace an expression of shape $\alpha(g) - \alpha(ga^2)$ by $2\alpha(g)$.

Next we consider the $\mathbb{H}_{\mathbb{Q}}$-component where the projection of n must equal 0. With the representation above n is sent to

$$\begin{aligned} &2(\alpha(1) - \alpha(b^2) + \alpha(b^4) - \alpha(b^6) \\ &+i(\alpha(a) - \alpha(ab^2) + \alpha(ab^4) - \alpha(ab^6)) \\ &+j(\alpha(b) - \alpha(b^3) + \alpha(b^5) - \alpha(b^7)) \\ &+ij(\alpha(ab) - \alpha(ab^3) + \alpha(ab^5) - \alpha(ab^7))). \end{aligned}$$

Setting this equal to 0 gives the equations

$$\begin{aligned} \alpha(1) &= \alpha(b^2) + \alpha(b^6) - \alpha(b^4), \\ \alpha(a) &= \alpha(ab^2) + \alpha(ab^6) - \alpha(ab^4), \\ \alpha(b) &= \alpha(b^3) + \alpha(b^7) - \alpha(b^5), \\ \alpha(ab) &= \alpha(ab^3) + \alpha(ab^7) - \alpha(ab^5). \end{aligned} \tag{9}$$

Together with (8), this can be written compactly as

$$\alpha(g) + \alpha(gb^4) = \alpha(gb^2) + \alpha(gb^6) \ \forall g \in G. \tag{10}$$

https://doi.org/10.1017/prm.2025.10013 Published online by Cambridge University Press

We denote the representation of n in the $M_2(\mathbb{Q})$-component by $\begin{pmatrix} x_1 & y_1 \\ z_1 & w_1 \end{pmatrix}$ and in the $M_2(\mathbb{Q}(i))$-component by $\begin{pmatrix} x_2 & y_2 \\ z_2 & w_2 \end{pmatrix}$.

From the representation given above, we get

$$x_1 = 2(\alpha(1) + \alpha(b^2) + \alpha(b^4) + \alpha(b^6) - \alpha(b) - \alpha(b^3) - \alpha(b^5) - \alpha(b^7))$$

which using (9) transforms to

$$x_1 = 4(\alpha(b^2) + \alpha(b^6) - \alpha(b^3) - \alpha(b^7)). \tag{11}$$

Similarly, we get

$$w_1 = 4(\alpha(b^2) + \alpha(b^6) + \alpha(b^3) + \alpha(b^7)). \tag{12}$$

As one of our conditions on n is $x_1 = -w_1$ by lemma 3.7 this gives, using also (9),

$$\alpha(b^2) = -\alpha(b^6),\ \alpha(1) = -\alpha(b^4). \tag{13}$$

Furthermore, we compute

$$y_1 = 2(-\alpha(a) - \alpha(ab^2) - \alpha(ab^4) - \alpha(ab^6) - \alpha(ab) - \alpha(ab^3) - \alpha(ab^5) - \alpha(ab^7))$$

which we convert using (9) to

$$y_1 = 4(-\alpha(ab^2) - \alpha(ab^6) - \alpha(ab^3) - \alpha(ab^7)). \tag{14}$$

Similarly

$$z_1 = 4(\alpha(ab^2) + \alpha(ab^6) - \alpha(ab^3) - \alpha(ab^7)). \tag{15}$$

We now calculate the $\mathbb{Q}(i)$-representation. We get

$$\begin{aligned} x_2 = 2(&\alpha(1) - \alpha(b^4) + \alpha(ab^2) - \alpha(ab^6) \\ &+ i(-\alpha(a) + \alpha(ab^4) + \alpha(b^2) - \alpha(b^6))). \end{aligned}$$

Using (9) and (13), this becomes

$$\begin{aligned} x_2 = 2(&-2\alpha(b^4) + \alpha(ab^2) - \alpha(ab^6) \\ &+ i(2\alpha(ab^4) - 2\alpha(b^6) - \alpha(ab^2) - \alpha(ab^6))). \end{aligned}$$

Similarly,

$$\begin{aligned} w_2 = 2(&-2\alpha(b^4) - \alpha(ab^2) + \alpha(ab^6) \\ &+ i(-2\alpha(ab^4) - 2\alpha(b^6) + \alpha(ab^2) + \alpha(ab^6))). \end{aligned}$$

With the condition $x_2 = -w_2$ from lemma 3.7, this gives $\alpha(b^4) = 0 = \alpha(b^6)$ and together with (13) we conclude

$$\alpha(1) = \alpha(b^2) = \alpha(b^4) = \alpha(b^6) = 0 \tag{16}$$

https://doi.org/10.1017/prm.2025.10013 Published online by Cambridge University Press

and

$$x_2 = 2(\alpha(ab^2) - \alpha(ab^6) + i(2\alpha(ab^4) - \alpha(ab^2) - \alpha(ab^6))) \tag{17}$$

as well as

$$w_2 = 2(-\alpha(ab^2) + \alpha(ab^6) + i(-2\alpha(ab^4) + \alpha(ab^2) + \alpha(ab^6))). \tag{18}$$

We compute the other coefficients as

$$y_2 = 2(\alpha(b) - \alpha(b^5) + \alpha(ab^3) - \alpha(ab^7) + i(\alpha(b^3) - \alpha(b^7) - \alpha(ab) + \alpha(ab^5))$$

which by (9) transforms to

$$y_2 = 2(-2\alpha(b^5) + \alpha(b^3) + \alpha(b^7) + \alpha(ab^3) - \alpha(ab^7) + i(2\alpha(ab^5) + \alpha(b^3) - \alpha(b^7) - \alpha(ab^3) - \alpha(ab^7))). \tag{19}$$

Similarly, also by (9),

$$z_2 = 2(2\alpha(ab^5) - \alpha(b^3) + \alpha(b^7) - \alpha(ab^3) - \alpha(ab^7) + i(-2\alpha(b^5) + \alpha(b^3) + \alpha(b^7) - \alpha(ab^3) + \alpha(ab^7))). \tag{20}$$

Moreover, from (11) and (16), we have

$$x_1 = -4(\alpha(b^3) + \alpha(b^7)). \tag{21}$$

We now compute the quadratic equations from lemma 3.7. Then

$$x_1^2 = 16(\alpha(b^3)^2 + 2\alpha(b^3)\alpha(b^7) + \alpha(b^7)^2) \tag{22}$$

and from (14) and (15) we get

$$-y_1 z_1 = -16(-\alpha(ab^2)^2 - 2\alpha(ab^2)\alpha(ab^6) - \alpha(ab^6)^2 + \alpha(ab^3)^2 + 2\alpha(ab^3)\alpha(ab^7) + \alpha(ab^7)^2). \tag{23}$$

The analogues equations for the $M_2(\mathbb{Q}(i))$-component give by (17)

$$x_2^2 = 8(-2\alpha(ab^4)^2 + 2\alpha(ab^2)\alpha(ab^4) + 2\alpha(ab^6)\alpha(ab^4) - 2\alpha(ab^2)\alpha(ab^6) + i(2\alpha(ab^2)\alpha(ab^4) - 2\alpha(ab^6)\alpha(ab^4) - \alpha(ab^2)^2 + \alpha(ab^6)^2)) \tag{24}$$

https://doi.org/10.1017/prm.2025.10013 Published online by Cambridge University Press

and by (19) and (20)

$$\begin{aligned}-y_2z_2 = -8(&2\alpha(b^3)\alpha(b^5) - 2\alpha(b^7)\alpha(b^5) - \alpha(b^3)^2 + \alpha(b^7)^2\\ &+ 2\alpha(ab^3)\alpha(ab^5) - 2\alpha(ab^7)\alpha(ab^5) - \alpha(ab^3)^2 + \alpha(ab^7)^2\\ &+ 2i(\alpha(ab^5)^2 - \alpha(ab^3)\alpha(ab^5) - \alpha(ab^7)\alpha(ab^5)\\ &+ \alpha(b^5)^2 - \alpha(b^3)\alpha(b^5) - \alpha(b^7)\alpha(b^5)\\ &+ \alpha(b^3)\alpha(b^7) + \alpha(ab^3)\alpha(ab^7))).\end{aligned} \tag{25}$$

We now show certain congruences modulo 2 which will provide the key for the final argument. First note that the imaginary part of $-y_2z_2$ is divisible by 16. So this is also true for the imaginary part of x_2^2 implying $-\alpha(ab^2)^2 + \alpha(ab^6)^2 \equiv 0 \bmod 2$ which means

$$\alpha(ab^2) \equiv \alpha(ab^6) \mod 2. \tag{26}$$

We next show that $\alpha(b^3) \equiv \alpha(b^7) \bmod 2$ and also $\alpha(ab^3) \equiv \alpha(ab^7) \bmod 2$. Assume that $\alpha(b^3) \not\equiv \alpha(b^7) \bmod 2$. Then one of them is even and the other is odd which implies by (22) that $\frac{x_1^2}{16} \equiv 1 \bmod 4$. Note that (26) implies that

$$\alpha(ab^2) + 2\alpha(ab^2)\alpha(ab^6) + \alpha(ab^6)^2 = (\alpha(ab^2) + \alpha(ab^6))^2 \equiv 0 \mod 4.$$

So from (23)

$$\frac{-y_1z_1}{16} \equiv -(\alpha(ab^3)^2 + 2\alpha(ab^3)\alpha(ab^7) + \alpha(ab^7)^2) = -(\alpha(ab^3) + \alpha(ab^7))^2 \mod 4$$

which can only be congruent to 0 or -1 modulo 4, contradicting $x_1^2 = -y_1z_1$. Hence

$$\alpha(b^3) \equiv \alpha(b^7) \mod 2. \tag{27}$$

We now consider the real parts of x_2^2 and $-y_2z_2$. The real part of x_2^2 is divisible by 16. So by (25) and (27)

$$0 \equiv Re(-y_2z_2) \equiv -8(-\alpha(ab^3)^2 + \alpha(ab^7)^2) \mod 16$$

which implies

$$\alpha(ab^3) \equiv \alpha(ab^7) \mod 2. \tag{28}$$

Together with (8), (10), and (16), the congruences (26), (27), and (28) can be compactly written as

$$\alpha(g) + \alpha(gb^4) \equiv 0 \mod 2 \quad \forall g \in G. \tag{29}$$

These are all the equations and congruences we need.

Let now $e \in \mathrm{PCI}(\mathbb{Q}G)$. If e corresponds to a component which is not a matrix component, then $ne = 0$ which is clearly an element in $\mathbb{Z}G$. To analyse the other elements of $\mathrm{PCI}(\mathbb{Q}G)$, we will deploy lemma 2.7. Let first $e \in \mathrm{PCI}(\mathbb{Q}G)$ be the

https://doi.org/10.1017/prm.2025.10013 Published online by Cambridge University Press

element corresponding to the $M_2(\mathbb{Q})$-representation and let χ be its character. Then from the representation given above we get

$$\chi(g) = \begin{cases} 2, & g \in \langle b^2 \rangle, \\ -2, & g \in a^2\langle b^2 \rangle, \\ 0, & \text{else.} \end{cases}$$

So by lemma 2.7 we can compute the coefficient of ne at a generic element $g \in G$ in the following way, where we use first the values of χ, then (8) and then (10):

$$\begin{aligned} &\frac{k}{|G|}\sum_{h\in G}\alpha(gh^{-1})\chi(h^{-1}) \\ &\quad= \frac{2}{32}\big(2(\alpha(g)+\alpha(gb^2)+\alpha(gb^4)+\alpha(gb^6) \\ &\qquad -\alpha(ga^2)-\alpha(ga^2b^2)-\alpha(ga^2b^4)-\alpha(ga^2b^6))\big) \\ &\quad= \frac{1}{8}\big(2(\alpha(g)+\alpha(gb^2)+\alpha(gb^4)+\alpha(gb^6))\big) \\ &\quad= \frac{1}{4}\big(2(\alpha(g)+\alpha(gb^4))\big) = \frac{1}{2}\big(\alpha(g)+\alpha(gb^4)\big). \end{aligned}$$

By (29), all these numbers are integers and hence $ne \in \mathbb{Z}G$.

Finally let $e \in \mathrm{PCI}(\mathbb{Q}G)$ be the element corresponding to the component $M_2(\mathbb{Q}(i))$ and χ its character. The argument will be similar to the previous case. Note that we consider χ as a character of a $\mathbb{Q}$-representation, so that each of the entries in the representation given in (7) corresponds to a 2×2-matrix and i corresponds to a matrix with trace 0, e.g. to its rational canonical form $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$. Hence

$$\chi(g) = \begin{cases} 4, & g \in \langle a^2b^4 \rangle, \\ -4, & g \in \{a^2, b^4\}, \\ 0, & \text{else.} \end{cases}$$

We again use lemma 2.7 to compute the coefficient of ne at g, where we use first the values of χ and then (8):

$$\begin{aligned} \frac{k}{|G|}\sum_{h\in G}\alpha(gh^{-1})\chi(h^{-1}) &= \frac{2}{32}\big(4(\alpha(g)+\alpha(ga^2b^4)-\alpha(ga^2)-\alpha(gb^4))\big) \\ &= \frac{1}{4}\big(2(\alpha(g)+\alpha(gb^4))\big) = \frac{1}{2}\big(2\alpha(g)+\alpha(gb^4)\big). \end{aligned}$$

Hence again by (29), all the coefficients of ne are integers. Overall we conclude that G has the (ND) property. □

Our next goal is to show that $G(2,2,3)$ is in fact the only nilpotent counterexample to conjecture 1.1. In the nilpotent case, by Theorem 2.8, we need to understand nilpotent groups with SSN and the groups $G(p,m,n)$ from (6) in particular. The

https://doi.org/10.1017/prm.2025.10013 Published online by Cambridge University Press

proof for this class of groups will proceed through several lemmas which separate the cases which remain open. All of them will be handled by a similar construction which will be made concrete in all the cases. It is inspired by an argument in [30].

LEMMA 3.8. *Let* p *be a prime,* $r, s \in \mathbb{Z}G$, $y \in \mathcal{Z}(\mathbb{Z}G)$, *and* $e \in \mathbb{Q}G$ *a central idempotent such that the following hold:*

(i) $r^2 = s^2 = rs = sr = 0$,
(ii) $\mathrm{er} = \mathrm{r}$, $\mathrm{es} = 0$,
(iii) $y(r+s)/p \in \mathbb{Z}G$,
(iv) $yr/p \notin \mathbb{Z}G$.

Then G *does not have ND.*

Proof. By (i), we have $rs = sr$, so that by (i) $(y(r+s)/p)^2 = y^2(r+s)^2/p^2 = 0$. So by (iii) $y(r+s)/p$ is a nilpotent element in $\mathbb{Z}G$ and moreover $ey(r+s)/p = yr/p$ by (ii). So by (iv) $(y(r+s)/p$ is non-zero and G does not have ND. □

The property of having one matrix component was systematically studied for groups with SSN by Jespers and Sun. We record the result relevant for this section which motivates the following lemmas.

LEMMA 3.9. [28, Lemmas 4.2, 4.3] *For* $G = G(p, m, n)$ *the algebra* $\mathbb{Q}G$ *has one matrix component if and only if* $\mathrm{n} = 1$ *or* $p = m = n = 2$.

The proofs of the next four lemmas all employ lemma 3.8. The first one will be especially detailed to facilitate the understanding of the arguments later also.

LEMMA 3.10. *Let* $G = G(2, m, n)$ *with* $n \geq 2$ *and* $(m, n) \notin \{(2,2), (2,3)\}$. *Then* G *does not have ND.*

Proof. In this situation, it was already shown by Liu that G does not have ND when either $m = 2$ and $n \geq 4$ or $m = 3$ [30, Lemma 2.8]. While Liu's statement of the lemma is different, the proof shows exactly that these groups do not have (ND). As our proof is uniform for all cases, this will include a repetition of Liu's result. The goal is to use lemma 3.8 and the items (i)–(iv) refer to this lemma. We set $p = 2$.

Let

$$r = a(a^{p^{m-1}} + b)(1 - a^{p^{m-1}})(1 + b^p)\widetilde{b^{p^2}},$$
$$s = a(a^{p^{m-2}} + b)(1 - a^{p^{m-1}})(1 - b^p)\widetilde{b^{p^2}},$$
$$y = 1 + a^{p^{m-2}}.$$

Note that

$$(1 + b^p)(1 - b^p)\widetilde{b^{p^2}} = (1 - b^{p^2})\widetilde{b^{p^2}} = 0,$$

https://doi.org/10.1017/prm.2025.10013 Published online by Cambridge University Press

so that $rs = sr = 0$ follows using that b^p is central in G. Furthermore,

$$\begin{aligned} a(a^{p^{m-1}} + b)a(a^{p^{m-1}} + b) &= a^p(a^{p^{m-1}} + ba^{p^{m-1}})(a^{p^{m-1}} + b) \\ &= a^p(1 + ba^{p^{m-1}} + b + b^p a^{p^{m-1}}) = a^p((1 - b^p) + (1 + a^{p^{m-1}})(b + b^p)). \end{aligned}$$

As

$$(1 - b^p)(1 + b^p)\widetilde{b^{p^2}} = 0 = (1 + a^{p^{m-1}})(1 - a^{p^{m-1}}), \tag{30}$$

this implies $r^2 = 0$. Moreover,

$$\begin{aligned} a(a^{p^{m-2}} + b)a(a^{p^{m-2}} + b) &= a^p(a^{p^{m-2}} + ba^{p^{m-1}})(a^{p^{m-2}} + b) \\ &= a^p(a^{p^{m-1}} + ba^{p^{m-2}} + ba^{p^{m-1}+p^{m-2}} + b^p a^{p^{m-1}}) \\ &= a^p(a^{p^{m-1}}(1 + b^p) + ba^{p^{m-2}}(1 + a^{p^{m-1}})) \end{aligned}$$

which by (30) also implies $s^2 = 0$. So (i) follows.

To construct the idempotent for (ii), note again that b^p is central in G so that if $f \in \mathrm{PCI}(\mathbb{Q}G)$, then $b^p f = \zeta I$ for a certain root of unity ζ, where I denotes the identity matrix of some size. The same argument applies to $a^{p^{m-1}}$. Now let $e \in \mathrm{PCI}(\mathbb{Q}G)$ which is the sum of all primitive central idempotents f such that $fa^{p^{m-1}}$ has order p and fb^p is the identity. Note that as $G' = \langle a^{p^{m-1}} \rangle$, this implies that fb is not central. So for each such f we have $rf \neq 0$. It is clear that $se = 0$ as $(1 - b^p)e = 0$. Furthermore, if f' is any primitive central idempotent such that $f'b^p$ is not the identity, then $f'(1 + b^p)\widetilde{b^{p^2}} = 0$. Similarly, if $f'a^{p^{m-1}}$ does not have order p, it must be the identity, so $f'(1 - a^{p^{m-1}}) = 0$. We conclude $r(1 - e) = 0$ and so $re = r$ and (ii) holds.

Next,

$$\begin{aligned} y(r + s) &= ya(1 - a^{p^{m-1}})\widetilde{b^{p^2}}((a^{p^{m-1}} + b)(1 + b^p) + (a^{p^{m-2}} + b)(1 - b^p)) \\ &= ya(1 - a^{p^{m-1}})\widetilde{b^{p^2}}(a^{p^{m-1}} + b^p a^{p^{m-1}} + a^{p^{m-2}} - b^p a^{p^{m-2}} + 2b) \\ &= ya(1 - a^{p^{m-1}})\widetilde{b^{p^2}}((a^{p^{m-2}}(1 + a^{p^{m-2}}) + b^p a^{p^{m-2}}(-1 + a^{p^{m-2}}) + 2b). \end{aligned}$$

Using that $1 + a^{p^{m-2}} \equiv -1 + a^{p^{m-2}} \equiv 1 - a^{p^{m-2}} \bmod 2$ this means

$$\begin{aligned} y(r + s) &\equiv a(1 + a^{p^{m-2}})(1 - a^{p^{m-2}})(1 - a^{p^{m-1}})\widetilde{b^{p^2}}(a^{p^{m-2}} + b^p a^{p^{m-2}}) \\ &= a(1 - a^{p^{m-1}})(1 - a^{p^{m-1}})\widetilde{b^{p^2}}(a^{p^{m-2}} + b^p a^{p^{m-2}}) \\ &\equiv a(1 + a^{p^{m-1}})(1 - a^{p^{m-1}})\widetilde{b^{p^2}}(a^{p^{m-2}} + b^p a^{p^{m-2}}) = 0 \mod 2. \end{aligned}$$

Hence $y(r + s)/p \in \mathbb{Z}G$ and (iii) holds.

Finally, it is easy to see that the coefficient of ab in the element

$$yr = (1 + a^{p^{m-2}})a(a^{p^{m-1}} + b)(1 - a^{p^{m-1}})(1 + b^p)\widetilde{b^{p^2}}$$

is 1, so that $yr/p \notin \mathbb{Z}G$. This proves (iv) and the fact that G does not have (ND) hence follows. □

https://doi.org/10.1017/prm.2025.10013 Published online by Cambridge University Press

For the case of odd primes, we will use the following technical lemma.

LEMMA 3.11. *Let* p *be an odd prime,* k *a positive integer and*

$$X = \langle x, z \mid x^{p^2} = 1, z^{p^k} = 1, [x, z] = 1 \rangle \cong C_{p^2} \times C_{p^k}.$$

Then there exist $\alpha, \beta \in \mathbb{Z}X$ *such that in* $\mathbb{Z}X$ *the following congruences hold:*

$$(1 - x^p)(1 - x^p z) + (1 - x^{-p})(1 - x^{-p} z) \equiv (1 - x)^{p+1} \alpha \mod p$$

and

$$x(1 - x^p)(1 - x^p z) + x^{-1}(1 - x^{-p})(1 - x^{-p} z) \equiv (1 - x)^{p+1} \beta \mod p.$$

Proof. To simplify notation, we write for a positive integer ℓ:

$$\gamma(x, \ell) = 1 + x + x^2 + \cdots + x^\ell.$$

We will several times use the equation

$$(1 - x^\ell) = (1 - x)\gamma(x, \ell - 1). \tag{31}$$

We will also use that

$$(1 - x^p) \equiv (1 - x)^p \mod p. \tag{32}$$

We proceed to show the first congruence using first $1 - x^{-p} = -x^{-p}(1 - x^p)$ and later (31) and finally (32). We also use $x^{-p} = x^{p^2 - p}$ and $x^{-3p} = x^{p^2 - 3p}$.

$$\begin{aligned}
&(1 - x^p)(1 - x^p z) + (1 - x^{-p})(1 - x^{-p} z) \\
=&(1 - x^p)(1 - x^p z) - x^{-p}(1 - x^p)(1 - x^{-p} z) \\
=&(1 - x^p)(1 - x^p z - x^{-p}(1 - x^{-p} z)) \\
=&(1 - x^p)((1 - x^{-p}) - x^p z(1 - x^{-3p})) \\
=&(1 - x^p)((1 - x)\gamma(x, p^2 - p - 1) - x^p z(1 - x)\gamma(x, p^2 - 3p - 1)) \\
=&(1 - x^p)(1 - x)(\gamma(x, p^2 - p - 1) - x^p z\gamma(x, p^2 - 3p - 1)) \\
\equiv&(1 - x)^{p+1}(\gamma(x, p^2 - p - 1) - x^p z\gamma(x, p^2 - 3p - 1)) \mod p.
\end{aligned}$$

Note that when $p = 3$, then in the fourth line $1 - x^{-3p} = 0$, so that $p^2 - 3p - 1$ does not appear later in this case. This shows the first congruence.

https://doi.org/10.1017/prm.2025.10013 Published online by Cambridge University Press

Next, we show the second congruence, also using $1-x^{-p}=-x^{-p}(1-x^p)$, (31) and (32) and also that $x^{-3p-2}=x^{p^2-3p-2}$ for $p\neq 3$ and $x^{-3p-2}=x^{p^2-2}$ for $p=3$:

$$\begin{aligned}
&x(1-x^p)(1-x^pz)+x^{-1}(1-x^{-p})(1-x^{-p}z)\\
=&x(1-x^p)(1-x^pz)-x^{-1}x^{-p}(1-x^p)(1-x^{-p}z)\\
=&(1-x^p)(x(1-x^pz)-x^{-p-1}(1-x^{-p}z))\\
=&(1-x^p)(x-x^{-p-1}-x^{p+1}z+x^{-2p-1}z)\\
=&(1-x^p)(x(1-x^{-p-2})-x^{p+1}z(1-x^{-3p-2}))\\
=&(1-x^p)(1-x)(x\gamma(x,p^2-p-3)-x^{p+1}z\gamma(x,p^2-3p-3))\\
\equiv&(1-x)^{p+1}(x\gamma(x,p^2-p-3)-x^{p+1}\gamma(x,p^2-3p-3))\mod p,
\end{aligned}$$

where in the last two lines in case $p=3$ the expression p^2-3p-3 has to be replaced by p^2-3. This shows the second congruence. □

The next three lemmas will now take care of the remaining cases for the groups $G(p,m,n)$.

LEMMA 3.12. *Let* p *be odd, $m\geq 3$ and $n\geq 2$. Then $G=G(p,m,n)$ does not have ND.*

Proof. Set

$$\begin{aligned}
r&=(b-a^{p^{m-2}})a(1-a^{p^{m-1}})\widetilde{b^{p^2}}\prod_{i=0}^{p-2}(1-b^pa^{ip^{m-1}}),\\
s&=(b-a^{-p^{m-2}})a(1-a^{-p^{m-1}})\widetilde{b^{p^2}}\prod_{i=2}^{p}(1-b^pa^{ip^{m-1}}),\\
y&=(1-a^{p^{m-2}})^{p(p-1)-1}.
\end{aligned}$$

We will again show (i)–(iv) from lemma 3.8 which will imply that G does not have (ND). We analyse the irreducible representations of G in which r and s are not mapped to 0. Note that as a^p and b^p are central, they are mapped to a central matrix under every irreducible representation. Let R be an irreducible $\mathbb{Q}$-representation and e the corresponding primitive central idempotent of $\mathbb{Q}G$. Denote by I the identity matrix. If $R(b^{p^2})\neq I$, then $e\widetilde{b^{p^2}}=0$, as the sum over all the powers of a primitive p^ℓth root of unity equals 0 when $\ell\geq 1$. Moreover $R(b^p)=I$ implies $e(1-b^p)=0$. Hence, as both r and s contain the factor $(1-b^p)\widetilde{b^{p^2}}$ the inequality $er\neq 0$ implies that $R(b^p)=\zeta I$ for ζ a primitive pth root of unity while $es\neq 0$ implies $R(b^p)=\zeta' I$ for ζ' a primitive pth root of unity. Moreover, if $R(a^{p^{m-1}})=I$, then $e(1-a^{p^{m-1}})=0$. As $a^{p^{m-1}}$ has order p, we conclude that $er\neq 0$ implies $R(a^{p^{m-1}})=\xi I$ while $es\neq 0$ implies $R(a^{p^{m-1}})=\xi' I$ for certain primitive pth roots of unity ξ and ξ'. The factor $\prod_{i=1}^{p-2}(1-b^pa^{ip^{m-1}})$ in r means that $er\neq 0$ implies $R(b^p)\neq R(a^{ip^{m-1}})^{-1}$ for every $1\leq i\leq p-2$. From the fact that both b^p and $a^{p^{m-1}}$ are mapped to elements of order p, we conclude that $er\neq 0$ means $R(b^p)=$

https://doi.org/10.1017/prm.2025.10013 Published online by Cambridge University Press

$R(a^{p^{m-1}})$, i.e. $eb^p = ea^{p^{m-1}}$. Similarly $es \neq 0$ implies $eb^p = ea^{-p^{m-1}}$. It follows that r and s live in different components of $\mathbb{Q}G$, so that $rs = sr = 0$ and also (ii) holds.

We next show that $r^p = 0$. The non-central factors of r give

$$((b - a^{p^{m-2}})a)^p = a^p(b - a^{p^{m-2}})(ba^{(p-1)p^{m-1}} - a^{p^{m-2}})(ba^{(p-2)p^{m-1}} - a^{p^{m-2}}) \cdots (ba^{p^{m-1}} - a^{p^{m-2}}).$$

From the paragraph before we know that when $er \neq 0$, then $R(a^{p^{m-1}}) = \zeta I$ for some primitive pth root of unity ζ. So then

$$e((b - a^{p^{m-2}})a)^p = ea^p(b - a^{p^{m-2}})(b\zeta^{-1} - a^{p^{m-2}})(b\zeta^{-2} - a^{p^{m-2}}) \cdots (b\zeta - a^{p^{m-2}}).$$

We claim that the coefficient of $a^{ip^{m-2}}$ in the expression

$$(b - a^{p^{m-2}})(b\zeta^{-1} - a^{p^{m-2}})(b\zeta^{-2} - a^{p^{m-2}}) \cdots (b\zeta - a^{p^{m-2}})$$

is 0 for every $1 \leq i \leq p-1$. Indeed, using $\prod_{j=0}^{p-1}(X - \zeta^j) = X^p - 1$, as an equation in the polynomial ring $\mathbb{Z}[X]$, up to the factor b^i and possibly a sign this coefficient is the same as in $\prod_{j=0}^{p-1}(a^{p^{m-2}} - \zeta^j) = (a^{p^{m-2}})^p - 1$. So,

$$e((b - a^{p^{m-2}})a)^p = ea^p(b^p - a^{p^{m-1}}) = 0,$$

where the last equality follows from the previous paragraph. Hence, $r^p = 0$. A similar calculation shows also s^p, so that (i) follows.

We proceed to show (iii). We first calculate

$$\begin{aligned}
y(r+s) &= y\widetilde{b^{p^2}}(1 - b^p)\prod_{i=2}^{p-2}(1 - a^{ip^{m-1}}b^p) \\
&\quad \cdot ((b - a^{p^{m-2}})a(1 - a^{p^{m-1}})(1 - a^{p^{m-1}}b^p) \\
&\quad + (b - a^{-p^{m-2}})a(1 - a^{-p^{m-1}})(1 - a^{-p^{m-1}}b^p)) \\
&= y\widetilde{b^{p^2}}(1 - b^p)\prod_{i=2}^{p-2}(1 - a^{ip^{m-1}}b^p) \\
&\quad \cdot (ba((1 - a^{p^{m-1}})(1 - a^{p^{m-1}}b^p) + (1 - a^{-p^{m-1}})(1 - a^{-p^{m-1}}b^p)) \\
&\quad - a(a^{p^{m-2}}(1 - a^{p^{m-1}})(1 - a^{p^{m-1}}b^p) \\
&\quad + a^{-p^{m-2}}(1 - a^{-p^{m-1}})(1 - a^{-p^{m-1}}b^p))).
\end{aligned}$$

So the last two lines mean that, taking into account the factor y, it is enough to show that

$$y((1 - a^{p^{m-1}})(1 - a^{p^{m-1}}b^p) + (1 - a^{-p^{m-1}})(1 - a^{-p^{m-1}}b^p)) \equiv 0 \mod p \qquad (33)$$

https://doi.org/10.1017/prm.2025.10013 Published online by Cambridge University Press

and

$$y(a^{p^{m-2}}(1-a^{p^{m-1}})(1-a^{p^{m-1}}b^p) + a^{-p^{m-2}}(1-a^{-p^{m-1}})(1-a^{-p^{m-1}}b^p)) \equiv 0 \mod p. \tag{34}$$

Note that

$$y(1-a^{p^{m-2}})^{p+1} = (1-a^{p^{m-2}})^{p(p-1)-1+p+1} = (1-a^{p^{m-2}})^{p^2} \equiv (1-a^{p^m}) = 0 \mod p$$

by (32). So to prove (33) and (34), it is enough to show that the factors to the right of y contain a factor $(1-a^{p^{m-2}})^{p+1}$ modulo p. This follows by applying lemma 3.11 with $x = a^{p^{m-2}}$ and $z = b^p$. This shows (iii).

Finally, to get (iv), note that the coefficient of ba in yr is 1. This follows as none of the products one can get by factoring out the element yr gives ba except the trivial one which in turns follows as the powers appearing for a and b are otherwise not big enough to sum up to p^m or p^n, respectively, when a and b are both taken in as a factor. □

LEMMA 3.13. *Let* p *be odd,* m = 2 *and* n > m. *Then* $G = G(p, m, n)$ *does not have ND.*

Proof. Again we will show (i)–(iv) from lemma 3.11, this time using the elements:

$$r = (a - b^{p^{n-2}})b(1-b^{p^{n-1}})\prod_{i=0}^{p-2}(1-a^p b^{ip^{n-1}}),$$

$$s = (a - b^{-p^{n-2}})b(1-b^{-p^{n-1}})\prod_{i=2}^{p}(1-a^p b^{ip^{n-1}}),$$

$$y = (1-b^{p^{n-2}})^{p(p-1)-1}.$$

We again first analyse the properties of primitive central idempotents which do not map r or s to 0. Note that a^p and $b^{p^{n-1}}$ both have order p. Let $e \in \mathrm{PCI}(\mathbb{Q}G)$. The factor $(1-a^p)$ in both r and s means that $er \neq 0$ implies that ea^p has order p and also $es \neq 0$ means that ea^p has order p. From the factor $(1-b^{p^{n-1}})$ in r and the factor $(1-b^{-p^{n-1}})$ in s, we also get that $er \neq 0$ implies that $eb^{p^{n-1}}$ has order p and $es \neq 0$ implies the same. Finally, the rest of the factors appearing on the right from b then mean that $er \neq 0$ implies $ea^p = eb^{p^{n-1}}$ and $es \neq 0$ implies $ea^p = eb^{-p^{n-1}}$. This, in particular, gives that $rs = sr = 0$ and (ii).

Computing r^p and s^p is also very similar to the previous case. Namely the non-central part of r gives

$$((a - b^{p^{n-2}})b)^p = b^p(a - b^{p^{n-2}})(aa^p - b^{p^{n-2}})(aa^{2p} - b^{p^{n-2}})\cdots(aa^{(p-1)p} - b^{p^{n-2}}).$$

As ea^p has order p when $er \neq 0$, the coefficient of $(b^{p^{n-2}})^i$ in the expression

$$e(a - b^{p^{n-2}})(aa^p - b^{p^{n-2}})(aa^{2p} - b^{p^{n-2}})\cdots(aa^{(p-1)p} - b^{p^{n-2}})$$

https://doi.org/10.1017/prm.2025.10013 Published online by Cambridge University Press

is 0 for all $1 \leq i \leq p-1$, so that $e((a-b^{p^{n-2}})b)^p = eb^p(a^p - b^{p^{n-1}}) = 0$, implying $r^p = 0$. Similarly $s^p = 0$. Overall, we obtain (i).

Now,

$$\begin{aligned} y(r+s) = y(1-a^p)\prod_{i=2}^{p-2}(1-a^pb^{ip^{n-1}}) \\ \cdot ((a-b^{p^{n-2}})b(1-b^{p^{n-1}})(1-a^pb^{p^{n-1}}) \\ + (a-b^{-p^{n-2}})b(1-b^{-p^{n-1}})(1-a^pb^{-p^{n-1}})) \\ = \; y(1-a^p)\prod_{i=2}^{p-2}(1-a^pb^{ip^{n-1}}) \\ \cdot (ab((1-b^{p^{n-1}})(1-a^pb^{p^{n-1}}) + (1-b^{-p^{n-1}})(1-a^pb^{-p^{n-1}})) \\ - b(b^{p^{n-2}}(1-b^{p^{n-1}})(1-a^pb^{p^{n-1}}) \\ + b^{-p^{n-2}}(1-b^{-p^{n-1}})(1-a^pb^{-p^{n-1}}))). \end{aligned}$$

As $y(1-b^{p^{n-2}})^{p+1} = (1-b^{p^{n-2}})^{p(p-1)-1+p+1} = (1-b^{p^{n-2}})^{p^2} \equiv 0 \mod p$, it is hence enough to show that the expressions

$$(1-b^{p^{n-1}})(1-a^pb^{p^{n-1}}) + (1-b^{-p^{n-1}})(1-a^pb^{-p^{n-1}}) \tag{35}$$

and

$$b^{p^{n-2}}(1-b^{p^{n-1}})(1-a^pb^{p^{n-1}}) + b^{-p^{n-2}}(1-b^{-p^{n-1}})(1-a^pb^{-p^{n-1}}) \tag{36}$$

when considered modulo p both contain a factor $(1-b^{p^{n-2}})^{p+1}$. This follows by applying lemma 3.11 for $x = b^{p^{n-2}}$ and $z = a^p$. So we have (iii). Moreover analysing yr, we see that the coefficient of ab equals 1, so also (iv) follows and G does not have (ND) in this case. □

LEMMA 3.14. *Let* p *be odd. Then* $G = G(p,2,2)$ *does not have ND.*

Proof. We note that the case $p = 3$ was considered in [32, Lemma 2.2], but we will use different arguments. We will again show (i)–(iv) from lemma 3.11 using

$$\begin{aligned} r =& (b-a)(1-a^p)\prod_{i=0}^{p-2}(1-a^{ip}b^p), \\ s =& (b-a^{-1})(1-a^{-p})\prod_{i=2}^{p}(1-a^{ip}b^p), \\ y =& (1-a)^{p(p-1)-1}. \end{aligned}$$

The proof of the fact that $r^p = s^p = 0$ is different from the cases before, so that we postpone this to the end. We start again by analysing the properties of primitive central idempotents not annihilating r and s. Similarly as in the other cases, we get that $er \neq 0$ implies that ea^p and eb^p have order p and $ea^p = eb^p$ holds. Also,

https://doi.org/10.1017/prm.2025.10013 Published online by Cambridge University Press

$es \neq 0$ implies that ea^p and eb^p have order p and $ea^p = eb^{-p}$. So $rs = sr = 0$ and (ii) follow.

Similarly as we had to show (33) and (34) before we now need to obtain that

$$(1 - a^p)(1 - a^p b^p) + (1 - a^{-p})(1 - a^{-p} b^p)$$

and

$$a(1 - a^p)(1 - a^p b^p) + a^{-1}(1 - a^{-p})(1 - a^{-p} b^p)$$

both contain a factor $(1-a)^{p+1}$ when considered modulo p. This follows by applying lemma 3.11 for $x = a$ and $z = b^p$ and so we obtain (iii). It is also easy to see that the coefficient of b in yr is 1, so that (iv) holds.

It remains to prove $r^p = s^p = 1$. We first claim that there is exactly one $e \in \mathrm{PCI}(\mathbb{Q}G)$ such that $er \neq 0$. To see this, note that, since the centre of G is $\langle a^p \rangle \times \langle b^p \rangle$ and isomorphic to an elementary abelian group of rank 2, for each possible kernel different from the derived subgroup $\langle a^p \rangle$ there can be only one component with centre $\mathbb{Q}(\zeta)$ for dimension reasons. Here ζ denotes a primitive pth root of unity. Also, there is exactly one $\in \mathrm{PCI}(\mathbb{Q}G)e$ such that $es \neq 0$. We will work in these unique components using explicit representations to see that $r^p = s^p = 0$. Set

$$A = \begin{pmatrix} 0 & 0 & \cdots & 0 & 1 \\ \zeta & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 \\ \vdots & & \ddots & & \vdots \\ 0 & 0 & \cdots & 1 & 0 \end{pmatrix}$$

and

$$C = \begin{pmatrix} 1 & 0 & 0 & \cdots & 0 \\ 0 & \zeta^{-1} & 0 & \cdots & 0 \\ 0 & 0 & \zeta^{-2} & \cdots & 0 \\ \vdots & & & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & \zeta \end{pmatrix}.$$

Then $A^p = \zeta I$, where I denotes the identity matrix, and $C^{-1}AC = A^{p+1}$. Hence each map $R_i : G \to M_p(\mathbb{Q}(\zeta))$ sending a to A and b to $A^i C$ for $0 \leq i \leq p-1$ is a representation of G, since also $(A^i C)^p = A^{ip}$ is an element of order p. In fact, all these representations are irreducible: the degree of the representations is the smallest non-trivial divisor of the order of G, so any non-trivial decomposition would involve only linear representations. But the linear representations contain the derived subgroup $\langle a^p \rangle$ in their kernel, hence the character values of a^p under the sum of p linear representations is p, while the character value of a^p under every of the representations R_i is $p\zeta$. We note also that when D is a diagonal matrix with one of the diagonal entries being 0, then $(A^i D)^p = 0$. This follows, since the characteristic polynomial of $A^i D$ equals $-X^p + \zeta^i d_1 d_2 \cdots d_p$, where $d_1, \ldots, d_p$ are the diagonal elements of D, so that the only eigenvalue of $A^i D$ is 0 when one of the d_j's equals 0.

https://doi.org/10.1017/prm.2025.10013 Published online by Cambridge University Press

The $e \in \mathrm{PCI}(\mathbb{Q}G)$ which satisfies $er \neq 0$ corresponds to the representation R_1, as in general $R_i(a^{ip}) = R_i(b^p)$ and as we saw before $ea^p = eb^p$. Now $R_1(a-b) = AC - A = A(C-I)$ and $C - I$ is a diagonal matrix containing 0 on the diagonal. So, $r^p = 0$ follows. Similarly R_{p-1} is the representation corresponding to the primitive central idempotent not annihilating s and $D_{p-1}(b-a^{-1}) = A^{p-1}C - A^{-1} = A^{-1}(A^pC - I)$ and as also $A^pC - I$ is a diagonal matrix containing 0 on the diagonal, we get $s^p = 0$ by the paragraph before. This finishes the proof of (i) in this case and the theorem follows. □

We are finally ready to prove the main theorem of this section.

Proof of Theorem 3.5. By Theorem C, it remains to consider nilpotent group which have SSN. As observed in [33, Section 4], these were in fact classified in [12]. They fall into nine categories. For eight of these categories, it is shown in [27, Section 4] that if G lies in one of them, it has ND if and only if $\mathbb{Q}G$ has at most one matrix component. The last category which remains open in general are the groups $G(p, m, n)$.

We already know by Theorem 3.6 that $G(2, 2, 3)$ does have ND. So to exclude the cases of G having one matrix component by lemma 3.9, we can assume that $n \geq 2$ and $(m, n) \notin \{(2, 2), (2, 3)\}$ if $p = 2$. Then G does not have ND for any of the remaining cases by lemmas 3.10, 3.12, 3.13, and 3.14. □

3.3. Non-nilpotent groups

The goal of this section is to handle the non-nilpotent part of Theorem A. Namely, we show:

THEOREM 3.15. *Let* G *be a finite group which is not nilpotent and not an SSN group of unfaithful type. Then* G *has ND if and only if it has one matrix component.*

In case that G has more than one matrix component the proof of Theorem 3.15 will, in fact, construct an explicit nilpotent element $n \in \mathbb{Z}G$ and central idempotent e such that $ne \notin \mathbb{Z}G$. In §5.2, we will dig deeper into this and it will turn out that the existence of these elements is connected to the kernels of the irreducible $\mathbb{Q}$-representations of G.

Proof of Theorem 3.15 for G *solvable.* For every finite group G whenever $\mathbb{Q}G$ has at most one matrix component, then G has ND. Conversely, assume that G has ND and hence property SN. As G is assumed to not be an SSN group of unfaithful type, Proposition 2.17 says that $G \cong P \rtimes H$ for an elementary abelian p-group P, where the action is faithful, irreducible and $[x, h] \neq 1$ for every non-trivial $x \in P$ and $h \in H$. Moreover H is Dedekind. In other words, by Theorem 2.1, either H is abelian or $H \cong Q_8 \times D$ with D an abelian group of odd order. In the latter case, we denote by $c \in Q_8$ the unique (central) element of order 2.

Claim 1: P is the unique maximal abelian subgroup. Moreover, it contains no non-trivial subgroup which is normal in G. Also, a subgroup N of G is normal in G iff $P \subseteq N$. If H is abelian, then G is metabelian with $G' = P$. If H is non-abelian, then $G' = \langle P, c \rangle$ and $G'' = P$.

https://doi.org/10.1017/prm.2025.10013 Published online by Cambridge University Press

First notice that since P is elementary abelian and the action of H on P is irreducible it cannot contain a subgroup normal in G. Moreover, as $[x,h] \neq 1$ for all non-trivial $x \in P, h \in H$, P is indeed the unique maximal abelian subgroup. Now, if $G/P \cong H$ is abelian, then $G' \subseteq P$ and thus by the first part $G' = P$. If $H \cong Q_8 \times D$, we directly see that $G' \subseteq \langle P, c\rangle$. Using that $G' \cap P \subseteq P$ is normal in G one has that $P \subset G'$ and hence $G' = \langle P, c\rangle$. Analogously we see that $G'' \subseteq P$ and in fact $G'' = P$ as G'' is normal. Finally, consider $N \trianglelefteq G$. Then $N \cap P \subseteq P$ is normal in G, hence $N \subseteq P$ as H contains no normal subgroups. Conversely, if $P \subseteq N$ then $N/P \leq G/P$. As mentioned above G/P is Dedekind and thus N/P is normal as claimed.

Next note that G is strongly monomial, being abelian-by-supersolvable, and hence by [24, Theorem 3.5.10] all primitive central idempotents of $\mathbb{Q}G$ are of the form $e(G,N,K)$ for some strong Shoda pairs (N,K). As recorded in [27, Lemma 2.4.], $\mathbb{Q}[G]e(G,N,K)$ is commutative if and only if $G' \subseteq K$.

Claim 2: The tuples in $\{(P,K) \mid [P:K] = p\}$ are strong Shoda pair of G. Conversely, if (N,K) is a strong Shoda pair with $N \trianglelefteq G$, then $P \subseteq K$ or $N = P$.

Let $K \trianglelefteq N \trianglelefteq G$. Then [24, Corollary 3.5.11] tells that (N,K) is a strong Shoda pair exactly when N/K is cyclic and N/K is a maximal abelian subgroup of $N_G(K)/K$. In particular, $N' \subseteq K$.

To start notice that $\langle P,h\rangle/K$ is non-abelian for every $K \lneq P$ and non-trivial $h \in H$. This follows from [2, (24.6), p. 112] asserting that $P = [P, \langle h\rangle]$. Consequently, P/K is maximal abelian in $N_G(K)/K$ and hence (P,K) is a strong Shoda pair when $[P:K] = p$. Next, by the first claim $P \leq N$ when $N \trianglelefteq G$. Suppose $P \nsubseteq K$. If N/P is abelian, then $N' \leq P \cap K \lneq P$. As $N' \trianglelefteq G$, the first claim yields $N' = 1$ and so $N = P$. If N/P is non-abelian, then H is non-abelian and $c \in N$. So in that case $G' = \langle P, c\rangle \leq N$, which entails that $G'' = P \leq N' \leq K$, a contradiction. This proves the second claim.

By [24, Problem 3.4.4.], the number of simple components $\mathbb{Q}Ge(G,P,K)$ with $[P:K] = p$, denoted s, is equal to the number of orbits of H acting on $\mathcal{S} := \{K \mid [P:K] = p\}$. To count the latter we decompose $\mathcal{S} = \bigcup_{d||H|} \mathcal{S}_d$ with $\mathcal{S}_d := \{K \in \mathcal{S} \mid |N_H(K)| = d\}$. Note that the action of H on $\mathcal{S}$ preserves each $\mathcal{S}_d$ and denote by s_d the number of H-orbits thereon. Thus $s = \sum_{d||H|} s_d$ and

$$s_d = \frac{1}{|H|} \sum_{K \in \mathcal{S}_d} |N_H(K)| = \frac{d\,.\,|\mathcal{S}_d|}{|H|}. \tag{37}$$

Next let $\mathcal{T}_K$ be a left transversal for $N_H(K)$ in H. Then as every $K \in \mathcal{S}_d$ is a maximal subgroup, one has by Theorem 3.3 that

$$e_K := e(G,P,K) = \sum_{h \in \mathcal{T}_K} (\widehat{K}^h - \widehat{P}).$$

Now consider any non-trivial nilpotent element of the form

$$x = (1-y)g\widetilde{H}$$

with $1 \neq y \in H$ and $g \in G \setminus N_G(H)$ (which exists as H is non-normal).

https://doi.org/10.1017/prm.2025.10013 Published online by Cambridge University Press

Claim 3: If $xe_K \in \mathbb{Z}G$ for all $K \in \mathcal{S}$, then $s = 1$.

First write $y^g = t.v$ with $t \in P$ and $v \in H$. As x is non-trivial, also $t \neq 1$ and $x = g(1-y^g)\widetilde{H} = g(1-t)\widetilde{H}$. Therefore $g^{-1}xe_K = (1-t)e_K\widetilde{H} \in \mathbb{Z}G$. Because $K \subseteq P \trianglelefteq G$, one has that $\mathrm{supp}((1-t)e_K) \subseteq P$ and so $(1-t)e_K \in \mathbb{Z}P$. Next note that $(1-t)\widehat{P} = 0$ and $(1-t)\widehat{K^h} = 0$ exactly when $t \in K^h$. Therefore $(1-t)e_K \in \mathbb{Z}P$ exactly means that

$$\frac{|\{h \in \mathcal{T}_K \mid t \notin K^h\}|}{|K|} \in \mathbb{Z}.$$

Recall that $\mathrm{core}_G(K) = \ker(g \mapsto ge_K)$, by Theorem 3.3, which is trivial in this case. In particular $|\{h \in \mathcal{T}_K \mid t \notin K^h\}| \neq 0$. Therefore, if $K \in \mathcal{S}_d$ then $|K| \leq |\mathcal{T}_K| = |H|/d$. Now (37) entails that $s_d|K| \leq |S_d|$ which sums up to $s|K| \leq |S| = \frac{|P|-1}{p-1}$, since $|S|$ is the number of maximal dimensional subspaces in the $\mathbb{F}_p$-vector space P. As $[P : K] = p$ the latter inequality simplifies to $s(p-1) \leq p - \frac{1}{|K|} \leq p-1$, hence $s \leq 1$. In fact $s = 1$ by the second claim.

Next notice that by [27, Lemma 3.3], $\mathbb{Q}H$ has no non-zero nilpotent elements. Therefore, when decomposing $\mathbb{Q}G$ as

$$\mathbb{Q}G \cong \mathbb{Q}G\widehat{P} \oplus \mathbb{Q}G(1-\widehat{P})$$

the piece $\mathbb{Q}G\widehat{P} \cong \mathbb{Q}G/P \cong \mathbb{Q}H$ has no matrix components. So, it remains to prove that $\mathbb{Q}G(1-\widehat{P})$ is simple. By lemma 3.4

$$\dim_{\mathbb{Q}}(\mathbb{Q}Ge_K) = |H|(p-1)[G : N_G(K)].$$

Furthermore, $[G : N_G(K)] = [H : N_H(K)] = |\mathcal{T}_d|$ if $K \in \mathcal{S}_d$. By the third claim, there is a unique $d \mid |H|$ such that $s = s_d$ and $s = 1$. So (37) translates to $|\mathcal{T}_d| = |S| = \frac{|P|-1}{p-1}$. Altogether,

$$\dim_{\mathbb{Q}}(\mathbb{Q}G\widehat{P}) + \dim_{\mathbb{Q}}(\mathbb{Q}Ge_K) = |H| + |H|(|P|-1) = |H|.|P| = \dim_{\mathbb{Q}}(\mathbb{Q}G).$$

Thus $\mathbb{Q}G(1-\widehat{P}) = \mathbb{Q}Ge_K$ is indeed simple, finishing the proof. □

It now remains to consider finite non-solvable groups. In this case, we prove that none of the groups as in Proposition 2.18 have ND. This will be done by proving that for every such group there is always a bicyclic nilpotent element which does not have ND.

Proof of Theorem 3.15 for G *non-solvable.* If G has SN, then it does not have ND by [27, Proposition 3.4]. So assume G has SN. By Proposition 2.18, we know G has a unique minimal normal subgroup S which is a direct product of isomorphic non-abelian simple groups and that G/S is Dedekind.

Let $y \in G$ be an element of order 2 and $x \in G$ such that $y^x \notin \langle y \rangle$. Such x and y exist, as S has even order by the Feit–Thompson Theorem. Hence we can construct

https://doi.org/10.1017/prm.2025.10013 Published online by Cambridge University Press

the non-trivial nilpotent element $n = (1-y)x(1+y)$. If we write n in the shape as in lemma 2.7, then

$$\alpha(g) = \begin{cases} 1, & g = x \text{ or } g = xy, \\ -1, & g = yx \text{ or } g = yxy, \\ 0, & \text{else.} \end{cases}$$

So by lemma 2.7 the coefficient of ne at x is

$$\frac{k}{|G|}\sum_{h\in G}\alpha(h)\chi(x^{-1}h) = \frac{k}{|G|}\chi\left(1+y-x^{-1}yx(1+y)\right) = \frac{k}{|G|}\chi\left(1-[x,y]\right), \quad (38)$$

where in the last step we used $y = y^{-1}$ as well as the fact that y and $x^{-1}yx$ are conjugate and so have the same character value, which allows us to cancel them. If S is not contained in the kernel of χ, then the value appearing in (38) is not 0. Moreover, we have

$$\left|\frac{k}{|G|}\chi\left(1-[x,y]\right)\right| \leq \frac{2\chi(1)k}{|G|} = \frac{2\dim_{\mathbb{Q}}(e\mathbb{Q}G)}{|G|}.$$

So if the last is a rational number smaller than 1 for χ corresponding to a faithful representation, the product ne cannot lie in $\mathbb{Z}G$.

Now set $f = \widehat{S}$. Then $\mathbb{Q}G = f\mathbb{Q}G \oplus (1-f)\mathbb{Q}G$ and the direct summand $(1-f)\mathbb{Q}G$ corresponds to all the irreducible faithful representations of G. None of the indecomposable direct summands in $(1-f)\mathbb{Q}G$ is a division algebra, as $\mathrm{SL}(2,5)$ is the only non-solvable group which is a finite subgroup of a division algebra [44, 2.1.4]. If $(1-f)\mathbb{Q}G$ is decomposable, then one of its indecomposable direct summands must have dimension smaller than $\frac{|G|}{2}$, as $f\mathbb{Q}G$ has positive dimension and $|G| = \dim(f\mathbb{Q}G) + \dim((1-f)\mathbb{Q}G)$. Now the number of simple components of $\mathbb{Q}G$ equals the number of conjugacy classes of cyclic subgroups of G [24, Corollary 7.1.12]. The components in $f\mathbb{Q}G$ correspond to conjugacy classes in G/S, i.e. classes not lying in S except for the class of the trivial element. But as S certainly contains at least three conjugacy classes, we conclude that $(1-f)\mathbb{Q}G$ has at least two indecomposable summands. □

4. On a measure for unipotents to have an integral decomposition

In [27, Section 6], it was observed by Jespers–Sun that one can measure how far a given finite group G is from not having ND via a certain group denoted $q(G)$, whose definition only depends on $\mathcal{U}(\mathbb{Z}G)$. In loc.cit. also two rather general problems about $q(G)$ were presented: to classify the groups G for which $q(G)$ is finite and to establish a connection between the structure of $q(G)$ and the simple components of $\mathbb{Q}G$. We present answers to the two problems. Namely we will show that $q(G)$ is a finite group when no simple component of $\mathbb{Q}G$ is exceptional, and infinite when it has a simple component isomorphic to $M_2(\mathbb{Q})$ and a further group-theoretical condition holds. We end by defining and pointing out that the obstruction might also be of interest for arithmetic subgroups of general semisimple algebraic groups.

https://doi.org/10.1017/prm.2025.10013 Published online by Cambridge University Press

4.1. The measure and link to elementary subgroups

Consider the Wedderburn–Artin decomposition

$$\mathbb{Q}G \cong \bigoplus_{e \in \mathrm{PCI}(\mathbb{Q}G)} \mathrm{M}_{n_e}(D_e), \tag{39}$$

where $\mathbb{Q}Ge \cong \mathrm{M}_{n_e}(D_e)$ with D_e a finite-dimensional division algebra over $\mathbb{Q}$. Moreover let $\mathcal{U}(\mathbb{Z}G)_{un} := \{\alpha \in \mathcal{U}(\mathbb{Z}G) \mid \alpha \text{ is unipotent } \}$ be the set of unipotent units in $\mathcal{U}(\mathbb{Z}G)$. For every $e \in \mathrm{PCI}(\mathbb{Q}G)$ consider the subset

$$\mathcal{E}_G(e) := \{\alpha \in \mathcal{U}(\mathbb{Z}G)_{un} \mid (\alpha - 1)e = \alpha - 1\}$$

of unipotent elements such that $\mathbb{Q}Ge$ is the only component to which the element projects non-trivially.

Denote by $\mathrm{SL}_1(\mathbb{Z}G)$ the group of elements in $\mathcal{U}(\mathbb{Z}G)$ whose projections to every simple component of $\mathbb{Q}G$ all have reduced norm 1 over the centre of that component (cf. [24, p. 67] for the definition). Note that $\langle \mathcal{U}(\mathbb{Z}G)_{un} \rangle$ and $\langle \mathcal{E}_G(e) \rangle$ are normal subgroups of $\mathcal{U}(\mathbb{Z}G)$ which are contained in $\mathrm{SL}_1(\mathbb{Z}G)$. The measure is the following quotient group:

$$q(G) := \langle \mathcal{U}(\mathbb{Z}G)_{un} \rangle / \langle \mathcal{E}_G(e) \mid e \in \mathrm{PCI}(\mathbb{Q}G) \rangle. \tag{40}$$

As noticed in [27, Section 6], G has ND if and only if $q(G) = 1$. As such it indeed measures how far G is from having ND. Furthermore in loc.cit., the authors asked when this group is finite and how its structure is connected to the simple components of $\mathbb{Q}G$. To answer this, we will investigate certain concrete subgroups of $\langle \mathcal{U}(\mathbb{Z}G)_{un} \rangle$.

Let $\mathcal{O}$ be an order in a division algebra D of finite dimension over $\mathbb{Q}$ and J a non-zero ideal in $\mathcal{O}$. Then we set

$$E_n(J) := \langle e_{ij}(r) \mid 1 \leq i \neq j \leq n,\, r \in J \rangle,$$

where $e_{ij}(r)$ is the elementary matrix in $\mathrm{GL}_n(\mathcal{O})$ which has 1 on the diagonal and r in the (i, j)-entry. Next, partition $\mathrm{PCI}(\mathbb{Q}G)$ into the two subsets $\mathrm{PCI}(\mathbb{Q}G)_{div} := \{e \in \mathrm{PCI}(\mathbb{Q}G) \mid \mathbb{Q}Ge \text{ is a division algebra}\}$ and its complement $\mathrm{PCI}(\mathbb{Q}G)_{\geq 2}$ of primitive central idempotents yielding simple components of reduced degree at least 2. In this definition, we also view a field as a division algebra.

Classical results imply directly the following useful fact, where the index at the right hand side can be infinite.

Proposition 4.1. *With notation as in (39), let* $f = \sum_{e' \in \mathrm{PCI}(\mathbb{Q}G)_{div}} e'$ *and for every* $e \in \mathrm{PCI}(\mathbb{Q}G)_{\geq 2}$ *fix a maximal order* $\mathcal{O}_e$ *in* $\mathrm{D_e}$. *Then, there exists a subgroup* $\mathrm{U_e}$ *of* $\langle \mathcal{U}(\mathbb{Z}G)_{un} \rangle$ *which is of the form* $1 - e + E_{n_e}(J_e)$ *for some non-zero ideal* $\mathrm{J_e}$ *of* $\mathcal{O}_e$. *Consequently,*

$$|q(G)| \leq [\mathrm{SL}_1(\mathbb{Z}G)(1-f) : \prod_{e \in \mathrm{PCI}(\mathbb{Q}G)_{\geq 2}} U_e] \leq \prod_{e \in \mathrm{PCI}(\mathbb{Q}G)_{\geq 2}} [\mathrm{SL}_{n_e}(\mathcal{O}_e) : E_{n_e}(J_e)].$$

Proof. For every $e \in \mathrm{PCI}(\mathbb{Q}G)_{\geq 2}$ one can choose an idempotent f_e in $\mathbb{Q}G$ such that ef_e is non-central in $\mathbb{Q}Ge$. Consider the associated generalized bicyclic units

https://doi.org/10.1017/prm.2025.10013 Published online by Cambridge University Press

$\mathrm{GBic}^{\{f_e\}}(\mathbb{Q}G)$, see [24, Section 11.2] for definition. Then following [22, Theorem 6.3] the group $\mathrm{GBic}^{\{f_e\}}(\mathbb{Q}G)$ contains a subgroup U_e of the form $1 - e + E_{n_e}(J_e)$ for some non-zero ideal J_e of $\mathcal{O}_e$. As $\mathrm{GBic}^{\{f_e\}}(\mathbb{Q}G)$ is a subgroup of $\langle \mathcal{U}(\mathbb{Z}G)_{un} \rangle$ the previous implies the first part of the statement.

Next note that $\mathrm{SL}_1(\mathbb{Z}G)(1-f)$ is the projection of $\mathrm{SL}_1(\mathbb{Z}G)$ onto the simple components of $\mathbb{Q}G$ of reduced degree at least 2. Also notice that a unipotent unit α in $\mathbb{Z}G$ projects in every simple component to a unipotent element and in particular has reduced norm 1 there. Thus $\langle \mathcal{U}(\mathbb{Z}G)_{un} \rangle$ can be viewed as a subgroup of $\mathrm{SL}_1(\mathbb{Z}G)(1-f)$. Moreover, by definition $\mathrm{SL}_1(\mathbb{Z}G)(1-f)$ is a subgroup of $\prod_{e \in \mathrm{PCI}(\mathbb{Q}G)_{\geq 2}} \mathrm{SL}_{n_e}(\mathcal{O}_e)$. Furthermore, $U_e \leq \mathcal{E}_G(e)$ as elementary matrices are unipotent. Altogether, as we are both increasing the nominator and decreasing the denominator, this yields the desired inequalities. □

Whether the elementary subgroups $E_n(I)$, for $n \geq 2$, are of finite index in $SL_n(\mathcal{O})$ is related to the celebrated answers on the Subgroup Congruence Problem. In particular, it depends on the so called S-rank of $\mathrm{SL}_n(D)$ where S is the set of Archimedian places of $\mathcal{Z}(D)$. More precisely, if this invariant is at least 2, then $E_n(I)$ will be of finite index in $\mathrm{SL}_n(\mathcal{O})$ [6, 8, 43, 46, 49]. These facts lead to call a finite dimensional simple algebra *exceptional* if it is of one of the following types:

I: a non-commutative division algebra which is not a totally definite quaternion algebra,
II: $\mathrm{M}_2(D)$ with D either $\mathbb{Q}$, an imaginary quadratic extension of $\mathbb{Q}$ or a totally definite quaternion algebra with centre $\mathbb{Q}$.

As recorded in [4, Lemma 6.9], the exceptional simple algebras $\mathrm{M}_n(D)$ with $n \geq 2$ are exactly those for which the S-rank of $\mathrm{SL}_n(D)$ is 1. If $n = 1$, there is no non-trivial unipotent element in $\mathrm{SL}_n(\mathcal{O})$. Thus the terminology 'exceptional' refers to the fact that subgroups generated by unipotent elements in $\mathrm{SL}_n(\mathcal{O})$ are not sufficient to describe $\mathrm{SL}_1(\mathbb{Z}G)$ up to commensurability.

By [14], $\mathbb{Q}G$ has an exceptional component of reduced degree 2 if and only if G maps onto a list of 56 groups. The table in the appendix of [4] demonstrates that $\mathrm{M}_2(\mathbb{Q})$ is the most recurrent exceptional component of that type as for only 19 of the 56 groups no $\mathrm{M}_2(\mathbb{Q})$ is implied. Now suppose that there exists a primitive central idempotent e of $\mathbb{Q}G$ such that $\mathbb{Q}Ge \cong \mathrm{M}_2(\mathbb{Q})$. If $|G|$ is not divisible by 3, then [3, Remark 6.17] tells that $Ge \cong D_8 = \langle a, b \mid a^4 = b^2 = 1, a^b = a^{-1} \rangle$. In other words, in that case, G is an extension of the form

$$1 \to Q \to G \to D_8 \to 1.$$

Thus there exist some $g, h \in G$ such that $ge = a$ and $he = b$. As shown below when Q is big enough, under the following condition G is very far from having ND:

$$(\star) \quad \frac{o(h)}{o(hQ)} \leq 2.$$

THEOREM 4.2. *Let* G *be a finite group. Then the following hold:*

https://doi.org/10.1017/prm.2025.10013 Published online by Cambridge University Press

(i) *If* $\mathbb{Q}G$ *has no exceptional components of type II, then* $\mathrm{q}(\mathrm{G})$ *is finite.*
(ii) *If* G *has order at most* 16*, then* $\mathrm{q}(\mathrm{G})$ *is finite.*
(iii) *If* G *has order bigger than* 16*, maps onto* D_8 *and this surjection satisfies* $(\star)$*, then* $\mathrm{q}(\mathrm{G})$ *is an infinite non-torsion group.*

The above answers both questions of Jespers–Sun formulated in [27, Section 6]. More precisely, Proposition 4.1 and the proof of Theorem 4.2 will show that for nilpotent elements to have an integral decomposition is not truly connected to the simple components of $\mathbb{Q}G$. The relationship is rather a combination of the congruence level of $\mathbb{Z}G$ in the maximal order of $\mathbb{Q}G$ on the one hand and the rank of the simple matrix components of $\mathbb{Q}G$ on the other hand.

The algebra $\mathbb{Q}G$ has a component $\mathrm{M}_2(\mathbb{Q})$ if and only if G maps onto D_8 or S_3 [3, Remark 6.17]. Thus the mapping onto D_8 in Theorem 4.2 is implied, if $\mathbb{Q}G$ has a $\mathrm{M}_2(\mathbb{Q})$ component and $3 \nmid |G|$. The latter restriction appears due to the use of results in [22, Section 10], but we expect it is not needed. As explained in the examples below, some variant of the condition $(\star)$ is however certainly necessary.

Example 4.3.

(1) All the groups in the family

$$G(2,2,n) = \langle a, b \mid 1 = a^4 = b^{2^n}, a^b = a^{-1} \rangle$$

have a matrix component $\mathrm{M}_2(\mathbb{Q})$ since $G(2,2,n)/\langle b^2 \rangle \cong D_8$. The surprising $G(2,2,3)$ has order 32 and satisfies $o(b) = 4o(bQ)$. Furthermore, by Theorem 3.6, it has ND (i.e. $q(G) = 1$). Thus $G(2,2,3)$ is minimal with respect to being in none of the cases described in Theorem 4.2.

(2) Examples of groups satisfying $(\star)$ are split extensions of D_8 or more generally split extension of D_{2^n} with $n \geq 3$. These groups even satisfy $o(h) = o(hQ)$, giving a wide class of examples where $q(G)$ is an infinite (non-torsion) group. However, when $o(h) = 2o(hQ)$, there also exist examples that are not split extension of D_{2^n}, such as $G(2,2,2) = \langle a, b \mid a^4 = b^4 = 1, a^b = a^{-1} \rangle$ or the families of groups with the property that all simple matrix components of $\mathbb{Q}G$ are of the form $\mathrm{M}_2(\mathbb{Q})$. Such groups have been classified in [23] and in case of 2-groups are given by seven possible families (see [22, Section 10.3]), some of which are split extensions of D_8 while others are not. The groups in all these families except the last have exponent 4, so they certainly satisfy $(\star)$. The last series is a split extension of a generalized quaternion group of order 16 and also satisfies $(\star)$.

(3) It follows from [27, Section 5.2] that the SSN groups of unfaithful type defined in definition 2.16 have no exceptional components of type II. Thus by Theorem 4.2 for these groups $q(G)$, the obstruction to ND, is finite. In §5, we will see more fine properties of that class of groups, which all indicate the difficulty to understand those.

https://doi.org/10.1017/prm.2025.10013 Published online by Cambridge University Press

Now denote for a positive integer n by $\Gamma(n)$ the principal congruence subgroup of level n in $\mathrm{SL}_2(\mathbb{Z})$, which is the kernel of the reduction modulo n map. Concretely,

$$\Gamma(n) = \left\{ \begin{pmatrix} 1+nk_{11} & nk_{12} \\ nk_{21} & 1+nk_{22} \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \mid k_{ij} \in \mathbb{Z} \right\}.$$

We will need the following results which seems to be known to experts, but which we could not find explicitly in the literature.

LEMMA 4.4. *Let* u *be a unipotent matrix in* $\mathrm{SL}_2(\mathbb{Z})$. *Then* u *is conjugate inside* $\mathrm{SL}_2(\mathbb{Z})$ *to a matrix of the form* $\begin{pmatrix} 1 & m \\ 0 & 1 \end{pmatrix}$ *with* $m \in \mathbb{Z}$.

Proof. Denote $u-1 = \begin{pmatrix} x & y \\ z & w \end{pmatrix}$ which is by definition a nilpotent matrix. We will prove that $u-1$ is conjugate inside $\mathrm{SL}_2(\mathbb{Z})$ to a matrix of the form $\begin{pmatrix} 0 & m \\ 0 & 0 \end{pmatrix}$ with $m \in \mathbb{Z}$.

To start, by lemma 3.7, $x = -w$ and $x^2 = -yz$. Hence if $z=0$ or $y=0$, then $u-1$ is of the form $\begin{pmatrix} 0 & y \\ 0 & 0 \end{pmatrix}$, respectively $\begin{pmatrix} 0 & 0 \\ z & 0 \end{pmatrix} = S^{-1} \begin{pmatrix} 0 & -z \\ 0 & 0 \end{pmatrix} S$ with $S = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$. Hence we may assume that $y \neq 0$ in which case $u-1 = \begin{pmatrix} x & y \\ \frac{-x^2}{y} & -x \end{pmatrix}$. We will now give the required conjugating matrix explicitly.

Define $\overline{x} = \frac{x}{gcd(x,y)}$ and $\overline{y} = \frac{y}{gcd(x,y)}$. Also take $a, b \in \mathbb{Z}$ such that $a\overline{x} + b\overline{y} = 1$. Now define $S = \begin{pmatrix} \overline{y} & a \\ -\overline{x} & b \end{pmatrix}$. Note that $S^{-1} = \begin{pmatrix} b & -a \\ \overline{x} & \overline{y} \end{pmatrix}$ is in $\mathrm{SL}_2(\mathbb{Z})$. Thus the following claim would finish the proof of the first part of the statement.

Claim: $S^{-1}(u-1)S = \begin{pmatrix} 0 & m \\ 0 & 0 \end{pmatrix}$ for some $m \in \mathbb{Z}$.

It suffices to prove that $\begin{pmatrix} \overline{y} \\ -\overline{x} \end{pmatrix}$ is an eigenvector of $u-1$ with eigenvalue 0 and that $\begin{pmatrix} a \\ b \end{pmatrix}$ is a generalized eigenvector. The former is directly verified using the definition of $\overline{x}$ and $\overline{y}$. For the latter simply note that the columns of $u-1$ are linearly dependent and that the $\mathbb{Q}$-spans of $\begin{pmatrix} \overline{y} \\ -\overline{x} \end{pmatrix}$ and $\begin{pmatrix} y \\ -x \end{pmatrix}$ are equal. In other words, both columns of $u-1$ are eigenvectors and hence every vector is a generalized eigenvector. □

https://doi.org/10.1017/prm.2025.10013 Published online by Cambridge University Press

For a group Γ and a subgroup $H \leq \Gamma$, we will denote by $cl_\Gamma(H)$ the normal closure of H in Γ. This will only be needed in the next lemma and the following proof of Theorem 4.2.

LEMMA 4.5. *Let be* n *a finite index subgroup of* $\Gamma(n)$ *for some* n *where* n *is largest such that* $H \leq \Gamma(n)$. *Then the quotient* $H/\langle B \in H \mid B \text{ is unipotent } \rangle$ *is infinite provided* $n \geq 6$. *In that case, it is a non-torsion group.*

Moreover, if n *is a positive integer smaller than or equal to* 5, *then the subgroup* $cl_{SL_2(\mathbb{Z})}\left(\langle \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} \rangle\right)$ *has finite index in* $\mathrm{SL}_2(\mathbb{Z})$.

Proof. Consider the normal subgroup

$$N = \langle B \in H \mid B \text{ is unipotent } \rangle$$

of H. As $\Gamma(n)$ is a normal subgroup of $\mathrm{SL}_2(\mathbb{Z})$ lemma 4.4 yields that every generator of N is conjugate to an element of the form $\begin{pmatrix} 1 & m \\ 0 & 1 \end{pmatrix}$ with $m \equiv 0 \mod n$. Thus N is a subgroup of $cl_{\mathrm{SL}_2(\mathbb{Z})}\left(\langle \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} \rangle\right)$. Denote the image of this normal closure in $\mathrm{PSL}_2(\mathbb{Z})$ by $K(n)$. It is known, e.g. see [38, Chapter VIII, Section 13], that $\mathrm{PSL}_2(\mathbb{Z})/K(n)$ is isomorphic to the triangle group $\langle x_1, x_2 \mid x_1^2 = x_2^3 = (x_1x_2)^n = 1 \rangle$ with parameters $(2, 3, n)$. Moreover, this group is infinite if and only if $n \geq 6$. This directly yields the last part of the lemma. Furthermore, since $\Gamma(n)$ is of finite index in $\mathrm{SL}_2(\mathbb{Z})$ the quotient $\Gamma(n)/cl_{\mathrm{SL}_2(\mathbb{Z})}\left(\langle \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} \rangle\right)$ is infinite if $n \geq 6$. Subsequently, as H is of finite index in $\Gamma(n)$, the quotient H/N is infinite in that case and the description of the conjugacy classes of torsion elements in $\mathrm{PSL}_2(\mathbb{Z})/K(n)$, see [36, Theorem 2.10], also yields that H/N is non-torsion. □

We can now prove the main result of this section.

Proof of Theorem 4.2. Assume the notation of (39). Take $e \in \mathrm{PCI}(\mathbb{Q}G)_{\geq 2}$ and let $\mathcal{O}_e$ be any maximal order in D_e where $\mathbb{Q}Ge \cong \mathrm{M}_{n_e}(D_e)$. Now consider the subgroup $U_e = 1 - e + E_n(J_e)$ of $\langle \mathcal{U}(\mathbb{Z}G)_{un} \rangle$ given by Proposition 4.1. As mentioned earlier, if $\mathbb{Q}Ge$ is not exceptional, then $E_{n_e}(J_e)$ is a finite index subgroup of $\mathrm{SL}_{n_e}(\mathcal{O}_e)$ (e.g. see [6, 48]). Therefore if $\mathbb{Q}G$ has no exceptional components of type II, then the right most bound in Proposition 4.1 is finite, yielding the first part.

Now suppose that the order of G is bigger than 16, G maps onto D_8 and this surjection satisfies $(\star)$. Then there exists a primitive central idempotent e of $\mathbb{Q}G$ such that $Ge \cong D_8$ and $\mathbb{Q}Ge \cong \mathrm{M}_2(\mathbb{Q})$. Let $\varphi_e : G \to Ge$ and $Q = \ker(\varphi_e)$. Therefore, we can take $g, h \in G$ such that $Ge \cong \langle \varphi_e(g) \rangle \rtimes \langle \varphi_e(h) \rangle$ with $o(gQ) = 4$, $o(hQ) = 2$ and $[gQ, hQ] = (gQ)^2$. Denote $a := \varphi_e(g)$ and $b := \varphi_e(h)$.

One has a ring monomorphism

$$\phi : \mathbb{Z}Ge \to \mathrm{M}_2(\mathbb{Z})$$

https://doi.org/10.1017/prm.2025.10013 Published online by Cambridge University Press

defined by

$$a \mapsto \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad ab \mapsto \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad b \mapsto \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

with image

$$\mathrm{Im}(\phi) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{M}_2(\mathbb{Z}) \mid a \equiv d \text{ and } b \equiv c \bmod 2 \right\}.$$

That the image is the latter can be directly verified and is also recorded in [22, Proposition 8.1]. The triple (gh, h, Q) obtained above satisfies the conditions from [22, Definition 10.5 & Theorem 10.6] and thus one has the associated non-trivial group of H-units $\mathcal{H}(gh, h, Q)$. As $G = \langle gh, h, Q \rangle$, we can use [22, Theorem 10.8], saying that $\mathcal{H}(gh, h, Q) = \mathrm{SL}_1(\mathbb{Z}G) \cap 1 - e + \mathbb{Q}Ge$. In other words, $\mathcal{H}(gh, h, Q)$ is the largest subgroup of $\mathrm{SL}_1(\mathbb{Z}G)$ fully contained in $\mathrm{SL}_2(\mathbb{Z})$ (with contained we mean that the subgroup projects trivially on all the other simple components of $\mathbb{Q}G$). Furthermore, $\mathcal{H}(gh, h, Q) = 1 - e + V_{m_e}$ with $m_e = 2|Q|$ and where

$$V_{m_e} = \left\{ \begin{pmatrix} 1 + m_e\, l_2 & m_e\, t_1 \\ m_e\, t_2 & 1 + m_e\, l_1 \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \mid l_1 \equiv l_2 \text{ and } t_1 \equiv t_2 \bmod 2 \right\}$$

is a subgroup of index 2 in $\Gamma(m_e)$ and V_{m_e} is a normal subgroup of $\mathcal{U}(\mathbb{Z}Ge)$. By lemma 4.5, the subgroup

$$N_e := \langle u \in V_{m_e} \mid u \text{ is unipotent } \rangle \tag{41}$$

is a subgroup of infinite index in V_{m_e} if $m_e \geq 6$. In other words, N_e is of infinite index when $|Q| > 2$. This inequality is satisfied as $16 < |G| = 8|Q|$. Remark that by the above $N_e = \varphi_e(\langle \mathcal{E}_G(e') : e' \in \mathrm{PCI}(\mathbb{Q}G) \rangle)$.

Next we investigate the image of the subgroup $\mathrm{Bic}(G)$ of $\langle \mathcal{U}(\mathbb{Z}G)_{un} \rangle$ which is generated by the bicyclic units, i.e. all elements of the form $1+(1-t)v\widetilde{t}$ or $1+\widetilde{t}v(1-t)$ with $t, v \in G$. Concretely, consider the element $u := 1+\widetilde{h}\, gh(1-h^{-1})$. One directly sees that

$$ue = e + \frac{o(h)}{o(hQ)}(1+b)\, ab(1-b).$$

A direct computation yields that

$$\phi(ue) = \begin{pmatrix} 1 + \frac{2o(h)}{o(hQ)} & -\frac{2o(h)}{o(hQ)} \\ \frac{2o(h)}{o(hQ)} & 1 - \frac{2o(h)}{o(hQ)} \end{pmatrix} \in \Gamma\left(\frac{2o(h)}{o(hQ)}\right).$$

Using the procedure from the proof of lemma 4.4, we find that $S^{-1}\phi(ue)S = \begin{pmatrix} 1 & -\frac{2o(h)}{o(hQ)} \\ 0 & 1 \end{pmatrix}$ with $S = \begin{pmatrix} 1 & -2 \\ 1 & -1 \end{pmatrix}$. However, S is not an element in $\varphi_e(\mathrm{SL}_1(\mathbb{Z}G))$; therefore, we will take normal closures to finish the argument. More precisely, we will make use of the following general group theoretical fact which is easy to prove.

https://doi.org/10.1017/prm.2025.10013 Published online by Cambridge University Press

Claim: Let $K \leq H \leq \Gamma \leq \widehat{\Gamma}$ with K normal in $\widehat{\Gamma}$ and H normal in Γ. If $[H : K]$ and $[\widehat{\Gamma} : \Gamma]$ are finite, then also $[cl_{\widehat{\Gamma}}(H) : K]$ is finite.

We apply this to $K = N_e$ defined in (41) which is a normal subgroup in $\mathcal{H}(gh, h, Q)e = V_{m_e}$. As unipotent matrices stay unipotent under conjugation, it is also normal in $\widehat{\Gamma} = \mathcal{U}(\mathbb{Z}Ge)$. By [22, Proposition 8.2], $\mathcal{U}(\mathbb{Z}Ge)$ has index 3 in $\mathrm{SL}_2(\mathbb{Z})$. We also take $H = \varphi_e(\langle \mathcal{U}(\mathbb{Z}G)_{un} \rangle)$ which is normal in $\Gamma = \mathrm{SL}_1(\mathbb{Z}G)e$. Now, since $\mathbb{Z}G$ is an order contained in the order $\prod_{f \in \mathrm{PCI}(\mathbb{Q}G)_{div}} \mathbb{Z}Gf \times \prod_{e \in \mathrm{PCI}(\mathbb{Q}G)_{\geq 2}} \mathrm{M}_{n_e}(\mathcal{O}_e)$, it follows that the corresponding SL_1 are subgroups of finite index [24, Lemma 4.6.9 & Proposition 5.5.1]. Therefore, $\Gamma = \mathrm{SL}_1(\mathbb{Z}G)e$ is of finite index in $\widehat{\Gamma} = \mathcal{U}(\mathbb{Z}Ge)$. Now suppose that N_e would be of finite index in $\varphi_e(\langle \mathcal{U}(\mathbb{Z}G)_{un} \rangle$. Then by the above claim N_e would also be of finite index in $cl_{\mathcal{U}(\mathbb{Z}Ge)}(\varphi_e(\langle \mathcal{U}(\mathbb{Z}G)_{un} \rangle))$. The latter group contains $cl_{\mathcal{U}(\mathbb{Z}Ge)}(\langle \phi(ue) \rangle))$ which is isomorphic to $cl_{\mathcal{U}(\mathbb{Z}Ge)^S}\left(\langle \begin{pmatrix} 1 & -4 \\ 0 & 1 \end{pmatrix} \rangle\right)$ which is of finite index in $\mathrm{SL}_2(\mathbb{Z})$ by lemma 4.5. Consequently also N_e is of finite index in $\mathrm{SL}_2(\mathbb{Z})$ which, as noticed earlier, is a contradiction since $m_e \geq 6$.

Altogether we have obtained that $[\varphi_e(\langle \mathcal{U}(\mathbb{Z}G)_{un} \rangle) : \varphi_e(\langle \mathcal{E}_G(e') : e' \in \mathrm{PCI}(\mathbb{Q}G) \rangle)]$ is infinite. But would $|q(G)| = [\langle \mathcal{U}(\mathbb{Z}G)_{un} \rangle : \langle \mathcal{E}_G(e') : e' \in \mathrm{PCI}(\mathbb{Q}G) \rangle]$ be finite, then so would be the image under φ_e. Thus indeed $q(G)$ is an infinite group and also non-torsion in view of how we used lemma 4.5.

Finally assume that $|G| \leq 16$. Following [27, Remark 3.12.(ii)] if G has also SN, then it has at most one matrix component and hence has ND. In fact looking at the classification of groups of small order one readily verifies that the only groups of order at most 16 with more than one matrix component are $D_{12}, D_{16}, D_8 \times C_2$, the semidihedral group $D_{16}^- = \langle a, b \mid a^8 = b^2 = 1, a^b = a^3 \rangle$ and

$$G(16,3) := \langle a, b \mid a^4 = b^4 = (ab)^2 = 1, (a^2)^b = a^2 \rangle.$$

The last two groups have SmallGroup ID $[16, 8]$ and $[16, 3]$, respectively. The latter is sometimes given in the literature with the presentation $\langle a, b, c \mid a^2 = b^2 = c^4 = [a, b] = [b, c] = 1, c^a = bc \rangle$.

In case of $D_8 \times C_2$ and $G(16, 3)$, the simple matrix components are of the form $\mathrm{M}_2(\mathbb{Q})$. For D_{16}, there is also a non-exceptional component of the form $\mathrm{M}_2(\mathbb{Q}(\sqrt{2}))$. As explained earlier, for each of their components $\mathrm{M}_2(\mathbb{Q})$, there exists a primitive central idempotent e and a triple (g, h, Q) such that $\mathcal{H}(g, h, Q)e = V_{2|Q|}$ is a subgroup of finite index in $\mathrm{SL}_1(\mathbb{Z}Ge) \leq \mathrm{SL}_2(\mathbb{Z})$. Since these groups have order 16 one has that $\mathcal{H}(g, h, Q)e = V_4$. For the component $\mathrm{M}_2(\mathbb{Q}(\sqrt{2}))$, we apply Proposition 4.1 to find a subgroup U_e in $\mathcal{E}_G(e)$ of the form $E_2(J_e)$ with J_e a non-zero ideal in the ring of integers of $\mathbb{Q}(\sqrt{2})$. As $\mathrm{M}_2(\mathbb{Q}(\sqrt{2}))$ is not exceptional, $E_2(J_e)$ is of finite index in $\mathrm{SL}_1(\mathbb{Z}Ge)$. Summarized, in all these cases, we find in $\langle \mathcal{E}_G(e) \mid e \in \mathrm{PCI}(\mathbb{Q}G) \rangle$ a subgroup which is of finite index in $\prod_{e \in \mathrm{PCI}(\mathbb{Q}G)_{\geq 2}} \mathrm{SL}_{n_e}(\mathcal{O}_e)$ and hence also in $\langle \mathcal{U}(\mathbb{Z}G)_{un} \rangle$, as desired.

For the groups D_{12} and D_{16}^- such a subgroup in $\langle \mathcal{E}_G(e) \mid e \in \mathrm{PCI}(\mathbb{Q}G) \rangle$ can also be constructed. In case of D_{12}, the matrix components are of the form $\mathrm{M}_2(\mathbb{Q})$ and the required subgroups are constructed in the proof of [25, Theorem 2]. In the case of D_{16}^-, the matrix components are both exceptional, namely $\mathrm{M}_2(\mathbb{Q})$ and $\mathrm{M}_2(\mathbb{Q}(\sqrt{-2}))$. For the $\mathrm{M}_2(\mathbb{Q})$ component, one can use the same argument as for

https://doi.org/10.1017/prm.2025.10013 Published online by Cambridge University Press

the other groups of order 16 and for $\mathrm{M}_2(\mathbb{Q}(\sqrt{-2}))$ the necessary subgroup is the matrix group from [26, Theorem 2]. □

Remark 4.6.

(1) In [27, Section 6], it was stated that $q(G)$ is always torsion. The explanation given there, however, only yields that for every element $u \in \mathcal{U}(\mathbb{Z}G)_{un}$ there exists an integer m such that $u^m \in \prod_{e \in \mathrm{PCI}(\mathbb{Q}G)} \mathcal{E}_G(e)$. As shown in Theorem 4.2, in general, $q(G)$ is not torsion.
(2) One could also consider RG for R an order in some number field F. Then $\mathcal{U}(FG) \cong \prod_{i=1}^{q} \mathrm{GL}_{n_i}(D_i)$ for some finite dimensional division algebras over F. Completely analogously one could define a quotient group as (40), say $q(\mathcal{U}(RG))$. Proposition 4.1, in fact, also holds in this generality and the first part of Theorem 4.2 also. From the description of exceptional components of type II, we see that if F is not $\mathbb{Q}$ or an imaginary quadratic extension of $\mathbb{Q}$, then FG has no such exceptional components and hence $q(\mathcal{U}(RG))$ is finite. This conclusion, for example, holds if R contains a primitive mth root of unity with m not a divisor of 4 or 6.

4.2. A brief look at general semisimple algebraic groups

To finish this section, we would like to briefly point out that the group $q(G)$ can also be introduced for arithmetic subgroups of more general semisimple algebraic groups than $\mathcal{U}(\mathbb{Q}G)$.

Let F be a number field and S a non-empty finite set of places of F containing the Archimedean places. Associated is the ring of S-integers $\mathcal{O}_S = \{x \in F \mid |x|_v \leq 1 \text{for all } v \notin S\}$. Now consider a linear algebraic F-group $\mathbf{G}$ and fix an F-embedding $\mathbf{G} \hookrightarrow GL_n(F)$. Using this the group of S-integral points is defined as $\mathbf{G}(\mathcal{O}_S) := \mathbf{G}(F) \cap GL_n(\mathcal{O}_S)$. A subgroup of $\mathbf{G}(F)$ commensurable with $\mathbf{G}(\mathcal{O}_S)$ is called an S-arithmetic subgroup

Suppose now that $\mathbf{G}$ is a semisimple algebraic group which we also assume to be simply connected. In that case $\mathbf{G}$ is a direct product of simply connected almost-simple algebraic F-subgroups [41, Theorem 2.6], say $\mathbf{G} = \prod_{i=1}^{m} \mathbf{G}_i$. Let Γ be an S-arithmetic subgroup of $\mathbf{G}(F)$. Analogously as in the case of $\mathcal{U}(\mathbb{Z}G)$, denote by Γ^+ the group generated by the F-rational unipotent elements lying in Γ and by $\mathcal{E}_\Gamma(i)$ the subgroup generated by those unipotents projecting only non-trivially in $\mathbf{G}_i(F)$. Then one can define

$$q(\Gamma) = \Gamma^+ / \prod_{i=1}^{q} \mathcal{E}_\Gamma(i).$$

Again this group measures to what extend the unipotents of Γ have a decomposition in unipotents over $\mathcal{O}_S$. As in the case of $\mathcal{U}(\mathbb{Z}G)$, the size of $q(\Gamma)$ can be bounded using elementary subgroups of $\mathcal{E}_\Gamma(i)$. In this generality, for an ideal J of $\mathcal{O}_S$, a principal congruence subgroup is a group of the form $\mathbf{G}(J) := \mathbf{G}(F) \cap \mathrm{SL}_n(J)$. If U_i^+ is the unipotent radical of a minimal parabolic F-subgroup of $\mathbf{G}_i(F)$ and U_i^- the unipotent radical of an opposed (i.e. $U_i^+ \cap U_i^- = \{1\}$) minimal parabolic subgroup,

https://doi.org/10.1017/prm.2025.10013 Published online by Cambridge University Press

then the elementary subgroup $E(J_i)$ is the group generated by $U_i^+ \cap \mathbf{G}_i(J)$ and $U_i^- \cap \mathbf{G}_i(J)$.

The known solutions to the Subgroup Congruence Problem [42, 50] again yield that each $\mathcal{E}_\Gamma(i)$ contains some $E(J_i)$ which is of finite index, if S-rank$(\mathbf{G}_i(F)) = \sum_{v\in S} \text{rank}_{F_v}(\mathbf{G}_i(F))$ is at least 2. Here F_v is a local field, the completion of F at v, and $\text{rank}_{F_v}(\mathbf{G}_i(F))$ the dimension of a largest split F_v-torus. Finally recall that by a theorem of Borel-Tits [11] $\mathbf{G}_i(F)$ contains non-trivial unipotent elements if and only if F-rank$(\mathbf{G}_i(F)) \geq 1$. In that case $\mathbf{G}_i(F)$ is called anisotropic. Thus with an analogue reasoning one can obtain the following variant of Proposition 4.1:

PROPOSITION 4.7. *Consider the notations above and suppose S-rank$(\mathbf{G}_i(F)) \geq 2$ for all anisotropic $\mathbf{G}_i(F)$. Then,*

$$|q(\Gamma)| < \infty.$$

In particular, in this case, finiteness of $q(\Gamma)$ does not depend on the chosen S*-arithmetic subgroup Γ.*

It would be interesting to know for which other types of algebraic groups and arithmetic subgroups, the triviality and finiteness of $q(\Gamma)$ is of significance. In particular, recall that Γ is a lattice in the Lie group $\mathbf{G}(\mathbb{R})$ and the following seems relevant to obtain for example a variant of Theorem 4.2.

QUESTION 4.8. Does the group $q(\Gamma)$ or its cardinality have a topological interpretation?

5. Further related properties: nilpotent decomposition, different kernels, and bicyclic resistance

In this final section, we introduce and study two further properties which naturally appeared in our research on the ND property. The first is a property, having different kernels, which turns out to hold for all groups with one matrix component but behaves better from a structural perspective. The second property, being bicyclic resistant, can be regarded as a partial ND property. We find that for groups with SN these two new properties are equivalent which also explains some of the hardships we had to endure in the previous sections. We then finish the article by some remarks on the connection of bicyclic resistance with the Zassenhaus conjectures, remark 5.22, as well as in §5.3 with observations on the Multiplicative Jordan Decomposition and a final question which remains open.

5.1. Property of having different kernels

In this section, we consider a property which turns out to be satisfied by all groups having at most one matrix component, but which is also a natural property by itself in the context of representation theory over $\mathbb{Q}$. To introduce this property, let

https://doi.org/10.1017/prm.2025.10013 Published online by Cambridge University Press

$e \in \mathbb{Q}G$ be a central idempotent. Recall that in (5) we defined the homomorphism

$$\varphi_e : G \to Ge, \quad g \mapsto ge.$$

If e is the primitive central idempotent corresponding to a given irreducible $\mathbb{Q}$-representation of G, then $\ker(\varphi_e)$ equals the kernel of that representation.

DEFINITION 5.1. *A finite group* G *is said to have the* Different Kernel property, DK *in short, if for every orthogonal pair* $e, f \in \mathrm{PCI}(\mathbb{Q}G)$ *one has* $\ker(\varphi_e) \neq \ker(\varphi_f)$. *In other words, any two non-equivalent irreducible* $\mathbb{Q}$*-representations of* G *have different kernels.*

As we will see in §5.2, property DK is connected to property ND but behaves better from a structural perspective. We remark that in principle one can define the DK property also over bigger fields than $\mathbb{Q}$. We do not go further in this direction, but note that the classes of groups one considers will be directly restricted by this. For example, the cyclic group of order 3 has DK but does not have the corresponding property over a field containing a primitive 3rd root of unity.

One of our main motivations to introduce this property in the context of this article is the following result.

THEOREM 5.2. *Let* G *be a finite group such that* $\mathbb{Q}G$ *has at most one matrix component. Then* G *has DK.*

Before proving this, we make some other interesting observations. We first reformulate DK as a condition on the set of primitive central idempotents.

PROPOSITION 5.3. *Let* G *be a finite group. Then* G *has DK if and only if* $\mathrm{PCI}(\mathbb{Q}G) \subseteq \{\epsilon(G, N) \mid N \trianglelefteq G\}$. *In that case* $\mathrm{PCI}(\mathbb{Q}G) = \{\epsilon(G, \ker(\varphi_e)) \mid e \in \mathrm{PCI}(\mathbb{Q}G)\}$.

Proof. Given a normal subgroup N of G we define the set $\mathcal{I}(N) = \{e \in \mathrm{PCI}(\mathbb{Q}G) \mid N \subseteq \ker(\varphi_e)\}$ which corresponds to the irreducible $\mathbb{Q}$-representations containing N in their kernel. Note that $\mathbb{Q}G\widehat{N} = \bigoplus_{e \in \mathcal{I}(N)} \mathbb{Q}Ge$ and hence $\mathbb{Q}G(1 - \widehat{N}) = \bigoplus_{e \in \mathrm{PCI}(\mathbb{Q}G) \setminus \mathcal{I}(N)} \mathbb{Q}Ge$. Therefore, using the most right form of $\epsilon(G, N)$ in (3), we see that by construction $\epsilon(G, N)$ is the central idempotent which corresponds to exactly those irreducible $\mathbb{Q}$-representations which have kernel equal to N. Thus $\epsilon(G, N)$ is not primitive, say $e, f \in \mathrm{PCI}(\mathbb{Q}G)$ are orthogonal summands of $\epsilon(G, N)$, if and only if $N = \ker(\varphi_e) = \ker(\varphi_f)$, i.e. if and only if G does not have DK. □

A direct consequence together with [24, Corollary 3.3.3] is:

COROLLARY 5.4. *Abelian groups have DK.*

This also gives:

LEMMA 5.5. *Let* $e, f \in \mathrm{PCI}(\mathbb{Q}G)$ *such that* $\mathbb{Q}Ge$ *and* $\mathbb{Q}Gf$ *are commutative. Then* $\ker(\varphi_e) = \ker(\varphi_f)$ *if and only if* $\mathrm{e} = \mathrm{f}$. *Consequently, if there is a unique* $e \in \mathrm{PCI}(\mathbb{Q}G)$ *such that* $\mathbb{Q}Ge$ *is not commutative, then* G *has DK.*

https://doi.org/10.1017/prm.2025.10013 Published online by Cambridge University Press

Proof. If $e \neq f$ but $\ker(\varphi_e) = \ker(\varphi_f)$, then the group G/G' would not have DK, contradicting corollary 5.4.

Next assume that e is the unique idempotent with $\mathbb{Q}Ge$ not commutative. In other words, $G' \not\subseteq \ker(\varphi_e)$ but $G' \subseteq \ker(\varphi_f)$ for every other $f \in \mathrm{PCI}(\mathbb{Q}G)$. Moreover, the first part tells that the primitive central idempotents different from e have also different kernels, hence altogether G has DK. □

Example 5.6. Q_8, D_8, and A_4 all have DK. Indeed this follows directly from the preceding lemma as

$$\mathbb{Q}Q_8 \cong 4\mathbb{Q} \oplus \mathbb{H}_{\mathbb{Q}}, \quad \mathbb{Q}D_8 \cong 4\mathbb{Q} \oplus M_2(\mathbb{Q}), \quad \mathbb{Q}A_4 \cong \mathbb{Q} \oplus \mathbb{Q}(\zeta) \oplus M_3(\mathbb{Q}),$$

where $\mathbb{H}_{\mathbb{Q}}$ denotes the rational quaternions and ζ a primitive 3rd root of unity.

Example 5.7. The two smallest groups not to have DK are the symmetric group S_4 and $\mathrm{SL}(2,3)$. This is clear for S_4: the natural permutation representation from which the trivial submodule has been cancelled is an integral irreducible representation. But so is its twist by the sign representation $S_4 \to \{\pm 1\}$.

Setting $G = \mathrm{SL}(2,3) \cong Q_8 \rtimes C_3$, one has

$$\mathbb{Q}G \cong \mathbb{Q}A_4 \oplus \mathbb{H}_{\mathbb{Q}} \oplus M_2(\mathbb{Q}(\zeta)) \cong \mathbb{Q}C_3 \oplus M_3(\mathbb{Q}) \oplus \mathbb{H}_{\mathbb{Q}} \oplus M_2(\mathbb{Q}(\zeta)),$$

where $\mathbb{H}_{\mathbb{Q}}$ denotes the rational quaternions and ζ a primitive third root of unity. The representations of G corresponding to $\mathbb{H}_{\mathbb{Q}}$ and $M_2(\mathbb{Q}(\zeta))$ are both faithful, i.e. have trivial kernel.

It might be tempting to attempt a proof of Theorem 5.2 by assuming G does not have DK and taking orthogonal $e, f \in \mathrm{PCI}(\mathbb{Q}G)$ such that $\ker(\varphi_e) = \ker(\varphi_f)$ and such that $\mathbb{Q}Ge$ and $\mathbb{Q}Gf$ are both matrix components. However, example 5.7 shows that this cannot be assumed in general. Hence we have to follow another strategy.

Proposition 5.8. *Let $N \trianglelefteq G$ and* H *be a finite groups. Then the following hold.*

(1) *If* G *has DK, then G/N has DK.*
(2) *If* G *and* H *have DK and the orders of* G *and* H *are coprime, then* G × H *has DK.*

Proof. Every irreducible $\mathbb{Q}$-representation of G/N is also an irreducible $\mathbb{Q}$-representation of G, so the first item follows.

For the second claim recall that $\mathbb{Q}[G \times H] \cong \mathbb{Q}G \otimes \mathbb{Q}H$. If $e \in \mathrm{PCI}(\mathbb{Q}G)$ and $f \in \mathrm{PCI}(\mathbb{Q}H)$ then $e \otimes f$ is a central idempotent in $\mathbb{Q}[G \times H]$. If $e' \in \mathrm{PCI}(\mathbb{Q}G)$ such that $ee' = 0$, then $(e \otimes f)(e' \otimes f) = 0$, so different central idempotents obtained in this way are orthogonal. We claim that all these idempotents are in fact central primitive. Indeed the number of primitive central idempotents in $\mathbb{Q}(G \times H)$ is the same as the number of conjugacy classes of cyclic subgroups in $G \times H$ by [24, Corollary 7.1.12]. As the orders of G and H are coprime, this is the same as the

https://doi.org/10.1017/prm.2025.10013 Published online by Cambridge University Press

product of the numbers of conjugacy classes of cyclic subgroups of G and H, so we have

$$|\operatorname{PCI}(\mathbb{Q}[G\times H])| = |\operatorname{PCI}(\mathbb{Q}G)|\cdot|\operatorname{PCI}(\mathbb{Q}H)|. \tag{42}$$

As we saw above every primitive summand of $e\otimes f$ is orthogonal with every primitive summand of $e'\otimes f$. So if $e\otimes f$ would not be primitive, this would contradict (42).

It remains to show that $\ker(\varphi_{e\otimes f}) \neq \ker(\varphi_{e'\otimes f})$ which will follows from the assumptions by showing $\ker(\varphi_{e\otimes f}) = \ker(\varphi_e)\times\ker(\varphi_f) \leq G\times H$. For this recall that the representation corresponding to $e\otimes f$ can be obtained as the Kronecker product between the representations corresponding to e and f. Denote by I the identity matrix (abusing notation it will have varying size). Now if $A\otimes B = I$ for A and B matrices of finite order, then A and B must be diagonal and $dB = I$ for any element d on the diagonal of A. But if A is a matrix coming from a representation of G and B a matrix coming from a representation of H, then the orders of A and B are coprime. So $dB = I$ implies $d = 1$ and $B = I$, in total $A = I$ and $B = I$. □

Example 5.9. We show that property DK is not closed under taking direct products when the orders of the factors are not assumed to be of coprime order and that (42) is also not correct in general. For this let $G = D_{10}\times C_5$. If $G' = \langle a\rangle$ and b is a central element of order 5, then from lemma 2.5 we deduce that $(\langle a,b\rangle, \langle ab\rangle)$ and $(\langle a,b\rangle, \langle a^2b\rangle)$ are strong Shoda pairs which correspond to non-equivalent faithful $\mathbb{Q}$-representations.

Example 5.10. We show that property DK is not closed under taking subgroups. First consider the following group which has GroupId [32,11] in the SmallGroupLibrary[10]:

$$H = \langle a,b,c \mid a^4 = b^4 = c^2 = 1, [a,b] = [b,c] = 1, [a,c] = a^2b\rangle \cong (C_4\times C_4)\rtimes C_2.$$

Using lemma 2.5, we see that in H the strong Shoda Pairs $(\langle a,b\rangle, \langle a\rangle)$ and $(\langle a,b\rangle, \langle ab\rangle)$ provide two different elements in $\operatorname{PCI}(\mathbb{Q}H)$ such that both corresponding representations are faithful, i.e. H does not have DK.

Now consider the group

$$\begin{aligned} G = \langle a,b,c,d \mid a^4 = b^4 = c^2 = d^2 = [a,b] = [b,c] = 1, [a,c] = a^2b,\\ [a,d] = a^2b^2, [b,d] = b^2, [c,d] = a^2b^{-1}\rangle\\ \cong ((C_4\times C_4)\rtimes C_2)\rtimes C_2 \cong H\rtimes C_2 \end{aligned}$$

which has GroupId [64, 135]. As this group is metabelian, we can apply lemma 2.5 with $A = \langle a,b\rangle$. We list the strong Shoda pairs which provide all the non-commutative components of $\mathbb{Q}G$ one obtains in this way without further details. Note that $G' = \langle a^2, b\rangle$:

https://doi.org/10.1017/prm.2025.10013 Published online by Cambridge University Press

$$(\langle A, c\rangle, \langle a^2b, c\rangle),\ (\langle A, c\rangle, \langle a^2b, a^2c\rangle),\ (\langle A, d\rangle, \langle a, b^2, d\rangle), (\langle A, d\rangle, \langle ab, b^2, d\rangle),$$
$$(\langle A, cd\rangle, \langle b, cd\rangle),\ (\langle A, cd\rangle, \langle b, a^2cd\rangle),\ (\langle A, d\rangle, \langle a\rangle).$$

We compute the kernels of the corresponding representations by Theorem 3.3. These are $\langle a^2b, c\rangle$, $\langle a^2b, a^2c\rangle$, $\langle ad, a^2\rangle$, $\langle abd, a^2\rangle$, $\langle b, cd\rangle$, $\langle b, a^2cd\rangle$, and 1, respectively. Hence all kernels are different and G has DK.

LEMMA 5.11. *Let* m *be an integer,* q *a prime not dividing* m *and* $G = C_m \rtimes Q$ *a non-trivial semi-direct product where* Q *is a* q*-group which is either abelian or generalized quaternion. Let* $a \in G$ *be of order* m. *In case* Q *is generalized quaternion, assume that a maximal cyclic subgroup of* Q *acts trivially on* $\langle a\rangle$. *Moreover, if* $[a, g] \neq 1$ *for some* $g \in Q$, *then* $[\langle a\rangle, \langle g\rangle] = \langle a\rangle$ *holds. Then* G *has DK.*

Proof. G is metabelian and hence we can apply lemma 2.5 looking for strong Shoda pairs (H, K) in G. By lemma 5.5, we can restrict our attention to those satisfying $G' \not\subseteq K$ and we will further assume this condition. Let A be a maximal abelian subgroup of G containing G'. As $[A, \langle g\rangle] = G'$ for every $g \notin A$, we get $A = H$. When Q is generalized quaternion we can write $A = \langle a\rangle \times \langle b\rangle$, where $\langle b\rangle$ is a maximal cyclic subgroup of Q. If Q is abelian we have $A = \langle a\rangle \times (\mathcal{Z}(G) \cap Q)$. In any case, the condition that q does not divide m implies that every subgroup of A is normal in G. Hence when (A, K) is a strong Shoda pair and $e = e(G, A, K)$, we have $\ker(\varphi_e) = K$ by Theorem 3.3. In particular, each irreducible $\mathbb{Q}$-representation of G is uniquely determined by its kernel and G has DK. □

With this we can show DK for some interesting classes of groups.

COROLLARY 5.12. *Let* G *be an SSN group of unfaithful type. Then* G *has DK.*

PROPOSITION 5.13. *Let* G *be a finite subgroup of the multiplicative group of a division algebra in characteristic* 0. *Then* G *has DK if and only if it is not isomorphic to one of the following:*

(1) *the binary octahedral group,*
(2) $\mathrm{SL}(2, 5)$,
(3) $\mathrm{SL}(2, 3) \times H$ *for* H *a group of order coprime to* 6.

Proof. The finite subgroups of division algebras in characteristic 0 were obtained by Amitsur, we refer to [44, Theorems 2.1.4 and 2.1.5] for a full account. It follows that when G is not one of the three possibilities listed explicitly in the statement, then G is the direct product of groups of coprime orders such that each factor has the shape given in lemma 5.11. So by lemma 5.11 and Proposition 5.8, we conclude that G has DK. It remains to show that this is not the case for the three cases listed.

If G is the binary octahedral group, then $G/\mathcal{Z}(G) \cong S_4$, so that G does not have DK by Proposition 5.8 and example 5.7. Similarly, if $G \cong \mathrm{SL}(2, 3) \times H$, then G maps onto $\mathrm{SL}(2, 3)$, so we can again use Proposition 5.8 and example 5.7. For

https://doi.org/10.1017/prm.2025.10013 Published online by Cambridge University Press

$G = \mathrm{SL}(2,5)$, we observe that G maps onto a non-abelian simple group, namely A_5. But a non-abelian simple group can never have DK, indeed otherwise $\mathbb{Q}G$ would only have two components, but G has certainly more than two conjugacy classes of cyclic subgroups, which would contradict [24, Corollary 7.1.12]. □

Proof of Theorem 5.2. To start we reduce the statement to the case that G embeds in a division algebra of finite dimension over $\mathbb{Q}$. Let G be a group of minimal order violating the conditions, i.e. G is a group with at most one matrix component, but there exist orthogonal $e, f \in \mathrm{PCI}(\mathbb{Q}G)$ such that $\ker(\varphi_e) = \ker(\varphi_f)$. Set $N = \ker(\varphi_e)$. Then G/N is also a group with at most one matrix component, which does not have DK, namely it has two non-equivalent faithful representations. By the minimality of G we conclude that $N = 1$. By lemma 5.5, we know that neither $\mathbb{Q}Ge$ nor $\mathbb{Q}Gf$ is a field. On the other hand at most one of them, say $\mathbb{Q}Ge$, can be a matrix-component. Hence $\mathbb{Q}Gf$ is a non-commutative division algebra D and as $\ker(\varphi_f) = 1$, it follows that G is isomorphic to a multiplicative subgroup of D.

So we assume that G is a subgroup of a division algebra of characteristic 0. By Proposition 5.13, many of those groups have DK independently from the property of having one matrix component and we will be done once we see that the three exceptions listed in the proposition do not have one matrix component. By example 5.7, this is true for $\mathrm{SL}(2,3)$ and also S_4, which is the image of the binary octahedral group. Also $\mathbb{Q}\,\mathrm{SL}(2,5)$ contains a direct summand isomorphic to $\mathbb{Q}A_5$, which has more than one matrix component. □

We next show that another class of groups of interest in this article has DK.

LEMMA 5.14. *Let* G *be a nilpotent group with SSN. Then* G *has DK.*

Proof. Assume first that G is a Dedekind group. As abelian groups have DK by corollary 5.4 and Q_8 has DK by example 5.6, the property DK for G follows from Proposition 5.8.

So we can assume that G is one of the nine classes (BJ1)–(BJ9) listed in [27, Theorem 4.1]. The groups in (BJ3) are a direct product of a quaternion group of order 8 and a cyclic group of odd order, so they have DK by the same argument as Dedekind groups. The groups (BJ2), (BJ6), (BJ7) have one matrix component by [27, Lemma 4.5 & p. 11], so they have DK by Theorem 5.2. It remains to study the groups in (BJ1), (BJ4), (BJ5), (BJ8), and (BJ9). All those groups are metabelian and so we can apply lemma 2.5 to show that they have DK and by lemma 5.5 we can consider only strong Shoda pairs (H, K) such that K does not contain the commutator subgroup. For all groups, we will list a full set of non-equivalent strong Shoda pairs based on lemma 2.5 and the kernels of the corresponding representations which follow from Theorem 3.3. It will follow that kernels are pairwise different and the groups have DK.

(BJ4) We have, cf. [27, p. 120],

$$G = \langle a, b, c \mid a^9 = b^3 = [a,b] = 1, a^c = ab, b^c = a^{-3}b, c^3 = a^3 \rangle,$$

so $G' = \langle a^3, b \rangle$. We let $A = \langle a, b \rangle \cong C_9 \times C_3$ be a maximal abelian subgroup containing G'. As A is a maximal subgroup of G, we have

https://doi.org/10.1017/prm.2025.10013 Published online by Cambridge University Press

$H = A$. The conjugacy classes of subgroups of A which have cyclic quotients and do not contain G', i.e. which can play the role of K in the strong Shoda pair (H, K), are $\{\langle b\rangle, \langle a^{-3}b\rangle, \langle a^3b\rangle\}$ and $\{\langle a\rangle, \langle ab\rangle, \langle a^{-1}b\rangle\}$. The corresponding kernels of the representations, i.e. $\mathrm{core}_G(K)$, are $\langle a^3\rangle$ and 1, respectively.

(BJ5) We have

$$G = \langle a, b \mid a^8 = 1, a^b = a^{-1}, a^4 = b^4\rangle,$$

so $G' = \langle a^2\rangle$. Let $A = \langle a, b^2\rangle \cong C_8 \times C_2$. As A is a maximal subgroup of G, we have $H = A$. The conjugacy classes of subgroups of A which have cyclic quotients and do not contain G' are $\{\langle a^2b^2\rangle, \langle a^{-2}b^2\rangle\}$ and $\{\langle a^4b^2\rangle\}$. The corresponding kernels of the representations are 1 and $\langle b^2\rangle$, respectively.

(BJ8) We have

$$G = \langle a, b, c \mid a^4 = b^4 = [a, b] = 1, a^c = ab^2, b^c = ba^2, c^2 = a^2\rangle,$$

so $G' = \langle a^2, b^2\rangle$. Let $A = \langle a, b\rangle \cong C_4 \times C_4$. As A is a maximal subgroup of G, we have $H = A$. The conjugacy classes of subgroups of A which have cyclic quotients and do not contain G' are $\{\langle a\rangle, \langle ab^2\rangle\}$, $\{\langle b\rangle, \langle ba^2\rangle\}$, $\{\langle ab\rangle\}$, and $\{\langle a^{-1}b\rangle\}$. The corresponding kernels of the representations are $\langle a^2\rangle$, $\langle b^2\rangle$, $\langle ab\rangle$, and $\langle a^{-1}b\rangle$, respectively.

(BJ9) We have

$$G = \langle a, b, c, d \mid a^4 = b^4 = [a, b] = 1, a^c = a^{-1}, b^c = b^{-1}a^2,$$
$$a^d = a^{-1}b^2, b^d = b^{-1}, c^2 = a^2b^2, d^2 = a^2\rangle,$$

so $G' = \langle a^2, b^2\rangle$. Let $A = \langle a, b\rangle \cong C_4 \times C_4$. In this case, A is a not a maximal subgroup of G, but as all the proper subgroups containing it, namely $\langle A, c\rangle$, $\langle A, d\rangle$, and $\langle A, cd\rangle$, have derived subgroup G', we still have $H = A$. The conjugacy classes of subgroups of A which have cyclic quotients and do not contain G' are $\{\langle a\rangle, \langle ab^2\rangle\}$, $\{\langle b\rangle, \langle ba^2\rangle\}$, and $\{\langle ab\rangle, \langle a^{-1}b\rangle\}$. The corresponding kernels of the representations are $\langle a^2\rangle$, $\langle b^2\rangle$, and $\langle a^2b^2\rangle$, respectively.

(BJ1) We have for p a prime, $m \geq 2$ and $n \geq 1$

$$G = \langle a, b \mid a^{p^m} = b^{p^n} = 1, a^b = a^{1+p^{m-1}}\rangle,$$

so $G' = \langle a^{p^{m-1}}\rangle$. Let $A = \langle a, b^p\rangle \cong C_{p^m} \times C_{p^{n-1}}$. As A is a maximal subgroup of G, we have $H = A$. The subgroups of A which have cyclic quotients are $K = \langle a^jb^p\rangle$ for some integer j such that the order of a^j is at most p^{n-1}. If p divides j, then $a^jb^p \in \mathcal{Z}(G)$ and K is itself the kernel of the corresponding representation. If p does not divide j, then the kernel is $\langle a^{jp}b^{p^2}\rangle$. If k is also a number not divisible by p such that $\langle a^{jp}b^{p^2}\rangle = \langle a^{kp}b^{p^2}\rangle$, then $j \equiv k \bmod p^{m-1}$ so that a^jb^p is conjugate to a^kb^p and hence the corresponding K give equivalent strong Shoda pairs.

□

https://doi.org/10.1017/prm.2025.10013 Published online by Cambridge University Press

5.2. Nilpotent decomposition with specific idempotents or nilpotents

The proof of Theorem 3.15 works by constructing a particular type of nilpotent element $n \in \mathbb{Z}G$, which we will call bicyclic nilpotent, and a central idempotent $e \in \mathbb{Q}G$ such that $ne \notin \mathbb{Z}G$ if and only if G has more than one matrix component. We formalize this in the following way.

DEFINITION 5.15. *For elements $g, h \in G$ and* H *a subgroup of* G *containing* h *we call $(1-h)g\widetilde{H}$ and $\widetilde{H}g(1-h)$ a* bicyclic nilpotent *element.*

We call G bicyclic resistant*, if for every bicyclic nilpotent element $n \in \mathbb{Z}G$ and every central idempotent $e \in \mathbb{Q}G$ one has $ne \in \mathbb{Z}G$.*

Interestingly, a group having SN will have DK exactly when all the bicyclic nilpotent elements have a nilpotent decomposition. More precisely, in the remainder of the section, we will work towards proving the following result.

THEOREM 5.16. *Let* G *be a finite group with SN. Then the following are equivalent:*

(1) G *is bicyclic resistant.*
(2) G *is supersolvable or $\mathbb{Q}G$ has one matrix component.*
(3) G *has DK.*

The methods of the proof of Theorem 3.15 in fact suggest that it might be interesting to study analogues of the property ND only considering certain nilpotent elements and certain central idempotents.

DEFINITION 5.17. *Let* E *be a set of central idempotents in $\mathbb{Q}G$ and $n \in \mathbb{Z}G$ a nilpotent element. We say that* n has ND with respect to E*, if $ne \in \mathbb{Z}G$ holds for every $e \in E$.*

With this terminology at hand, we can give a new characterization of property SN in terms of such kind of local ND. This characterization implies that bicyclic resistant groups have SN.

PROPOSITION 5.18. *Let* G *be a finite group. The following are equivalent:*

(1) G *has SN.*
(2) *All bicyclic nilpotent elements have ND with respect to $\{\epsilon(G,N) \mid N \trianglelefteq G\}$.*
(3) *All bicyclic nilpotent elements have ND with respect to $\{\widehat{N} \mid N \trianglelefteq G\}$.*

Proof. Let $Y \leq G$, $x \in G$, $y \in Y$ and denote $n = (1-y)x\widetilde{Y}$. Remark that $n\widehat{N} = (1-y).x.\widetilde{\langle N, Y\rangle}.\frac{|Y\cap N|}{|N|}$. This implies that one can choose N such that $0 \neq n\widehat{N}$ exactly when YN is not normal, i.e. there exists a non-trivial $x \notin N_G(YN)$. Moreover, when $0 \neq n\widehat{N}$, it is in $\mathbb{Z}G$ exactly when $|Y \cap N| = |N|$. In other words, when $N \leq Y$. These two observations combined imply the equivalence between (1) and (3).

https://doi.org/10.1017/prm.2025.10013 Published online by Cambridge University Press

To see that (2) and (3) are equivalent note first that

$$n\epsilon(G,N) = n\widehat{N} \prod_{M/N \in \mathcal{M}(G/N)} (1 - \widehat{M}) = \sum_{M \trianglelefteq G} a_M n \widehat{M}$$

for certain integers a_M. If (3) holds, then $n\widehat{M} \in \mathbb{Z}G$ for every $M \trianglelefteq G$ and consequently (2) holds. To see that (2) implies (3) we argue by induction on the minimal length of a chain of normal subgroups from N to G. For the induction start notice $n\epsilon(G,G) = n\widehat{G}$. Now let $N \trianglelefteq G$. Then

$$n\epsilon(G,N) = n\widehat{N} \prod_{M/N \in \mathcal{M}(G/N)} (1 - \widehat{M}) = n\widehat{N} + \sum_{N \lneq M \trianglelefteq G} a_M n \widehat{M},$$

for certain integers a_M, is an element of $\mathbb{Z}G$. As $\sum_{N \lneq M \trianglelefteq G} a_M n\widehat{M} \in \mathbb{Z}G$ by induction, we conclude $n\widehat{N} \in \mathbb{Z}G$. □

Proposition 5.18 combined with Proposition 5.3 now yield the following.

Corollary 5.19. *Let* G *be a finite group with DK. Then* G *has SN if and only if it is bicyclic resistant.*

We show that some other classes of interest are also bicyclic resistant using the following lemma.

Lemma 5.20. *Let* p *and* q *be primes and* G *a semi-direct product* $P \rtimes Q$ *of a cyclic* p*-group* P *and a cyclic* q*-group* Q *such that* G' *is cyclic of prime order. Then* G *is bicyclic resistant.*

Proof. Let $a, b \in G$ such that $\langle a \rangle = P$ and $\langle b \rangle = Q$. We will separate two cases which only differ in technical details though.

Assume first that $p = q$. Then our conditions imply that the action of Q on P is of order p, i.e. $b^p \in \mathcal{Z}(G)$. To construct a non-trivial bicyclic nilpotent element in $\mathbb{Z}G$, we need to find $g, u \in G$ and a subgroup U of G containing u such that $u^g \notin U$. In the present conditions, the only elements which generate non-normal cyclic subgroups of G are those of shape $\langle a^i b \rangle$ for some integer i. Any subgroup of G containing $\langle a^i b \rangle$ properly will also contain G' and hence be normal. So, up to left-right symmetry, the only non-trivial bicyclic nilpotent elements in $\mathbb{Z}G$ are of shape $(1 - a^i b)g\widehat{\langle a^i b \rangle}$. We fix such a generic element $n \in \mathbb{Z}G$.

The group G is metabelian, so we can use lemma 2.5 to construct all the elements of $\mathrm{PCI}(\mathbb{Q}G)$. Fix $A = \langle a, b^p \rangle$, a maximal abelian subgroup of G containing G'. Assume $e \in \mathrm{PCI}(\mathbb{Q}G)$ with $e = e(G,H,K)$. If $ne \neq 0$, then K does not contain G'. On the other hand, K does contain H' and H contains A, which implies $H = A$. Set $S = \langle b^p \rangle$. Then we can write $\widehat{\langle a^i b \rangle} = g_1 \widetilde{S} + \cdots + g_n \widetilde{S}$ for $g_1, \ldots, g_n$ a transversal of S in $\langle a^i b \rangle$. So $ne \neq 0$ implies $\widetilde{S}e \neq 0$. As S is a central cyclic group and the sum of all the roots of unity of the same order equals 0, this implies $S \leq \ker(\varphi_e)$ and so $S \leq K$. As S is a maximal subgroup of A among those not containing G', we obtain $K = S$. So e is uniquely determined by the property $ne \neq 0$. Hence for every $f \in \mathrm{PCI}(\mathbb{Q}G)$ one has $nf = 0$ or $nf = n$. Overall, G is bicyclic resistant.

https://doi.org/10.1017/prm.2025.10013 Published online by Cambridge University Press

Next assume $p \neq q$. Then our conditions imply that P has order p. Similarly as in the previous case, the only elements of G which do not generate normal cyclic subgroups are those of shape $\langle a^i b^j \rangle$ for some integers i and j such that $b^j \notin \mathcal{Z}(G)$. A subgroup of G containing $\langle a^i b^j \rangle$ either contains G' or will be a cyclic q-group. So a generic bicyclic nilpotent element n can be written as $(1 - a^i b^j) g \widetilde{R}$, where R is a cyclic q-group containing $a^i b^j$. Again we want to use lemma 2.5. Let $S = \mathcal{Z}(G) \cap Q$. Then $A = \langle a \rangle \times S$ is a maximal abelian subgroup of G containing G'. As before choosing $e = e(G, H, K)$ one concludes $H = A$. Moreover we note that $S \leq R$, so we can again write $\widetilde{R} = g_1 \widetilde{S} + \cdots + g_n \widetilde{S}$ for $g_1, \ldots, g_n$ a transversal of S in R. So $ne \neq 0$ implies $\widetilde{S} \neq 0$, but this is only possible if $S \leq K$. This means $e = e(G, A, S)$, so the element of $\mathrm{PCI}(\mathbb{Q}G)$ which satisfies $ne \neq 0$ is unique. □

This implies on one hand that the work carried out for the proof of Theorem 3.5 could not be carried out using bicyclic nilpotent elements, as well as that these elements cannot serve to solve the remaining case of SSN groups of unfaithful type.

Corollary 5.21. *The groups $G(p, m, n)$, defined in §3.2, are bicyclic resistant. Also, the SSN groups of unfaithful type are bicyclic resistant.*

We are finally ready to describe which groups with SN are bicyclic resistant.

Proof of Theorem 5.16. Following corollary 5.19 we know that (3) implies (1). Next suppose (1), i.e. G is bicyclic resistant. Since SSN groups of unfaithful type and nilpotent groups are supersolvable, it remains to consider the groups dealt within Theorem 3.15. The proof of Theorem 3.15, in fact, constructs a bicyclic nilpotent element $n \in \mathbb{Z}G$ and a central idempotent $e \in \mathbb{Q}G$ such that $ne \notin \mathbb{Z}G$ if and only if G has more than one matrix component. In other words, those groups are bicyclic resistant if and only if G has one matrix component, which finishes the proof that (1) implies (2).

Now suppose (2). If $\mathbb{Q}G$ has one matrix component, then it has DK by Theorem 5.2. Therefore, we may assume that $\mathbb{Q}G$ has more than one matrix component and is supersolvable. If G is even nilpotent, then by Proposition 2.8 the group G has SSN and so also DK by lemma 5.14. It remains to consider the case that G is supersolvable but not nilpotent. It is easily verified that the group $P \rtimes H$ with H acting irreducibly and faithfully as in Proposition 2.17 is supersolvable if and only if P is cyclic and so also H is cyclic. Using lemma 5.11, we now see that supersolvable not nilpotent SN groups have DK. □

Remark 5.22. One could wonder in how far being bicyclic resistant is a property of the group ring $\mathbb{Z}G$ defined independently of the group basis G. In general, this is not clear, but at least for those groups where a positive answer to the second Zassenhaus conjecture is known, this is the case. Recall that the second Zassenhaus conjecture asked, if it is true that when H is a group of normalized units of $\mathbb{Z}G$ of the same order as G, there necessarily exists a unit $x \in \mathbb{Q}G$ such that $H^x = G$. It is clear that if such a unit exists the bicyclic nilpotent elements which can be defined using the elements of G are conjugate in $\mathbb{Q}G$ to those which can be defined using H. As the central idempotents of $\mathbb{Q}G$ do not change under conjugation of course, it follows that in this situation being bicyclic resistant does not depend on

https://doi.org/10.1017/prm.2025.10013 Published online by Cambridge University Press

the chosen group basis. More strongly one could even take any two units of $\mathbb{Z}G$ which generate a subgroup of finite order to construct a bicyclic nilpotent. This will also not break bicyclic resistance at least when the third Zassenhaus conjecture has a positive answer for G, i.e. if every finite subgroup of units in $\mathbb{Z}G$ is conjugate in the units of $\mathbb{Q}G$ to a subgroup of $\pm G$.

We remark that nilpotent groups are known to satisfy the third Zassenhaus conjecture [52] as well as metacyclic groups $A \rtimes B$ when A and B have coprime orders [47]. So neither could we have constructed bicyclic nilpotent elements with respect to any finite subgroup of units of $\mathbb{Z}G$ for the groups $G(p, m, n)$ in §3.2 to prove Theorem 3.5, nor will this be possible to resolve ND for SSN groups of unfaithful type.

These observations might lead to wonder, if in fact the third Zassenhaus Conjecture might hold for all groups with DK. This is, however, not the case: it can be checked that the counterexample to the conjecture presented in [19] does have property DK.

5.3. Concluding remarks on the Jordan decomposition

The motivation of the work of Jespers–Sun [27] was to contribute to the precise classification of groups having Multiplicative Jordan Decomposition. Though many contributions have been made here, the complete classification remains elusive. We refer to [16] for a survey and to [29, 51] for the only results to have appeared since.

Remark that a first major difference between ND and MJD is that the latter implies that the reduced degree of all simple components are at most 3 [1]. However, there exists groups having ND with a simple component of arbitrary large reduced degree, e.g. the groups $C_{p^m} \rtimes C_{p^n}$ in [27, Theorem A].

Next, analysing all groups for which the Multiplicative Jordan Decomposition is known to hold and those for which it remains open, using [37, Section 7.4] and [27], one finds first that all groups which are known to have the Multiplicative Jordan Decomposition have at most one matrix component. The only groups among those for which it remains open with more than one matrix component are the groups of type $C_p \rtimes C_{2^k}$ with $k \geq 3$ and $p \equiv 1 \bmod 8$ and where the action of the cyclic 2-group is by inversion. Note that these groups are SSN groups of unfaithful type—so exactly from the series for which the equivalence between property ND and having at most one matrix component remains open. Hence an answer to the following might solve the Multiplicative Jordan Decomposition for a new series and provide an answer to whether the Multiplicative Jordan Decomposition for a group implies that it has at most one matrix component.

QUESTION 5.23. Let p and q be primes and $G = C_p \rtimes C_{q^k}$ for some natural number k such that the action of C_{q^k} is not faithful. Is it true that G has ND if and only if it has one matrix component?

The smallest group with more than one matrix component for which the Multiplicative Jordan Decomposition remains unknown is

$$\langle x, a \mid x^{17} = a^8 = 1, x^a = x^{-1} \rangle \cong C_{17} \rtimes C_8.$$

https://doi.org/10.1017/prm.2025.10013 Published online by Cambridge University Press

In [16, Section 4.1], it is called 'a challenging open case'. We can confirm it is challenging. Answering our question would also eliminate the last question mark in [27, Figure 1].

Acknowledgements

We thank B. Sury and Amir Behar for useful conversations concerning lemma 4.5. We also thank Eric Jespers and Wei-Liang Sun for interesting conversations. We would also like to thank the referee for many suggestions which improved the readability of the article.

The first author is grateful to Fonds Wetenschappelijk Onderzoek vlaanderen—FWO (grant 88258) and le Fonds de la Recherche Scientifique—FNRS (grant 1.B.239.22) for financial support.

The second author was supported by the Spanish ministry of Science and Innovation under a Ramon y Cajal grant (reference RYC2021-032471-I) and a Severo Ochoa Grant CEX2019-000904-S funded by MCIN/AEI/10.13039/501100011033.

References

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

2 M. Aschbacher. *Finite group theory*, Volume 10 of Cambridge Studies in Advanced Mathematics, 2nd edn (Cambridge University Press, Cambridge, 2000).

3 A. Bächle, G. Janssens, E. Jespers, A. Kiefer and D. Temmerman. A dichotomy for integral group rings via higher modular groups as amalgamated products. *J. Algebra* **604** (2022), 185–223.

4 A. Bächle, G. Janssens, E. Jespers, A. Kiefer and D. Temmerman. Abelianization and fixed point properties of linear groups and units in integral group rings. *Math. Nachr.* **296** (2023), 8–56.

5 A. Bächle, S. Maheshwary and L. Margolis. Abelianization of the unit group of an integral group ring. *Pacific J. Math.* **312** (2021), 309–334.

6 A. Bak and U. Rehmann. The congruence subgroup and metaplectic problems for $\mathrm{SL}_{n\geq 2}$ of division algebras. *J. Algebra* **78** (1982), 475–547.

7 G. K. Bakshi, O. Broche Cristo, A. Herman, A. Konovalov, S. Maheshwary, A. Olivieri, G. Olteanu, A. del Rio, I. Van Gelder. Wedderga—Wedderburn decomposition of group algebras, version 4.0.0. https://gap-packages.github.io/wedderga/, 2020.

8 H. Bass, J. Milnor and J.-P. Serre. Solution of the congruence subgroup problem for SL_n ($n \geq 3$) and Sp_{2n} ($n \geq 2$). *Inst. Hautes Études Sci. Publ. Math.* 33 (1967), 59–137.

9 Y. G. Berkovich and Z. Janko. *Groups of prime power order. Volume 4*, volume 61 of De Gruyter Expo. Math. (De Gruyter, Berlin, 2016).

10 H. U. Besche, B. Eick and E. O'Brien. SmallGrp: The GAP Small Groups Library, version 1.4.1. https://gap-packages.github.io/smallgrp/, 2019.

11 A. Borel and J. Tits. Groupes reductifs. *Publ. Math. Inst. Hautes Étud. Sci.* **27** (1965), 659–755.

12 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)(1)** (2009), 177–185.

13 J. D. Dixon, M. P. F. du Sautoy, A. Mann and D. Segal. *Analytic pro-p groups*, volume 61 of Cambridge Studies in Advanced Mathematics, 2nd edn (Cambridge University Press, Cambridge, 1999).

14 F. Eisele, A. Kiefer and I. Van Gelder. Describing units of integral group rings up to commensurability. *J. Pure Appl. Algebra* **219** (2015), 2901–2916.

15 A. Garcia-Blazquez and A. del Rio. The isomorphism problem for rational group algebras of finite metacyclic groups. *J. Pure Appl. Algebra* **229** (2025), 107951.

https://doi.org/10.1017/prm.2025.10013 Published online by Cambridge University Press

16 A. W. Hales and I. B. S. Passi. *Group rings and Jordan decomposition*, In Groups, Rings, Group Rings, and Hopf Algebras, pp. 103–111 (Amer. Math. Soc., Providence, RI, 2017), volume 688 of *Contemp. Math.*

17 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.

18 T. Hawkins. Weierstrass and the theory of matrices. *Arch. Hist. Exact Sci.* **17** (1977), 119–163.

19 M. Hertweck. Another counterexample to a conjecture of Zassenhaus. *Beiträge Algebra Geom.* **43** (2002), 513–520.

20 B. Huppert. *Endliche Gruppen. I*, volume 134 of Grundlehren Math. Wiss. (Springer, Cham, 1967).

21 I. M. Isaacs. *Character theory of finite groups*. Corrected reprint of the 1976 original [Academic Press, New York; MR0460423, AMS Chelsea Publishing, Providence, RI, 2006].

22 G. Janssens, E. Jespers and O. Schnabel. Units of twisted group rings and their correlations to classical group rings. *Adv. Math.* **458** (2024), 109983, 81.

23 E. Jespers and A. del Rio. A structure theorem for the unit group of the integral group ring of some finite groups. *J. Reine Angew. Math.* **521** (2000), 99–117.

24 E. Jespers and A. del Rio. Group Ring Groups. Vol. 1. Orders and Generic Constructions of Units (De Gruyter Graduate. De Gruyter, Berlin, 2016).

25 E. Jespers. Bicyclic units in some integral group rings. *Canad. Math. Bull.* **38** (1995), 80–86.

26 E. Jespers and M. M. Parmenter. Units of group rings of groups of order 16. *Glasgow Math. J.* **35** (1993), 367–379.

27 E. Jespers and W.-L. Sun. Nilpotent decomposition in integral group rings. *J. Algebra* **575** (2021), 127–158.

28 E. Kleinert and A. del Rio. On the indecomposability of unit groups. *Abh. Math. Sem. Univ. Hamburg* **71** (2001), 291–295.

29 W. Kuo and W.-L. Sun. The multiplicative Jordan decomposition in the integral group ring $\mathbb{Z}[Q_8 \times C_p]$. *J. Algebra* **534** (2019), 16–33.

30 C. -H. Liu. Multiplicative Jordan decomposition in group rings and p-groups with all noncyclic subgroups normal. *J. Algebra.* **371** (2012), 300–313.

31 C.-H. Liu and D. S. Passman. Multiplicative Jordan decomposition in group rings of 3-groups. *J. Algebra Appl.* **8** (2009), 505–519.

32 C.-H. Liu and D. S. Passman. Multiplicative Jordan decomposition in group rings of $2, 3$-groups. *J. Algebra Appl.* **9** (2010), 483–492.

33 C.-H. Liu and D. S. Passman. Groups with certain normality conditions. *Commun. Algebra* **44** (2016), 3308–3323.

34 K. Lux and H. Pahlings. *A computational approach*, volume 124 of Cambridge Studies in Advanced Mathematics (Cambridge University Press, Cambridge, 2010).

35 A. R. MacWilliams. On 2-groups with no normal Abelian subgroups of rank 3, and their occurrence as Sylow 2-subgroups of finite simple groups. *Trans. Am. Math. Soc.* **150** (1970), 345–408.

36 W. Magnus. Noneuclidean Tesselations and Their Groups, Vol. 61 (Academic Press [Harcourt Brace Jovanovich, Publishers], New York-London, 1974).

37 C. P. Milies and S. K. Sehgal. *An introduction to group rings*, volume 1 of Algebra and Applications (Kluwer Academic Publishers, Dordrecht, 2002).

38 M. Newman. Integral matrices. Academic Press, New York-London, 1972. *Pure and Applied Mathematics* **45**

39 A. Olivieri, A. del Rio and J. J. Simon. On monomial characters and central idempotents of rational group algebras. *Commun. Algebra* **32** (2004), 1531–1550.

40 D. S. Passman. *The algebraic structure of group rings*, Pure and Applied Mathematics (Wiley-Interscience [John Wiley & Sons], New York-London-Sydney, 1977).

41 V. Platonov and A. Rapinchuk. *Algebraic groups and number theory. Transl. from the Russian by Rachel Rowen*, volume 139 of Pure Appl. Math. Academic Press (Academic Press, Boston, MA, 1994).

42 M. S. Raghunathan. On the congruence subgroup problem. II. *Invent. Math.* **85** (1986), 73–117.

https://doi.org/10.1017/prm.2025.10013 Published online by Cambridge University Press

43 J.-P. Serre. Le problème des groupes de congruence pour SL2. *Ann. of Math. (2)* **92** (1970), 489–527.

44 M. Shirvani and B. A. F. Wehrfritz. *Skew linear groups*, volume 118 of London Mathematical Society Lecture Note Series (Cambridge University Press, Cambridge, 1986).

45 The GAP Group, *GAP – Groups, Algorithms, and Programming. Version 4.10.2* (2019), http://www.gap-system.org.

46 J. Tits. Systèmes générateurs de groupes de congruence. *C. R. Acad. Sci. Paris Sér. A-B* **283** (1976), Ai, A693–A695.

47 A. Valenti. Torsion units in integral group rings. *Proc. Amer. Math. Soc.* **120** (1994), 1–4.

48 L. N. Vasersteuin. The group SL_2 over Dedekind rings of arithmetic type, *Mat. Sb. (N.S.)* **89(131)** (1972), 313–322, 351.

49 L. N. Vasersteuin. Structure of the classical arithmetic groups of rank greater than 1. *Mat. Sb. (N.S.)* **91** (1973), 445–470, 472.

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

51 X. Wang and Q. Zhou. Multiplicative Jordan decomposition in integral group ring of group $K_8 \times C_5$. *Commun. Math. Res.* **33** (2017), 64–72.

52 A. Weiss. Torsion units in integral group rings. *J. Reine Angew. Math.* **415** (1991), 175–187.

https://doi.org/10.1017/prm.2025.10013 Published online by Cambridge University Press