Journal of Algebra 405 (2014) 1–34

Contents lists available at ScienceDirect

Journal of Algebra

www.elsevier.com/locate/jalgebra

On the Congruence Subgroup Problem for integral group rings ☆

Mauricio Caicedo, Ángel del Río *

Departamento de Matemáticas, Universidad de Murcia, 30100 Murcia, Spain

ARTICLE INFO

Article history:
Received 4 September 2013
Available online 25 February 2014
Communicated by Leonard L. Scott, Jr.

MSC:
19B37
20H05
20C05

Keywords:
Congruence Subgroup Problem
Integral group rings

ABSTRACT

Let G be a finite group, $\mathbb{Z}G$ the integral group ring of G and $\mathcal{U}(\mathbb{Z}G)$ the group of units of $\mathbb{Z}G$. The Congruence Subgroup Problem for $\mathcal{U}(\mathbb{Z}G)$ is the problem of deciding if every subgroup of finite index of $\mathcal{U}(\mathbb{Z}G)$ contains a congruence subgroup, i.e. the kernel of the natural homomorphism $\mathcal{U}(\mathbb{Z}G) \to \mathcal{U}(\mathbb{Z}G/m\mathbb{Z}G)$ for some positive integer m. The congruence kernel of $\mathcal{U}(\mathbb{Z}G)$ is the kernel of the natural map from the completion of $\mathcal{U}(\mathbb{Z}G)$ with respect to the profinite topology to the completion with respect to the topology defined by the congruence subgroups. The Congruence Subgroup Problem has a positive solution if and only if the congruence kernel is trivial. We obtain an approximation to the problem of classifying the finite groups for which the congruence kernel of $\mathcal{U}(\mathbb{Z}G)$ is finite. More precisely, we obtain a list L formed by three families of finite groups and 19 additional groups such that if the congruence kernel of $\mathcal{U}(\mathbb{Z}G)$ is infinite then G has an epimorphic image isomorphic to one of the groups of L. Regarding the converse of this statement we at least know that if one of the 19 additional groups in L is isomorphic to an epimorphic image of G then the congruence kernel of $\mathcal{U}(\mathbb{Z}G)$ is infinite. However, to decide for the finiteness of the congruence kernel in case G has an epimorphic image isomorphic to one of the groups in the three families of L one needs to

☆ This research is partially supported by the Spanish Government under Grant MTM2012-35240 with "Fondos FEDER" and Fundación Séneca of Murcia under Grant 04555/GERM/06.
* Corresponding author.

http://dx.doi.org/10.1016/j.jalgebra.2014.01.029

know if the congruence kernel of the group of units of an order in some specific division algebras is finite and this seems a difficult problem.

1. Introduction

Let A be a finite dimensional semisimple rational algebra and R a $\mathbb{Z}$-order in A. Let $\mathcal{U}(R)$ denote the group of units of R. For a positive integer m let $\mathcal{U}(R,m)$ denote the kernel of the natural group homomorphism $\mathcal{U}(R) \to \mathcal{U}(R/mR)$, i.e.

$$\mathcal{U}(R,m) = \big\{u \in \mathcal{U}(R):\ u-1 \in mR\big\}.$$

More generally, if n and m are positive integers then $M_n(R)$ denotes the $n \times n$ matrix ring with entries in R, $\mathrm{GL}_n(R)$ denotes the group of units of $M_n(R)$, $\mathrm{SL}_n(R)$ denotes the subgroup of $\mathrm{GL}_n(R)$ formed by the elements of reduced norm 1, $\mathrm{GL}_n(R,m) = \mathcal{U}(M_n(R),m)$ and $\mathrm{SL}_n(R,m) = \mathrm{SL}_n(R) \cap \mathrm{GL}_n(R,m)$.

A subgroup of $\mathcal{U}(R)$ (respectively, $\mathrm{SL}_n(R)$) containing $\mathcal{U}(R,m)$ (respectively, $\mathrm{SL}_n(R,m)$) for some positive integer m is called a congruence subgroup of $\mathcal{U}(R)$ (respectively, $\mathrm{SL}_n(R)$). If m is a positive integer then R/mR is finite. Hence $\mathcal{U}(R,m)$ has finite index in $\mathcal{U}(R)$ and $\mathrm{SL}_n(R,m)$ has finite index in $\mathrm{SL}_n(R)$. Therefore every congruence subgroup of $\mathcal{U}(R)$ (respectively, $\mathrm{SL}_n(R)$) has finite index in $\mathcal{U}(R)$ (respectively, $\mathrm{SL}_n(R)$). The *Congruence Subgroup Problem* (*CSP*, for brevity) asks for the converse of this statement. More precisely, we say that the CSP has a positive solution for R (respectively, for $\mathrm{SL}_n(R)$) if every subgroup of finite index in $\mathcal{U}(R)$ (respectively, in $\mathrm{SL}_n(R)$) is a congruence subgroup. See [12] for a survey on a much more general version of the Congruence Subgroup Problem.

Serre introduced a quantitative version of the Congruence Subgroup Problem. Let $\mathcal{F}$ be the set of normal subgroups of finite index in $\mathcal{U}(R)$ and let $\mathcal{C}$ denote the set of congruence subgroups of $\mathcal{U}(R)$. Both $\mathcal{F}$ and $\mathcal{C}$ define bases of neighborhoods of 1 for group topologies in $\mathcal{U}(R)$. The corresponding completions are the projective limits

$$\mathcal{U}_{\mathcal{F}}(R) = \varprojlim_{N\in\mathcal{F}} \mathcal{U}(R)/N \quad \text{and} \quad \mathcal{U}_{\mathcal{C}}(R) = \varprojlim_{N\in\mathcal{C}} \mathcal{U}(R)/N.$$

The identity map of $\mathcal{U}(R)$ induces a surjective group homomorphism $\mathcal{U}_{\mathcal{F}}(R) \to \mathcal{U}_{\mathcal{C}}(R)$ and the kernel of this homomorphism is called the *congruence kernel* of $\mathcal{U}(R)$. The congruence kernel of $\mathrm{SL}_n(R)$ is defined similarly. It is easy to see that the CSP has a positive solution if and only if the congruence kernel is trivial. The quantitative version

E-mail addresses: mjose.caicedo@um.es (M. Caicedo), adelrio@um.es (Á. del Río).

of the CSP is the problem of calculating the congruence kernel. If S is another $\mathbb{Z}$-order in A then $mR \subseteq S$ and $mS \subseteq R$ for some positive integer m and $\mathcal{U}(R) \cap \mathcal{U}(S)$ has finite index in both $\mathcal{U}(R)$ and $\mathcal{U}(S)$. Using this it is easy to see that the congruence kernel of $\mathcal{U}(R)$ is finite if and only if the congruence kernel of $\mathcal{U}(S)$ is finite. In that case we say that A has the CSP property.

Assume now that $A = \prod_{i=1}^{k} M_{n_i}(D_i)$ is the Wedderburn decomposition of A (i.e. each n_i is a positive integer and D_i a finite dimensional rational division algebra) and let R_i be an order in D_i for every i. Then $\prod_{i=1}^{k} M_{n_i}(R_i)$ is an order in A, and for each i, $Z(R_i)$ is a $\mathbb{Z}$-order in $Z(D_i) \cong Z(M_{n_i}(D_i))$, $\mathcal{U}(Z(R_i)) \cap \mathrm{SL}_n(R_i)$ is finite and $\langle \mathcal{U}(Z(R_i)), \mathrm{SL}_n(R_i) \rangle$ has finite index in $\mathrm{GL}_n(R)$. Combining this with the facts that number fields have the CSP property and that the order chosen to check the CSP property does not make a difference, it is easy to see that A has the CSP property if and only if each non-commutative component $M_{n_i}(D_i)$ has the CSP property if and only if the congruence kernel of $\mathrm{SL}_{n_i}(R_i)$ is finite for every $i = 1, \ldots, k$.

The CSP for $\mathrm{SL}_n(R)$, with R an order in a finite dimensional division algebra D has been widely studied and solved except for the case when $n = 1$ and D is non-commutative (see e.g. [12]). An algebra is said to be *exceptional* if it is one of the following types:

(EC1) A non-commutative finite dimensional division rational algebra which is not a totally definite quaternion algebra.
(EC2) A two-by-two matrix ring over D with $D = \mathbb{Q}$, an imaginary quadratic extension of $\mathbb{Q}$ or a totally definite quaternion algebra over $\mathbb{Q}$.

By results of [4,16,7,17] every finite dimensional simple algebra not having the CSP property is exceptional. Moreover, the exceptional algebras of type (EC2) do not have the CSP property.

This paper addresses the CSP for integral group rings of finite groups. More precisely our aim is to classify the finite groups G for which the congruence kernel of $\mathcal{U}(\mathbb{Z}G)$ is finite (equivalently, the rational group algebra $\mathbb{Q}G$ has the CSP property). Besides the intrinsic interest of this question its solution has applications in the study of the group of units of $\mathbb{Z}G$, not only because a solution for the CSP provides relevant information on the normal subgroups of $\mathcal{U}(\mathbb{Z}G)$ but also because it can be used to obtain generators of a subgroup of finite index in $\mathcal{U}(\mathbb{Z}G)$ as it has been shown in [14] and [6].

We now explain our strategy. By the discussion above, the congruence kernel of $\mathcal{U}(\mathbb{Z}G)$ is finite if and only if every non-commutative simple component of $\mathbb{Q}G$ has the CSP property. If N is a normal subgroup of G then every simple component of $\mathbb{Q}(G/N)$ is a simple component of $\mathbb{Q}G$. Therefore, if $\mathbb{Q}G$ has the CSP property then $\mathbb{Q}(G/N)$ has the CSP property. This suggests the following approach to the problem. We say that G is *CSP-critical* if $\mathbb{Q}G$ does not have the CSP property but $\mathbb{Q}(G/N)$ has the CSP property for every non-trivial normal subgroup of G. Thus the congruence kernel of $\mathcal{U}(\mathbb{Z}G)$ is infinite if and only if G has a CSP-critical epimorphic image. The original problem hence reduces to classify the CSP-critical finite groups. Assume that G is a finite CSP-critical

group. Then G is isomorphic to a subgroup of an exceptional simple component of $\mathbb{Q}G$. Hence G is a subgroup of either a division algebra or a two-by-two matrix over a division algebra (see the paragraph after Corollary 1.2). The finite subgroups of division algebras have been classified by Amitsur [1] and the finite subgroups of two-by-two matrices over division algebras have been classified by Banieqbal [2]. Thus, in order to classify the CSP-critical groups it suffices to decide which of the groups of the classifications of Amitsur and Banieqbal are CSP-critical.

Unfortunately this strategy encounters a serious difficulty. Namely, the problem of deciding which algebras of type (EC1) have the CSP property seems to be far from reachable with the known techniques. So we address a more modest problem which is an approximation to the problem of classifying the CSP-critical groups. We say that a finite group is *CSP'-critical* if $\mathbb{Q}G$ has an exceptional component but $\mathbb{Q}(G/N)$ does not have exceptional components for any non-trivial normal subgroup N of G.

The main theorem of this paper is the following (see notation in Section 2):

Theorem 1.1. *A finite group G is CSP'-critical if and only if G is isomorphic to one of the following groups.*

(1) $C_q \times (C_p \rtimes_2 C_4)$ *with p and q different primes such that $3 \neq p \equiv -1 \bmod 4$, $q > 2$ and $2 \nmid o_q(p)$.*
(2) $C_p \rtimes_k C_n$ *with $n \geqslant 8$, p an odd prime not dividing n, $\frac{n}{k}$ is divisible by all the primes dividing n and one of the following conditions holds*:
   (a) $k = \gcd(n, p-1)$, *either n is odd or $p \equiv 1 \bmod 4$ and if $p = 5$ then $n = 8$.*
   (b) $k = \gcd(n, p-1)$, $3 \neq p \equiv -1 \bmod 4$ *and $n \neq 4$ and $v_2(n) = 2$.*
   (c) $3 \neq p \equiv -1 \bmod 4$, $n = 2^{v_2(p+1)+2}$ *and $k = 2^{v_2(p+1)+1}$.*
(3) $\mathcal{Q}_8 \times C_p$ *with p an odd prime and $o_p(2)$ odd.*
(4) $\mathrm{SL}(2,3) = \langle i, j\rangle_{\mathcal{Q}_8} \rtimes \langle g\rangle_3$, *with $i^g = j$, $j^g = ij$.*
(5) $\mathrm{SL}(2,5) = \langle u, v \mid u^4 = v^3 = 1,\ (uv)^5 = u^2\rangle$.
(6) $\mathcal{D}_6$.
(7) $\mathcal{D}_8$.
(8) $\mathcal{D}_{16}^+$.
(9) $\mathcal{Q}_8 \rtimes C_2 = \langle i, j\rangle_{\mathcal{Q}_8} \rtimes \langle a\rangle_2$, *with $i^a = i^{-1}$ and $j^a = j$.*
(10) $\mathcal{Q}_8 \times C_3$.
(11) $\mathcal{Q}_8 \curlyvee_2 \mathcal{D}_8$.
(12) $C_5 \rtimes_2 C_8$.
(13) $(C_3 \times C_3) \rtimes_2 C_8 = (\langle a\rangle_3 \times \langle b\rangle_3) \rtimes_2 \langle c\rangle_8$, *with $a^c = b^{-1}$ and $b^c = a$.*
(14) $\mathrm{SL}(2,3) \curlyvee_2 \mathcal{D}_8$.
(15) $\mathcal{C} = (\mathcal{Q}_8 \times \mathcal{Q}_8) \rtimes C_6 = (\langle i_1, j_1\rangle_{\mathcal{Q}_8} \times \langle i_2, j_2\rangle_{\mathcal{Q}_8}) \rtimes \langle b\rangle_6$ *with*

$$i_1^b = i_2, \qquad j_1^b = j_2, \qquad i_2^b = j_1 \quad \text{and} \quad j_2^b = i_1 j_1.$$

(16) $\mathrm{SL}(2,3) \curlyvee_2 C_4$.

(17) $\mathrm{SL}(2,9)$.

(18)

$$\begin{aligned}\mathcal{A}^+ &= \mathrm{SL}(2,5) \downarrow_4 C_8 = \langle v, d | d^8 = v^3 = 1, \left(d^2 v\right)^5 = d^4, v^d = v d^{-2}\left(v, d^2\right)\rangle \\ &= \langle u, v\rangle_{\mathrm{SL}(2,5)} \downarrow_4 \langle d\rangle_8,\end{aligned}$$

with u and v as in (5), $v^d = vu^{-1}(v,u)$ *and* $d^2 = u$.

(19)

$$\begin{aligned}\mathcal{A}^- &= \mathrm{SL}(2,5) \downarrow_4 C_8 = \langle v, d | d^8 = v^3 = 1, \left(d^{-2} v\right)^5 = d^4, v^d = v d^2\left(v, d^{-2}\right)\rangle \\ &= \langle u, v\rangle_{\mathrm{SL}(2,5)} \downarrow_4 \langle d\rangle_8,\end{aligned}$$

with u and v as in (5), $v^d = vu^{-1}(v,u)$ *and* $d^2 = u^{-1}$.

(20) $\mathcal{B}_1 = (\mathcal{Q}_8 \curlyvee_2 \mathcal{D}_8) \rtimes C_5$ *with with* $\mathcal{Q}_8 = \langle i, j\rangle$, $\mathcal{D}_8 = \langle a\rangle_4 \rtimes \langle b\rangle_2$, $C_5 = \langle c\rangle_5$,

$$i^c = j^{-1}b, \qquad j^c = i^{-1}, \qquad a^c = ia^{-1}b \quad \text{and} \quad b^c = i^{-1}a^{-1}.$$

(21) $\mathcal{B}_2 = (\mathcal{Q}_8 \curlyvee_2 \mathcal{D}_8) \downarrow_2 (C_5 \rtimes_2 C_4)$, *with* $\mathcal{Q}_8 = \langle i, j\rangle$, $\mathcal{D}_8 = \langle a\rangle_4 \rtimes \langle b\rangle_2$, $C_5 \rtimes_2 C_4 = \langle c\rangle_5 \rtimes_2 \langle d\rangle_4$,

$$\begin{aligned}&i^c = i^2 j, \qquad j^c = i^{-1}b, \qquad a^c = jba, \qquad b^c = ja, \\ &i^d = i^2 a, \qquad j^d = ib, \qquad a^d = i^{-1}, \qquad b^d = ja \quad \text{and} \quad d^2 = i^2.\end{aligned}$$

(22) $\mathcal{B} = (\mathcal{Q}_8 \curlyvee_2 \mathcal{D}_8) \downarrow_2 \mathrm{SL}(2,5)$ *with* $\mathcal{Q}_8 = \langle i, j\rangle$, $\mathcal{D}_8 = \langle a\rangle_4 \rtimes \langle b\rangle_2$, $\mathrm{SL}(2,5) = \langle u, v\rangle$ *as in* (5),

$$\begin{aligned}&i^u = i^3, \qquad j^u = jb, \qquad a^u = i^3 ab, \qquad b^u = b, \\ &i^v = i^2 jab, \qquad j^v = i^3 jab, \qquad a^v = ib, \qquad b^v = ia \quad \text{and} \quad u^2 = i^2.\end{aligned}$$

We now discuss how far is the classification of CSP'-critical groups given by Theorem 1.1 from the desired classification of CSP-critical groups and the consequences of Theorem 1.1 to the original problem of classifying the finite groups G for which the congruence kernel of $\mathcal{U}(\mathbb{Z}G)$ is finite. If the congruence kernel of $\mathcal{U}(\mathbb{Z}G)$ is not finite then $\mathbb{Q}G$ has an exceptional component and therefore G has a CSP'-critical epimorphic image. Therefore we at least have the following.

Corollary 1.2. *Let G be a finite group. If G does not have an epimorphic image isomorphic to any of the groups listed in Theorem 1.1 then the congruence kernel of $\mathcal{U}(\mathbb{Z}G)$ is finite.*

Suppose that G is CSP'-critical and let A be an exceptional component of $\mathbb{Q}G$. Let $\pi : \mathbb{Q}G \to A$ be a surjective homomorphism of algebras and let $N = \{g \in G\colon\ \pi(g) = 1\}$. Then A is an exceptional simple component of $\mathbb{Q}(G/N)$. Thus, by assumption, $N = 1$ and hence G is a subgroup of A. Thus, if G is CSP'-critical then G can be embedded

in any of its exceptional components. If one of these exceptional components is of type (EC2) then $\mathbb{Q}G$ does not have the CSP property and hence G is CSP-critical. Along the proof of Theorem 1.1 we will show that the only groups in the list of Theorem 1.1 not having an exceptional component of type (EC2) are precisely those of types (1)–(3) (Proposition 4.2). So we have

Corollary 1.3. *Let G be a finite group.*

(1) *If G is isomorphic to one of the groups in items* (4)–(22) *of Theorem 1.1 then G is CSP-critical.*
(2) *If G has an epimorphic image isomorphic to one of the groups in items* (4)–(22) *of Theorem 1.1 then the congruence kernel of $\mathcal{U}(\mathbb{Z}G)$ is infinite.*

Assume that G is a finite CSP-critical group other than the groups is items (4)–(22) of Theorem 1.1. Then $\mathbb{Q}G$ does not have any exceptional component of type (EC2) and therefore G is a subgroup of a division algebra. This is the case of the groups of types (1)–(3) in Theorem 1.1. For example if $G = \mathcal{Q}_8 \times C_p$ as in (3) then the only exceptional component of $\mathbb{Q}G$ is isomorphic to the quaternion algebra $\mathbb{H}(\mathbb{Q}(\zeta_p))$. In this case G is a CSP-critical if and only if $\mathbb{H}(\mathbb{Q}(\zeta_p))$ does not have the CSP property. So to decide the question for these groups one needs to decide whether this algebra has the CSP property. Similarly, if $G = C_q \times (C_p \rtimes_2 C_4)$ as in (1) (respectively, $G \cong C_p \rtimes C_n$ as in (2)) then the only exceptional component of $\mathbb{Q}G$ is isomorphic to the quaternion algebra $A = (\frac{(\zeta_p - \zeta_p^{-1})^2, -1}{\mathbb{Q}(\zeta_q, \zeta_p + \zeta_p^{-1})})$ (respectively, the cyclic algebra $A = (\mathbb{Q}(\zeta_{pk})/F(\zeta_k), \zeta_k)$, where F is the only subfield of $\mathbb{Q}(\zeta_p)$ with $[\mathbb{Q}(\zeta_p) : F] = \frac{n}{k}$). In both cases G is CSP-critical if and only if A does not have the CSP property. In case these groups are CSP-critical, then the CSP-critical groups are exactly the CSP'-critical groups, i.e. those listed in Theorem 1.1. However, if some of these groups are not CSP-critical then there could exist some CSP-critical groups, not included in Theorem 1.1. Such groups should have one proper epimorphic image isomorphic to one of the groups in items (1)–(3) of Theorem 1.1.

2. Notation, preliminaries and some tools

In this section we fix the notation which will be used throughout the paper.

The cardinality of a set X is denoted by $|X|$. As it is customary, the Euler totient function will be denoted φ.

For r, m and p integers with p prime and $\gcd(r, m) = 1$ let

$$\begin{aligned} v_p(m) &= \text{maximum non-negative integer } k \text{ such that } p^k \text{ divides } m;\\ o_m(r) &= \text{multiplicative order of } r \text{ modulo } m,\\ &\qquad \text{i.e. the minimum positive integer } k \text{ such that } r^k \equiv 1 \bmod m;\\ \zeta_m &= \text{complex primitive } m\text{-th root of unity.} \end{aligned}$$

We use the standard group and ring theoretical notation. For example, the of a group or ring X is denoted $Z(X)$; if $a \in X$ and $Y \subseteq X$ then $C_Y(a)$ denotes the centralizer of a in Y and we use the exponential notation for conjugation: $a^b = b^{-1}ab$.

If G is a group, then G' denotes the commutator subgroup of G and $\exp(G)$ the exponent of G. If $g \in G$ then $|g|$ denotes the order of g and g^G denotes the conjugacy class of g in G. If $X \subseteq G$ then $\langle X \rangle$ denotes the subgroup generated by X. This is simplified to $\langle g_1, \dots, g_n \rangle$ for $X = \{g_1, \dots, g_n\}$. Sometimes, we write $\langle g \rangle_n$ to emphasize that g has order n or $\langle g_1, \dots, g_n \rangle_G$ to represent a group isomorphic to G and generated by $g_1, \dots, g_n$ (Theorem 1.1 contains some examples of this). If H is a subgroup of G then $N_G(H)$ denotes the normalizer of H in G and $\mathrm{Core}_G(H) = \bigcap_{g \in G} H^g$, the core of H in G. The notation $H \leqslant G$ (respectively, $H < G, H \trianglelefteq G, H \lhd G$) means that H is a subgroup (respectively, proper subgroup, normal subgroup, proper normal subgroup) of G. If p is a prime integer the $O_p(G)$ denotes the unique maximal normal p-subgroup of G.

We use the following constructions of groups:

$G \rtimes_m H =$ semidirect product of H acting on G with kernel of order m;

$G \curlyvee_m H =$ central product of G and H with subgroups of order m identified;

$G \rfloor_m H =$ semidirect product of H acting on G with subgroups of order m identified.

Some groups that we encounter in the paper are

$$\begin{aligned}
C_n &= \text{cyclic group of order } n;\\
\mathcal{D}_{2m} &= \langle a \rangle_m \rtimes \langle b \rangle_2 \quad \text{with} \quad a^b = a^{-1} \quad \text{(dihedral group of order } 2m);\\
\mathcal{Q}_{4m} &= \langle j \rangle_{2m} \rfloor_2 \langle i \rangle_4 \quad \text{with} \quad j^i = j^{-1} \quad \text{(quaternion group of order } 4m);\\
\mathcal{D}_{16}^+ &= \langle a \rangle_8 \rtimes \langle b \rangle_2, \quad \text{with} \quad a^b = a^5;\\
\mathcal{D}_{16}^- &= \langle a \rangle_8 \rtimes \langle b \rangle_2, \quad \text{with} \quad a^b = a^3;\\
S_m &= \text{symmetric group on } m \text{ symbols};\\
A_m &= \text{alternating group on } m \text{ symbols};\\
\mathrm{SL}(n,q) &= \big\{a \in M_n(\mathbb{F}_q) \colon \det(a) = 1\big\}, \quad \text{with } \mathbb{F}_q \text{ the field with } q \text{ elements};\\
\mathrm{PSL}(n,q) &= \mathrm{SL}(n,q)/Z\big(\mathrm{SL}(n,q)\big);\\
T_\alpha^* &= \mathcal{Q}_8 \rtimes_{3^{\alpha-1}} \langle g \rangle_{3^\alpha} \quad \big(\text{observe that } T_1^* \cong \mathrm{SL}(2,3)\big).
\end{aligned}$$

We also will encounter the following metacyclic groups

$$G_{m,r} = \big\langle a, b \bigm| a^m = 1,\ b^n = a^t,\ a^b = a^r \big\rangle = \langle a \rangle_m \rfloor_s \langle b \rangle_{ns} = \big\langle a^s \big\rangle_t \rtimes_s \langle b \rangle_{ns} \tag{2.1}$$

with

$$\gcd(m,r)=1, \qquad n=o_m(r), \qquad s=\gcd(r-1,m),$$
$$st=m, \quad \text{and} \quad \gcd(ns,t)=1. \tag{2.2}$$

Let F be a field of characteristic different of 2 and let a,b non-zero elements of F. Then $(\frac{a,b}{F})$ denotes the quaternion F-algebra $F[i,j \mid ji=-ij,\ i^2=a,\ j^2=b]$. Moreover $\mathbb{H}(F)=(\frac{-1,-1}{F})$. A *totally definite quaternion algebra* is a quaternion algebra of the form $(\frac{a,b}{F})$ with F a totally real number field and a and b totally negative, i.e. for every embedding $\sigma: F\to\mathbb{C}$, $\sigma(F)\subseteq\mathbb{R}$ and $\sigma(a)$ and $\sigma(b)$ are negative.

If R is a ring and G is a group then $R*_\tau^\alpha G$ denotes a *crossed product* with action $\alpha: G\to \mathrm{Aut}(R)$ and twisting $\tau: G\times G\to \mathcal{U}(R)$ [11], i.e. the associative ring $R*_\tau^\alpha G=\bigoplus_{g\in G} Ru_g$ with multiplication given by the following rules:

$$u_g a=\alpha_g(a)u_g \quad \text{and} \quad u_g u_h=\tau(g,h)u_{gh} \quad (a\in R,\ g,h\in G).$$

In case $G=\langle g\rangle_n$ then the crossed product $R*_\tau^\alpha G$ is completely determined by $\sigma=\alpha_g$ and $a=u_g^n$. In this case we follow the notation of [13] and denote the crossed product by (R,σ,a). A *classical crossed product* is a crossed product $L*_\tau^\alpha G$, where L/F is a finite Galois extension, $G=\mathrm{Gal}(L/F)$ and α is the natural action of G on L. A classical crossed product $L*_\tau^\alpha G$ is denoted by $(L/F,\tau)$ [13]. A cyclic algebra is a classical crossed product $(L/F,\tau)$ where $\mathrm{Gal}(L/F)$ is cyclic. If $\mathrm{Gal}(L/F)=\langle\sigma\rangle_n$ and $a=u_\sigma^n$ then the cyclic algebra $(L/F,\tau)$ is usually denoted $(L/F,a)$. Every classical crossed product $(L/F,\tau)$ is a central simple F-algebra [13, Theorem 29.6].

Consider a finite group G with a cyclic normal subgroup $A=\langle a\rangle_m$ and assume that A is also a maximal abelian subgroup of G. Fix a right inverse $\phi: G/A\to G$ of the natural projection $G\to G/A$ (i.e. $\phi(gA)A=gA$ for every $g\in G$). Then we define a crossed product

$$\mathbb{Q}(G,A)=\mathbb{Q}(\zeta_m)*_\tau^\alpha G/A,$$

with action and twisting given by

$$\alpha_{gA}(\zeta_m)=\zeta_m^i, \quad \text{if } a^{\phi(gA)}=a^iA,$$
$$\tau\big(gA,g'A\big)=\zeta_m^j, \quad \text{if } \phi\big(gg'A\big)^{-1}\phi(gA)\phi\big(g'A\big)=a^j,$$

for each $g,g'\in G$. (Notice that G/A is abelian because A is the kernel of the action of G on A by conjugation.) The algebra $\mathbb{Q}(G,A)$ is independent of the map ϕ up to isomorphisms. Using the natural isomorphism $\mathrm{Aut}(A)\to\mathrm{Aut}(\mathbb{Q}(\zeta_m))$ one can transfer the action of G on A by conjugation to an action of G on $\mathbb{Q}(\zeta_m)$. If F is the fixed field of this action then $gA\mapsto\alpha_{gA}$ defines an isomorphism $G/A\to\mathrm{Gal}(\mathbb{Q}(\zeta_m)/F)$ and if we see this isomorphism as an identification then $\mathbb{Q}(G,A)$ is the classical crossed product $(\mathbb{Q}(\zeta_m)/F,\tau)$.

We will need to compute the Wedderburn decomposition of $\mathbb{Q}G$ for some finite groups. For that we use the method introduced in [9] which was extended in [10] and implemented in the GAP package Wedderga [3]. We introduce the main lines of this method now (see [9] for details).

Let G be a finite group. For a subgroup H of G, let $\widehat{H} = \frac{1}{|H|}\sum_{h\in H} h$. Clearly, $\widehat{H}$ is an idempotent of $\mathbb{Q}G$ which is central if and only if H is normal in G. If $K \lhd H \leqslant G$ and $K \neq H$ then let

$$\varepsilon(H,K) = \prod(\widehat{K} - \widehat{M}) = \widehat{K}\prod(1 - \widehat{M}),$$

where M runs through the set of all minimal normal subgroups of H containing K properly. We extend this notation by setting $\varepsilon(H,H) = \widehat{H}$. Clearly $\varepsilon(H,K)$ is an idempotent of the group algebra $\mathbb{Q}G$. Let $e(G,H,K)$ be the sum of the distinct G-conjugates of $\varepsilon(H,K)$, that is, if T is a right transversal of $C_G(\varepsilon(H,K))$ in G, then

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

Clearly, $e(G,H,K)$ is a central element of $\mathbb{Q}G$ and if the G-conjugates of $\varepsilon(H,K)$ are orthogonal, then $e(G,H,K)$ is a central idempotent of $\mathbb{Q}G$.

A *strong Shoda pair* of G is a pair (H,K) of subgroups of G satisfying the following conditions: $K \leqslant H \trianglelefteqslant N_G(K)$, H/K is cyclic and a maximal abelian subgroup of $N_G(K)/K$ and the different G-conjugates of $\varepsilon(H,K)$ are orthogonal.

If (H,K) is a strong Shoda pair of G then H has a linear character with kernel K, which we denote $\lambda_{H,K}$. Moreover $\lambda_{H,K}^G$, the character of G induced by $\lambda_{H,K}$, is irreducible, $\ker \lambda_{H,K}^G = \mathrm{Core}_G(K)$ and $e(G,H,K)$ is the unique primitive central idempotent e of $\mathbb{Q}G$ with $\lambda_{H,K}^G(e) \neq 0$. If $N = N_G(K)$ and $n = [G:N]$ then

$$\mathbb{Q}Ge(G,H,K) \cong M_n\big(\mathbb{Q}(N/K, H/K)\big). \tag{2.3}$$

A simple component of $\mathbb{Q}G$ of the form $\mathbb{Q}Ge(G,H,K)$, for (H,K) a strong Shoda pair is called an *SSP component* of $\mathbb{Q}G$.

A group is said to be *strongly monomial* if all the simple components of $\mathbb{Q}G$ are SSP components. Every abelian-by-supersolvable group is strongly monomial [9]. The following theorem shows that for metabelian groups we can compute the primitive central idempotents of $\mathbb{Q}G$ using some special strong Shoda pairs.

Theorem 2.1. *(See [9].) Let G be a metabelian finite group and let A be a maximal abelian subgroup of G containing G'. The primitive central idempotents of $\mathbb{Q}G$ are the elements of the form $e(G,H,K)$, where (H,K) is a pair of subgroups of G satisfying the following conditions*:

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

The classification of the finite groups which are subgroups of division rings was obtained by Amitsur [1]. If G is a finite subgroup of a division ring then a Sylow subgroup of G is either cyclic or a quaternion 2-group. A *Z-group* is a finite subgroup of a division ring with all Sylow subgroups cyclic. For the readers convenience we include in the following theorem the classification of finite subgroups of division rings in the form presented in [15].

Theorem 2.2. *(See [1,15].)*

(Z) *The Z-groups are*:
- (a) *the finite cyclic groups,*
- (b) $C_m \rtimes_2 C_4$ *with* m *odd and* C_4 *acting by inversion on* C_m *and*
- (c) $C_m \rtimes_k C_n$ *with* $\gcd(m,n) = 1$ *and, using the following notation*:

$$\begin{aligned} P_p &= \textit{Sylow } p\textit{-subgroup of } C_m, \\ Q_p &= \textit{Sylow } p\textit{-subgroup of } C_n, \\ X_p &= \{q \mid n\colon\ q \textit{ prime and } (P_p, Q_q) \neq 1\}, \\ R_p &= \prod_{q\in X_p} Q_q; \end{aligned}$$

we have $C_n = \prod_{p\mid m} R_p$ *and the following properties hold for every prime* $p \mid m$ *and* $q \in X_p$:
- (i) $v_q(o_{\frac{|G|}{|P_p||R_p|}}(p)) < o_{q^{v_q(k)}}(p)$,
- (ii) *if* q *is odd or* $p \equiv 1 \bmod 4$ *then* $v_q(p-1) \leqslant v_q(k)$ *and*
- (iii) *if* $q = 2$ *and* $p \equiv -1 \bmod 4$ *then* $v_2(k)$ *is either* 1 *or greater than* $v_2(p+1)$.

(NZ) *The finite subgroups of division rings which are not Z-groups are*:
- (a) $\mathcal{O}^* = \langle s,t \mid (st)^2 = s^3 = t^4\rangle$ *(binary octahedral group),*
- (b) $\mathcal{Q}_m$ *with* $v_2(m) \geqslant 3$,
- (c) $\mathcal{Q}_8 \times M$ *with* M *a Z-group of odd order such that* $o_{|M|}(2)$ *is odd,*
- (d) $\mathrm{SL}(2,3) \times M$, *with* M *a Z-group of order coprime to 6 and* $o_{|M|}(2)$ *odd, and*
- (e) $\mathrm{SL}(2,5)$.

Following the proof of Theorem 2.2, in either [1] or [15], one can discover a minimal division ring containing each of the groups in the classification. We will need this for the non-abelian Z-groups. Assume $G = \langle a\rangle_m \rtimes_k \langle b\rangle_n$ with $\gcd(m,n) = 1$, $b^a = a^r$ and $n = o_m(r)$. Then $A = \langle a, b^{\frac{n}{k}}\rangle$ is cyclic and normal and maximal abelian in G and hence $(A,1)$ is a strong Shoda pair of G. Moreover, $a \mapsto \zeta_m$, $b \mapsto u_b$ determines an injective group homomorphisms $G \to \mathcal{U}(\mathbb{Q}(G,A))$. Furthermore, $\mathbb{Q}(G,A)$ is the algebra given by the presentation $\mathbb{Q}(\zeta_{mk})[u_b \mid \zeta_m^{u_b} = \zeta_m^r,\ u_b^{\frac{n}{k}} = \zeta_k]$. If $f : G \to \mathcal{U}(D)$ is an injective group homomorphism then $f(a)$ and $f(b^{\frac{n}{k}})$ are commuting roots of unity of

Table 1
The list of CSP'-critical groups. The third column displays the exceptional component of the rational group algebra. The last column represents the identification of the group in the GAP library of small groups [5] except for the first three families of groups.

#	G	Excep. Comp.	GAP ID
(1)	$C_q \times (C_p \rtimes_2 C_4)$	$(\frac{(\zeta_p-\zeta_p^{-1})^2,-1}{\mathbb{Q}(\zeta_q,\zeta_p+\zeta_p^{-1})})$	
(2)	$C_p \rtimes_k C_n$	$(\mathbb{Q}(\zeta_{pk})/F(\zeta_k),\zeta_k)$ $([\mathbb{Q}(\zeta_p):F]=\frac{n}{k})$	
(3)	$\mathcal{Q}_8 \times C_p$	$\mathbb{H}(\mathbb{Q}(\zeta_p))$	
(4)	$\mathrm{SL}(2,3)$	$M_2(\mathbb{Q}(\zeta_3))$	$[24,3]$
(5)	$\mathrm{SL}(2,5)$	$M_2(\frac{-1,-3}{\mathbb{Q}})$	$[120,5]$
(6)	$\mathcal{D}_6$	$M_2(\mathbb{Q})$	$[6,1]$
(7)	$\mathcal{D}_8$	$M_2(\mathbb{Q})$	$[8,3]$
(8)	$\mathcal{D}_{16}^+$	$M_2(\mathbb{Q}(\zeta_4))$	$[16,6]$
(9)	$\mathcal{Q}_8 \rtimes C_2$	$M_2(\mathbb{Q}(\zeta_4))$	$[16,13]$
(10)	$\mathcal{Q}_8 \times C_3$	$M_2(\mathbb{Q}(\zeta_3))$	$[24,11]$
(11)	$\mathcal{Q}_8 \curlyvee_2 \mathcal{D}_8$	$M_2(\mathbb{H}(\mathbb{Q}))$	$[32,50]$
(12)	$C_5 \rtimes_2 C_8$	$(\mathbb{Q}(\zeta_5)/\mathbb{Q},-1)$	$[40,3]$
(13)	$(C_3 \times C_3) \rtimes_2 C_8$	$M_2(\frac{-1,-3}{\mathbb{Q}})$	$[72,19]$
(14)	$\mathrm{SL}(2,3) \curlyvee_2 \mathcal{D}_8$	$M_2(\mathbb{H}(\mathbb{Q}))$	$[96,202]$
(15)	$\mathcal{C}$	$M_2(\mathbb{H}(\mathbb{Q}))$	$[384,618]$
(16)	$\mathrm{SL}(2,3) \curlyvee_2 C_4$	$M_2(\mathbb{Q}(\zeta_4))$	$[48,33]$
(17)	$\mathrm{SL}(2,9)$	$M_2(\frac{-1,-3}{\mathbb{Q}})$	$[720,409]$
(18)	$\mathcal{A}^+$	$(\mathbb{Q}(\zeta_5)/\mathbb{Q},-1)$	$[240,90]$
(19)	$\mathcal{A}^-$	$(\mathbb{Q}(\zeta_5)/\mathbb{Q},-1)$	$[240,89]$
(20)	$\mathcal{B}_1$	$M_2(\mathbb{H}(\mathbb{Q}))$	$[160,199]$
(21)	$\mathcal{B}_2$	$M_2(\mathbb{H}(\mathbb{Q}))$	$[320,1581]$
(22)	$\mathcal{B}$	$M_2(\mathbb{H}(\mathbb{Q}))$	$[1920,241003]$

order m and k respectively and $f(a^b) = f(a)^r$. Therefore $\zeta_m \mapsto f(a)$ and $u_b \mapsto f(b)$ defines an algebra homomorphism $\mathbb{Q}(G,A) \to D$, which is injective because $\mathbb{Q}(G,A)$ is simple. In particular, if D is a division algebra then so is $\mathbb{Q}(G,A)$. This proves the following:

Lemma 2.3. *Let $G = \langle a\rangle_m \rtimes_k \langle b\rangle_n$ with $\gcd(m,n) = 1$, $b^a = a^r$ and $n = o_m(r)$ and let $A = \langle a, b^{\frac{n}{k}}\rangle$. Then G is a subgroup of a division algebra if and only if $\mathbb{Q}(G,A)$ is a division algebra.*

3. Sufficiency

In this section we prove the sufficiency part of Theorem 1.1, namely we prove that all the groups listed in the theorem are CSP'-critical. We have to prove that for each G in the list of Theorem 1.1, $\mathbb{Q}G$ has an exceptional component while $\mathbb{Q}\overline{G}$ does not have exceptional components for any proper epimorphic image $\overline{G}$ of G. Table 1 displays

the exceptional component obtained in each case and, except for the first three infinite families, identifies the groups in the GAP library.

To prove that the groups of type (2) are CSP'-critical we need the following lemma.

Lemma 3.1. *Let $G = \langle a\rangle_p \rtimes_k \langle b\rangle_n$ with p prime not dividing n. Let $A = \langle a, b^{n/k}\rangle$ and let F be the only subfield of $\mathbb{Q}(\zeta_p)$ of degree $\frac{(p-1)k}{n}$. Then the non-commutative simple components of $\mathbb{Q}G$ are the algebras of the form $B_h = \mathbb{Q}Ge(G, A, \langle b^{hn/k}\rangle)$ with $h \mid k$. Moreover $B_h \cong (\mathbb{Q}(\zeta_{ph})/F(\zeta_h), \zeta_h)$ for every $h \mid k$.*

Proof. As $G' = \langle a\rangle$ and A is cyclic and maximal abelian in G, a pair of subgroups of G satisfying the conditions of Theorem 2.1 is either of the form (G, K) with $G' \subseteq K$ or of the form (A, K) with $K \cap G' = 1$. If $G' \subseteq K$ then $\mathbb{Q}Ge(G, G, K)$ is commutative. Hence the lemma follows from Theorem 2.1 and (2.3). □

Proposition 3.2. *If G is one of the groups listed in Theorem 1.1 then G is CSP'-critical. Moreover $\mathbb{Q}G$ has an exceptional component of type* (EC1) *if and only if G is of one of the types* (1)–(3) *and $\mathbb{Q}G$ has an exceptional component of type* (EC2) *if and only if G is of one of the types* (4)–(22).

Proof. (1) Assume that $G = C_q \times (C_p \rtimes_2 C_4) = \langle a\rangle_{pq} \rtimes_2 \langle b\rangle_4$ satisfies the conditions of (1). Let $A = \langle a, b^2\rangle$, a cyclic subgroup of index 2 in G.

Using Theorem 2.1 one can calculate the non-commutative simple components of $\mathbb{Q}G$. They are

$$A_1 = \mathbb{Q}Ge(G, A, 1) \cong \big(\mathbb{Q}(\zeta_{pq})/\mathbb{Q}\big(\zeta_q, \zeta_p + \zeta_p^{-1}\big), -1\big) \cong \left(\frac{(\zeta_p - \zeta_p^{-1})^2, -1}{\mathbb{Q}(\zeta_q, \zeta_p + \zeta_p^{-1})}\right),$$

$$A_2 = \mathbb{Q}Ge\big(G, A, \langle b^2\rangle\big) \cong \big(\mathbb{Q}(\zeta_{pq})/\mathbb{Q}\big(\zeta_q, \zeta_p + \zeta_p^{-1}\big), 1\big) \cong M_2\big(\mathbb{Q}\big(\zeta_q, \zeta_p + \zeta_p^{-1}\big)\big),$$

$$A_3 = \mathbb{Q}Ge\big(G, A, \langle a^p\rangle\big) \cong \big(\mathbb{Q}(\zeta_p)/\mathbb{Q}\big(\zeta_p + \zeta_p^{-1}\big), -1\big) \cong \left(\frac{(\zeta_p - \zeta_p^{-1})^2, -1}{\mathbb{Q}(\zeta_p + \zeta_p^{-1})}\right) \quad \text{and}$$

$$A_4 = \mathbb{Q}Ge\big(G, A, \langle a^p, b^2\rangle\big) \cong \big(\mathbb{Q}(\zeta_p)/\mathbb{Q}\big(\zeta_p + \zeta_p^{-1}\big), 1\big) \cong M_2\big(\mathbb{Q}\big(\zeta_p + \zeta_p^{-1}\big)\big).$$

Observe that $m = pq$, $n = 4$ and $k = 2$ satisfy the conditions of (Z)(c) in Theorem 2.2. Thus G is a subgroup of a division algebra and hence, by Lemma 2.3, $A_1 = \mathbb{Q}(G, \langle a, b^2\rangle)$ is a division ring. It is not totally definite because its centre contains a primitive root of unity of order q. Thus A_1 is an exceptional algebra of type (EC1). However A_3 is a totally definite quaternion algebra because $(\zeta_p - \zeta_p^{-1})^2 < 0$ and A_2 and A_4 are not exceptional because $[\mathbb{Q}(\zeta_p + \zeta_p^{-1}) : \mathbb{Q}] = \frac{p-1}{2} > 2$. On the other hand every non-abelian proper quotient of G is isomorphic to either $C_p \rtimes C_4$, $\mathcal{D}_{2p}$ or $C_q \times \mathcal{D}_{2p}$. The group algebra $\mathbb{Q}(C_p \rtimes C_4)$ has two non-commutative components isomorphic to A_3 and A_4 respectively, the only non-commutative component of $\mathcal{D}_{2p}$ is isomorphic to A_4 and the non-commutative components of $\mathbb{Q}(C_q \times \mathcal{D}_{2p})$ are isomorphic to A_2 and A_4 respectively.

Thus $\mathbb{Q}\overline{G}$ does not have exceptional components for any proper quotient $\overline{G}$ and we conclude that G is CSP'-critical.

(2) Assume that $G = C_p \rtimes_k C_n = \langle a\rangle_p \rtimes_k \langle b\rangle_n$ with p, n and k as in (2), and let $A = \langle a, b^{\frac{n}{k}}\rangle$. The non-commutative simple components of $\mathbb{Q}G$ are the algebras B_h of Lemma 3.1 with $h \mid k$. The degree of B_h is $\frac{n}{k}$. Moreover, $B_h \cong \mathbb{Q}(H_h, A_h)$ with $H_h = G/\langle b^{h\frac{n}{k}}\rangle \cong C_p \rtimes_h C_{\frac{hn}{k}}$ and $A_h = A/\langle b^{h\frac{n}{k}}\rangle$. By Lemma 2.3, B_h is a division algebra if and only if H_h is one of the groups in items (Z)(b) or (Z)(c) in Theorem 2.2. Observe that G satisfies the conditions of (Z)(c) in Theorem 2.2. Hence B_k is a division algebra. If B_k is a totally definite quaternion algebra then $\frac{n}{k} = 2$ and $k = 2$ because the centre of B_k has a root of unity of order k. Hence $n = 4$ in contradiction with the hypothesis. Thus B_k is an exceptional algebra of type (EC1).

Any non-commutative simple component of the rational group algebra of a proper quotient $\overline{G}$ of G is isomorphic to B_h for some proper divisor h of k. So, in order to prove that $\mathbb{Q}\overline{G}$ does not have exceptional components, it is enough to prove that if h is a proper divisor of k then B_h is not exceptional. Assume first that B_h is exceptional of type (EC2). Then $\frac{n}{k}$, which is the degree of B_h, is 2 or 4 and hence n is a power of 2. Moreover the centre of B_h contains the unique subfield F of index $\frac{n}{k}$ in $\mathbb{Q}(\zeta_p)$. Thus either $\frac{n}{k} = 2$ and $F = \mathbb{Q}(\zeta_p + \zeta_p^{-1})$ or $\frac{n}{k} = 4$, $F = \mathbb{Q}$ and $p = 5$. The latter case is in contradiction with the hypothesis and in the former case F is contained in an imaginary quadratic extension of $\mathbb{Q}$ and hence $F = \mathbb{Q}$ and $p = 3$, again in contradiction with the hypothesis. This proves that B_h is not exceptional of type (EC2) and in particular that $\mathbb{Q}G$ does not have exceptional components of type (EC2). Secondly suppose that B_h is exceptional of type (EC1). Then B_h is a division algebra containing H_h and hence H_h is a non-cyclic Z-group. Thus $H_h = C_p \rtimes_h C_{\frac{hn}{k}}$ satisfies either (Z)(b) or (Z)(c). This does not hold if $p \equiv 1 \bmod 4$ because in that case $v_q(h) < v_q(k) = v_q(p-1)$ for some prime $q \mid \frac{hn}{k}$. Similarly, if $\frac{k}{h}$ is divisible by an odd prime q then $v_q(h) < v_q(k) = v_q(p-1)$ and hence H_h is not a Z-group. Thus $p \equiv -1 \bmod 4$ and $\frac{k}{h}$ is a power of 2. If G satisfies (2)(a) or (2)(b) then $v_2(k) = 1$ and hence h is odd. Then H_h does not satisfy the conditions of neither (Z)(b) nor (Z)(c), a contradiction. Thus G satisfies (2)(c). As $v_2(h) < v_2(k) = v_2(p+1) + 1$, H_h only can satisfy the conditions of (Z)(b) or (Z)(c) if $h = 2$. In this case $\frac{hn}{k} = 4$, so that $H_h = C_p \rtimes_2 C_4$. Then $B_h = (\mathbb{Q}(\zeta_p)/\mathbb{Q}(\zeta_p + \zeta_p^{-1}), -1)$, a totally definite quaternion algebra and hence it is not an exceptional component, as desired.

(3) Let $G = \mathcal{Q}_8 \times C_p$ with p an odd prime such that $o_p(2)$ is odd. Then the only non-commutative simple components of $\mathbb{Q}G$ are $\mathbb{H}(\mathbb{Q})$ and $\mathbb{H}(\mathbb{Q}(\zeta_p))$. The first one is a totally definite quaternion algebra and the second one is a division algebra by [8]. Since $\mathbb{Q}(\zeta_p)$ is not totally real, $\mathbb{H}(\mathbb{Q}(\zeta_p))$ is exceptional of type (EC1) and $\mathbb{Q}G$ does not have exceptional components of type (EC2). The only non-abelian proper quotient of G is $G/C_p \cong \mathcal{Q}_8$ and the only non-abelian simple component of $\mathbb{Q}\mathcal{Q}_8$ is $\mathbb{H}(\mathbb{Q})$. This proves that G is CSP'-critical.

To prove that if G is one of the groups in items (4)–(22) of Theorem 1.1 then it has an exceptional component of type (EC2) we will simply calculate the Wedderburn

decomposition of their rational group algebras and will observe that all of them have one component of isomorphic to one of the following algebras:

$$M_2(\mathbb{Q}), M_2\big(\mathbb{Q}(\zeta_4)\big), M_2\big(\mathbb{Q}(\zeta_3)\big), M_2\big(\mathbb{Q}(\sqrt{-2})\big),$$
$$M_2\big(\mathbb{H}(\mathbb{Q})\big), M_2\left(\frac{-1,-3}{\mathbb{Q}}\right), \big(\mathbb{Q}(\zeta_5)/\mathbb{Q}, -1\big). \tag{3.4}$$

The only one which is not obviously exceptional of type (EC2) is $A = (\mathbb{Q}(\zeta_5)/\mathbb{Q}, -1)$. Clearly A is not a division algebra, because its exponent is the order of -1 modulo the image of the norm of $\mathbb{Q}(\zeta_5)$ over $\mathbb{Q}$ [13, Corollary 30.7]. So it is enough to prove that $\mathbb{R} \otimes_{\mathbb{Q}} A$ is not split.

Observe that $A = \mathbb{Q}(G, \langle a\rangle) = \mathbb{Q}Ge(G, \langle a\rangle, 1)$ with $G = \langle a\rangle_5 \rtimes_2 \langle b\rangle_8$. The only irreducible character of G not vanishing in $e(G, \langle a\rangle, 1)$ is $\chi = \lambda^G_{\langle a\rangle,1}$ and it is given by the second and third row of the following table.

1	5	5	1	4	5	5	5	4	5
1	b	b^2	b^4	a	b^3	b^5	b^6	ab^4	b^7
4	0	0	-4	-1	0	0	0	-1	0

The first row gives the cardinality of the corresponding conjugacy class. Having in mind that $\chi(a^2) = \chi(a)$, because a and a^2 are conjugate in G, we can calculate the Frobenius–Schur indicator of χ which is

$$\frac{1}{|G|}\sum_{g\in G}\chi\big(g^2\big) = \frac{1}{20}\big(\chi(1) + 5\big(\chi\big(b^2\big) + \chi\big(b^4\big) + \chi\big(b^6\big)\big) + 4\chi\big(a^2\big)\big) = -1.$$

Therefore, $\mathbb{R} \otimes_{\mathbb{Q}} A$ is not split as desired. Thus $A = M_2(D)$ with D a totally definite quaternion algebra over $\mathbb{Q}$. (It can be proved that $D \cong (\frac{-2,-5}{\mathbb{Q}})$, but this is not relevant for us.)

To compute the Wedderburn components of the group algebras of the groups in items (4)–(22) we use the Wedderga package [3] and obtain the following decompositions:

$$\mathbb{Q}\,\mathrm{SL}(2,3) = \mathbb{Q} \oplus \mathbb{Q}(\zeta_3) \oplus M_3(\mathbb{Q}) \oplus \mathbb{H}(\mathbb{Q}) \oplus M_2\big(\mathbb{Q}(\zeta_3)\big).$$
$$\mathbb{Q}\,\mathrm{SL}(2,5) = \mathbb{Q} \oplus M_4(\mathbb{Q}) \oplus M_5(\mathbb{Q}) \oplus M_3\big(\mathbb{Q}(\sqrt{5})\big) \oplus M_3\big(\mathbb{H}(\mathbb{Q})\big)$$
$$\oplus \big(\mathbb{Q}(\zeta_5)/\mathbb{Q}(\sqrt{5}), -1\big) \oplus M_2\left(\frac{-1,-3}{\mathbb{Q}}\right).$$
$$\mathbb{Q}\mathcal{D}_6 = 2\mathbb{Q} \oplus M_2(\mathbb{Q}).$$
$$\mathbb{Q}\mathcal{D}_8 = 4\mathbb{Q} \oplus M_2(\mathbb{Q}).$$
$$\mathbb{Q}\mathcal{D}^+_{16} = 4\mathbb{Q} \oplus 2\mathbb{Q}(\zeta_4) \oplus M_2\big(\mathbb{Q}(\zeta_4)\big).$$
$$\mathbb{Q}(\mathcal{Q}_8 \rtimes C_2) = 8\mathbb{Q} \oplus M_2\big(\mathbb{Q}(\zeta_4)\big).$$

$$\begin{aligned}
\mathbb{Q}(\mathcal{Q}_8 \times C_3) &= 4\mathbb{Q} \oplus 4\mathbb{Q}(\zeta_3) \oplus \mathbb{H}(\mathbb{Q}) \oplus M_2\big(\mathbb{Q}(\zeta_3)\big).\\
\mathbb{Q}(\mathcal{Q}_8 \curlyvee_2 \mathcal{D}_8) &= 16\mathbb{Q} \oplus M_2\big(\mathbb{H}(\mathbb{Q})\big).\\
\mathbb{Q}(C_5 \rtimes_2 C_8) &= 2\mathbb{Q} \oplus \mathbb{Q}(\zeta_4) \oplus \mathbb{Q}(\zeta_8) \oplus M_4(\mathbb{Q}) \oplus \big(\mathbb{Q}(\zeta_5)/\mathbb{Q}, -1\big).\\
\mathbb{Q}\big(C_3^2 \rtimes_2 C_8\big) &= 2\mathbb{Q} \oplus \mathbb{Q}(\zeta_4) \oplus \mathbb{Q}(\zeta_8) \oplus 2M_4(\mathbb{Q}) \oplus 2M_2\left(\frac{-1,-3}{\mathbb{Q}}\right).\\
\mathbb{Q}\big(\mathrm{SL}(2,3) \curlyvee_2 \mathcal{D}_8\big) &= 4\mathbb{Q} \oplus 4\mathbb{Q}(\zeta_3) \oplus 4M_3(\mathbb{Q})\\
&\quad \oplus M_2\big(\big(\mathbb{Q}(\zeta_{12})/\mathbb{Q}(\zeta_3), -1\big)\big) \oplus M_2\big(\mathbb{H}(\mathbb{Q})\big).\\
\mathbb{Q}\mathcal{C} &= 2\mathbb{Q} \oplus 2\mathbb{Q}(\zeta_3) \oplus 2M_3(\mathbb{Q}) \oplus 2M_4(\mathbb{Q}) \oplus 2M_6(\mathbb{Q}) \oplus 2M_4\big(\mathbb{Q}(\zeta_3)\big)\\
&\quad \oplus M_6\big(\mathbb{H}(\mathbb{Q})\big) \oplus M_2\big(\big(\mathbb{Q}(\zeta_{12})/\mathbb{Q}(\zeta_3), -1\big)\big) \oplus M_2\big(\mathbb{H}(\mathbb{Q})\big).\\
\mathbb{Q}\big(\mathrm{SL}(2,3) \curlyvee_2 C_4\big) &= 2\mathbb{Q} \oplus 2\mathbb{Q}(\zeta_3) \oplus 2M_3(\mathbb{Q}) \oplus M_2\big(\mathbb{Q}(\zeta_{12})\big) \oplus M_2\big(\mathbb{Q}(\zeta_4)\big).\\
\mathbb{Q}\,\mathrm{SL}(2,9) &= \mathbb{Q} \oplus 2M_5(\mathbb{Q}) \oplus M_9(\mathbb{Q}) \oplus M_{10}(\mathbb{Q}) \oplus M_8\big(\mathbb{Q}(\sqrt{5})\big)\\
&\quad \oplus M_4\left(\frac{-1,-3}{\mathbb{Q}(\sqrt{5})}\right) \oplus M_4\left(\frac{-1,-3}{\mathbb{Q}(\sqrt{2})}\right) \oplus 2M_2\left(\frac{-1,-3}{\mathbb{Q}}\right).\\
\mathbb{Q}\mathcal{A}^+ &= 2\mathbb{Q} \oplus 2M_4(\mathbb{Q}) \oplus 2M_5(\mathbb{Q}) \oplus M_6(\mathbb{Q}) \oplus M_4\big(\mathbb{Q}(\zeta_3)\big)\\
&\quad \oplus M_6\big(\mathbb{Q}(\sqrt{-2})\big) \oplus \big(\mathbb{Q}(\zeta_5)/\mathbb{Q}, -1\big).\\
\mathbb{Q}\mathcal{A}^- &= 2\mathbb{Q} \oplus 2M_4(\mathbb{Q}) \oplus 2M_5(\mathbb{Q}) \oplus M_6(\mathbb{Q}) \oplus \big(\mathbb{Q}(\zeta_5, \sqrt{3})/\mathbb{Q}(\sqrt{3}), -1\big)\\
&\quad \oplus M_3\big(\mathbb{Q}(\sqrt{2}) \otimes_{\mathbb{Q}} D\big) \oplus \big(\mathbb{Q}(\zeta_5)/\mathbb{Q}, -1\big),\\
&\quad \text{where } \big(\mathbb{Q}(\zeta_5)/\mathbb{Q}, -1\big) = M_2(D).\\
\mathbb{Q}\mathcal{B}_1 &= \mathbb{Q} \oplus \mathbb{Q}(\zeta_5) \oplus 3M_5(\mathbb{Q}) \oplus M_2\big(\big(\mathbb{Q}(\zeta_{20})/\mathbb{Q}(\zeta_5), -1\big)\big) \oplus M_2\big(\mathbb{H}(\mathbb{Q})\big).\\
\mathbb{Q}\mathcal{B}_2 &= 2\mathbb{Q} \oplus 6M_5(\mathbb{Q}) \oplus M_2\big(\mathbb{Q}(\sqrt{5})\big) \oplus M_4\big(\mathbb{H}\big(\mathbb{Q}(\sqrt{5})\big)\big) \oplus 2M_2\big(\mathbb{H}(\mathbb{Q})\big).\\
\mathbb{Q}\mathcal{B} &= \mathbb{Q} \oplus 2M_5(\mathbb{Q}) \oplus 2M_{10}(\mathbb{Q}) \oplus M_{15}(\mathbb{Q}) \oplus M_5\big(\mathbb{Q}(\zeta_3)\big) \oplus M_{20}(\mathbb{Q})\\
&\quad \oplus M_4(\mathbb{Q}) \oplus M_3\big(\mathbb{Q}(\sqrt{5})\big) \oplus M_8\big(\mathbb{H}(\mathbb{Q})\big) \oplus M_{10}\big(\mathbb{H}(\mathbb{Q})\big)\\
&\quad \oplus M_6\big(\mathbb{H}\big(\mathbb{Q}(\sqrt{5})\big)\big) \oplus M_2\big(\mathbb{H}(\mathbb{Q})\big).
\end{aligned}$$

As we anticipated above each decomposition has one component of one of the types in (3.4). Moreover no simple component is exceptional of type (EC1).

To complete the proof it remains to prove that if G is one of the groups in items (4)–(22) of Theorem 1.1 and H is a proper epimorphic image of G then $\mathbb{Q}H$ does not have exceptional components. Some of these groups G do not have any non-abelian proper quotient and hence there is nothing to prove for them. The remaining groups G and their proper quotients H are listed in Table 2 (second and third columns respectively). We have to check that $\mathbb{Q}H$ does not have exceptional components for each H in the third column of Table 2. We do not need to consider the groups H which are a proper quotient of another group K in the third column because the simple components of $\mathbb{Q}H$ are also simple components of $\mathbb{Q}K$. This excludes $A_4, A_5, \mathcal{C}/Z(\mathcal{Q}_8 \times \mathcal{Q}_8)$ and $\mathcal{D}_{10}$.

Table 2
The non-abelian proper quotients of some of the CSP'-groups of types (4)–(22).

#	G	H
(4)	$\mathrm{SL}(2,3)$	$\mathrm{PSL}(2,3) \cong A_4$
(5)	$\mathrm{SL}(2,5)$	$\mathrm{PSL}(2,5) \cong A_5$
(10)	$\mathcal{Q}_8 \times C_3$	$\mathcal{Q}_8$
(12)	$C_5 \rtimes_2 C_8$	$C_5 \rtimes C_4$
(13)	$(C_3 \times C_3) \rtimes_2 C_8$	$(C_3 \times C_3) \rtimes C_4$
(14)	$\mathrm{SL}(2,3) \curlyvee_2 \mathcal{D}_8$	$A_4, C_2 \times A_4$
(15)	$\mathcal{C}$	$A_4, C_2 \times A_4, \mathcal{C}/Z(\mathcal{C}), \mathcal{C}/Z(\mathcal{Q}_8 \times \mathcal{Q}_8)$
(16)	$\mathrm{SL}(2,3) \curlyvee_2 C_4$	$A_4, C_2 \times A_4$
(17)	$\mathrm{SL}(2,9)$	$\mathrm{PSL}(2,9)$
(18)	$\mathcal{A}^+$	S_5
(19)	$\mathcal{A}^-$	S_5
(20)	$\mathcal{B}_1$	$\mathcal{B}_1/Z(\mathcal{B}_1)$
(21)	$\mathcal{B}_2$	$\mathcal{D}_{10}, \mathcal{B}_2/Z(\mathcal{B}_2)$
(22)	$\mathcal{B}$	$A_5, \mathcal{B}/Z(\mathcal{B}) = C_2^4 \rtimes A_5$

Moreover, $\mathbb{Q}(C_2 \times H) \cong \mathbb{Q}C_2 \otimes_{\mathbb{Q}} \mathbb{Q}H = 2\mathbb{Q}H$ and hence do not need to consider the groups of the form $C_2 \times H$. Hence we have only to verify that the following Wedderburn decomposition do not have exceptional components:

$$\begin{aligned}
\mathbb{Q}\mathcal{Q}_8 &= 4\mathbb{Q} \oplus \mathbb{H}(\mathbb{Q}).\\
\mathbb{Q}(C_5 \rtimes C_4) &= 2\mathbb{Q} \oplus \mathbb{Q}(\zeta_4) \oplus M_4(\mathbb{Q}).\\
\mathbb{Q}\big((C_3 \times C_3) \rtimes C_4\big) &= 2\mathbb{Q} \oplus \mathbb{Q}(\zeta_4) \oplus 2M_4(\mathbb{Q}).\\
\mathbb{Q}\big(\mathcal{C}/Z(\mathcal{C})\big) &= 2\mathbb{Q} \oplus 2\mathbb{Q}(\zeta_3) \oplus 2M_3(\mathbb{Q}) \oplus 2M_4(\mathbb{Q}) \oplus 2M_6(\mathbb{Q}) \oplus 2M_4\big(\mathbb{Q}(\zeta_3)\big).\\
\mathbb{Q}\,\mathrm{PSL}(2,9) &= \mathbb{Q} \oplus 2M_5(\mathbb{Q}) \oplus M_9(\mathbb{Q}) \oplus M_{10}(\mathbb{Q}) \oplus M_8\big(\mathbb{Q}(\sqrt{5}\,)\big).\\
\mathbb{Q}S_5 &= 2\mathbb{Q} \oplus 2M_4(\mathbb{Q}) \oplus 2M_5(\mathbb{Q}) \oplus M_6(\mathbb{Q}).\\
\mathbb{Q}\big(\mathcal{B}_1/Z(\mathcal{B}_1)\big) &= \mathbb{Q} \oplus \mathbb{Q}(\zeta_5) \oplus 3M_5(\mathbb{Q}).\\
\mathbb{Q}\big(\mathcal{B}_2/Z(\mathcal{B}_2)\big) &= 2\mathbb{Q} \oplus 6M_5(\mathbb{Q}) \oplus M_2\big(\mathbb{Q}(\sqrt{5}\,)\big).\\
\mathbb{Q}\big(\mathcal{B}/Z(\mathcal{B})\big) &= \mathbb{Q} \oplus 2M_5(\mathbb{Q}) \oplus 2M_{10}(\mathbb{Q}) \oplus M_{15}(\mathbb{Q}) \oplus M_5\big(\mathbb{Q}(\zeta_3)\big)\\
&\quad \oplus M_{20}(\mathbb{Q}) \oplus M_4(\mathbb{Q}) \oplus M_3\big(\mathbb{Q}(\sqrt{5}\,)\big).
\end{aligned}$$

This finishes the proof of the proposition. □

4. Necessity

In this section we prove the necessity part of Theorem 1.1. More precisely, throughout we assume that G is a finite CSP'-critical group and we prove that G is one of the groups

listed in Theorem 1.1. Since we have already proved that the groups in the theorem are CSP'-critical and, in particular, they have an exceptional component, we have

(P1) No proper quotient of G is isomorphic to one of the groups in Theorem 1.1.

As G is CSP'-critical, $\mathbb{Q}G$ has at least one exceptional component. Let A be any exceptional component of $\mathbb{Q}G$ and let $f : G \to \mathcal{U}(A)$ be the group homomorphism induced by the projection $\mathbb{Q}G \to A$. Then A is a simple exceptional component of $\mathbb{Q}(G/\ker f)$ and hence f is injective. Thus

(P2) G is embedded in one (all) exceptional component(s) of $\mathbb{Q}G$.

Definition 4.1. Let G be a finite subgroup of $\mathrm{GL}_2(D)$ where D is a division algebra of characteristic zero. One says that G is primitive in $M_2(D)$ if there is no non-singular 2×2 matrix A over D such that AgA^{-1} is monomial (i.e. every column and row has exactly one non-zero entry) for all $g \in G$. Otherwise one says that G is imprimitive.

We consider separately the following cases:

- G is a subgroup of a division ring (Proposition 4.2).
- G is not a subgroup of a division ring and G is metabelian (Proposition 4.4).
- G is not a subgroup of a division ring, G is not metabelian and G is an imprimitive subgroup of an exceptional component of $\mathbb{Q}G$ (necessarily of type (EC2)) (Proposition 4.9).
- G does not satisfy any of the previous conditions (Proposition 4.10). In particular, G is not metabelian and it is a primitive subgroup of an exceptional component of type (EC2).

The following proposition proves Theorem 1.1 for the case when G is a subgroup of a division ring.

Proposition 4.2. *Let G be a CSP'-critical group which can be embedded in a division ring. Then G is isomorphic to one of the groups in items* (1)–(5) *of Theorem 1.1.*

Proof. By the hypothesis G is one of the groups in Theorem 2.2. Assume first that G is not a Z-group, that is G satisfies one of the conditions (a)–(e) of (NZ). First, G is not of type (NZ)(a) because $\mathcal{O}^* = \langle s, t | (st)^2 = s^3 = t^4 \rangle$ and $\mathcal{O}^*/\langle t^2, (s, t^2) \rangle \cong \mathcal{D}_6$, in contradiction with (P1). If G is of type (NZ)(e) then $G \cong \mathrm{SL}(2, 5)$, that is G is as in item (5) of Theorem 1.1. By (P1), if G is of type (NZ)(d) then $G \cong \mathrm{SL}(2, 3)$, thus G is as in item (4) of Theorem 1.1.

We now prove that G is not of type (NZ)(b). Suppose that $G = \mathcal{Q}_m = \langle j \rangle \leftthreetimes_{\frac{m}{2}} \rtimes_2 C_4$ with $t = v_2(m) \geqslant 3$. If $t \geqslant 3$ then $G/\langle j^4 \rangle \cong \mathcal{D}_8$ in contradiction with (P1). If $3 \mid m$ then

$G/\langle j^3\rangle \cong \mathcal{D}_6$ in contradiction with (P1). Hence $t = 3$ and $3 \nmid m$. Moreover $A = \langle j\rangle$ is a maximal abelian subgroup of index 2 in G and $G' = \langle j^2\rangle$. Thus, by Theorem 2.1, the non-commutative simple components of $\mathbb{Q}G$ are of the form $\mathbb{Q}Ge(G, A, \langle j^d\rangle)$ with $d \mid \frac{m}{2}$ and $d \neq 1, 2$. Then

$$\mathbb{Q}Ge\big(G, A, \langle j^d\rangle\big) \cong \begin{cases} (\mathbb{Q}(\zeta_d)/\mathbb{Q}(\zeta_d + \zeta_d^{-1}), 1) \cong M_2(\mathbb{Q}(\zeta_d + \zeta_d^{-1})), & \text{if } d \mid \frac{m}{4}; \\ (\mathbb{Q}(\zeta_d)/\mathbb{Q}(\zeta_d + \zeta_d^{-1}), -1) \cong \mathbb{H}(\mathbb{Q}(\zeta_d + \zeta_d^{-1})), & \text{otherwise.} \end{cases}$$

None of these algebras is exceptional (the former because $d \neq 1, 2, 3, 4$ or 6 and the latter because it is a totally definite quaternion algebra). This yields a contradiction.

Assume that G is of type (NZ)(c), i.e. $G = \mathcal{Q}_8 \times M$, with M a Z-group of odd order $m > 1$ and $o_m(2)$ is odd. We claim that m is prime. As G is a subgroup of a division algebra D, the subalgebra D_1 of D generated by M is a division algebra which appears in the Wedderburn decomposition of $\mathbb{Q}M$. As M is a proper quotient of G, D_1 is not an exceptional component and hence the degree of D_1 is at most 2. However, since the order of M is odd the degree of D_1 is odd. Thus M is abelian. Then $M = C_n \times N$ for some subgroup N and some integer $n > 1$. If p is a divisor of n then M has a subgroup K of index p and $o_p(2)$ is odd. Then $G/K \cong \mathcal{Q}_8 \times C_p$. By (P1) we deduce that $K = 1$ and hence $m = p$, as desired. We conclude that $G = \mathcal{Q}_8 \times C_p$ with p an odd prime such that $o_p(2)$ is odd. Thus G is the group of item (3) of Theorem 1.1. This finishes the case when G is not a Z-group.

Suppose now that G is a CSP'-critical Z-group. Hence G is of type (Z)(b) or (Z)(c). We first prove that G is not of type (Z)(b). Otherwise $G = \langle a\rangle_m \rtimes_2 \langle b\rangle_4$ with m odd and b acting by inversion. If $3 \mid m$ then $G/\langle a^3, b^2\rangle \cong \mathcal{D}_6$, in contradiction with (P1). Thus $3 \nmid m$. Moreover, $A = \langle a, b^2\rangle$ is a maximal abelian subgroup of G of index 2 and $G' = \langle a\rangle$. Using Theorem 2.1, we have that every non-commutative simple component of $\mathbb{Q}G$ is of the form $\mathbb{Q}Ge(G, A, B)$ with B a subgroup of A not containing a. Fix such B and assume that $k = [A : B]$. By (2.3), $\mathbb{Q}Ge(G, A, B) = (\mathbb{Q}(\zeta_k)/\mathbb{Q}(\zeta_k + \zeta_k^{-1}), \epsilon)$ with $\epsilon = 1$ if $b^2 \in B$ and $\epsilon = -1$ if $b^2 \notin B$. In the second case $\mathbb{Q}Ge(G, A, B)$ is a totally definite quaternion algebra. In the first case $\mathbb{Q}Ge(G, A, B) = M_2(\mathbb{Q}(\zeta_k + \zeta_k^{-1}))$ which is not exceptional because k is divisible by a prime $p > 3$. Therefore $\mathbb{Q}G$ does not have any exceptional component, contradicting the hypothesis.

It remains to consider type (Z)(c). So suppose that $G = C_m \rtimes_k C_n$ satisfies the hypothesis of (Z)(c) and recall that the Sylow p-subgroup of C_m is denoted P_p and the Sylow p-subgroup of C_n is denoted Q_p. Let p be a prime divisor of m such that C_n does not act trivially on P_p. Let $q_1, \dots, q_h$ be the prime divisors q of n such that Q_q acts non-trivially on P_p and recall that $R_p = Q_{q_1} \cdots Q_{q_h}$. Let k_p be the order of the kernel of the action of R_p on P_p. Then $P_p \rtimes_{k_p} R_p$ is a direct factor of G and a subgroup of a division algebra of degree $\frac{|R_p|}{k_p}$ (see Lemma 2.3). This division algebra is an exceptional component unless $\frac{|R_p|}{k_p} = 2$. Therefore, since G is CSP'-critical, if $G \neq P_p \rtimes_{k_p} R_p$ then $\frac{|R_p|}{k_p} = 2$. This only can happen for one prime p, because Q_2 acts non-trivially on at most

one Sylow p-subgroup of C_m. This shows that $C_m = C_{m_0} \times P_p$ and $G = C_{m_0} \times (P_p \rtimes_k C_n)$ with $k = k_p$, $C_n = R_p = \langle b \rangle$ and $P_p = \langle a \rangle_{p^\alpha}$. Then $A = C_{m_0} \times \langle a, b^{n_p/k_p} \rangle$ is a cyclic normal subgroup and a maximal abelian subgroup of G. Hence $(A, 1)$ is a strong Shoda pair of G and hence $\mathbb{Q}(G, A, 1)$ is a simple component of $\mathbb{Q}G$ isomorphic to $\mathbb{Q}(G, A)$. Moreover, by Lemma 2.3, $\mathbb{Q}(G, A)$ is a division algebra of degree $\frac{n}{k}$.

We claim that $\alpha = 1$. Otherwise $\overline{G} = G/\langle a^{p^{\alpha-1}} \rangle$ satisfies the conditions of (Z)(c) and therefore $\mathbb{Q}(\overline{G}, \overline{A})$ is a division ring of degree $\frac{n}{k}$ which is a component of $\mathbb{Q}\overline{G}$. By assumption, $\mathbb{Q}(\overline{G}, \overline{A})$ has to be a totally definite quaternion algebra. Thus $n = 2k$, and the action of $\langle b \rangle$ on $\langle a \rangle$ is the only one of order 2, i.e. $a^b = a^{-1}$. Moreover, as the centre of $\mathbb{Q}(\overline{G}, \overline{A})$ contains $\mathbb{Q}(\zeta_{m_0 k})$ and m_0 is odd, necessarily $m_0 = 1$ and $k \leqslant 2$. However, the hypothesis of (Z)(c) implies that $k \neq 1$ and thus $k = 2$. Then G is as in case (Z)(b) which we have already excluded. This concludes the proof of the claim.

Suppose that $m_0 \neq 1$. Then $\langle a \rangle_p \rtimes_k \langle b \rangle_n$ is a non-commutative proper quotient of G and its rational group algebra has a simple component of degree $\frac{n}{k}$. The argument of the previous paragraph shows that $n = 4$, $k = 2$ and $a^b = a^{-1}$. A similar argument, now factoring by a subgroup of C_{m_0}, shows that m_0 is prime. Applying the conditions in (Z)(c) for $q = 2$ we have $v_2(o_{m_0}(p)) < o_2(p) = 1$ or equivalently $o_{m_0}(p)$ is odd. If $p = 3$ then $\mathcal{D}_6$ is a proper epimorphic image of G in contradiction with (P1). Moreover, if $p \equiv 1 \bmod 4$ then $1 = v_2(k) \geqslant v_2(p-1) \geqslant 2$, another contradiction. Thus $3 \neq p \equiv -1 \bmod 4$. We have proved that G satisfies the conditions of item (1) in Theorem 1.1 (with $q = m_0$).

Finally, suppose that $m_0 = 1$. Then $G = \langle a \rangle_p \rtimes_k \langle b \rangle_n$, $A = \langle a, b^{\frac{n}{k}} \rangle$ and every Sylow subgroup of $\langle b \rangle$ acts non-trivially on $\langle a \rangle$. Hence, if q is a prime divisor of n then $1 \leqslant v_q(\frac{n}{k}) \leqslant v_q(p-1) \leqslant v_q(k)$. In particular, $v_q(n) \geqslant 2$ and hence either $n = 4$ and $G = C_p \rtimes_2 C_4$ or $n \geqslant 8$. However in the first case G satisfies (Z)(b) which was excluded before. Thus $n \geqslant 8$. Suppose that $p \equiv 1 \bmod 4$. Then, by the hypothesis on (Z)(c), $v_q(p-1) \leqslant v_q(k)$ for every prime divisor q of n. Therefore $\gcd(n, p-1)$ divides k. By means of contradiction, suppose that $\gcd(n, p-1) \neq k$. Then $v_q(p-1) < v_q(k)$ for some prime divisor q of n. Let C be the subgroup of order q of $\langle b \rangle$ and $\overline{G} = G/C$. Then $1 \neq C \subseteq Z(G)$, $\overline{G} = C_p \rtimes_{\frac{k}{q}} C_{\frac{k}{q}}$, $(\overline{A}, 1)$ is a strong Shoda pair of $\overline{G}$ and $\mathbb{Q}(\overline{G}, \overline{A}) = \mathbb{Q}(G, A)$ is a simple component of $\mathbb{Q}\overline{G}$. Then $\overline{G}$ also satisfies the assumptions of (Z)(c), since $v_q(p-1) \leqslant v_q(\frac{k}{q})$. By Lemma 2.3, $\mathbb{Q}(G, A)$ is a non-commutative division algebra of degree $\frac{n}{k}$. Therefore $n = 2k$, the centre of this algebra is a totally real field containing $\mathbb{Q}(\zeta_k)$ and $k > 2$ because $v_2(k) \geqslant v_2(p-1) \geqslant 2$. This yields a contradiction. Hence $k = \gcd(n, p-1)$. If $p = 5$ then $\frac{n}{k}$ divides 4 and hence n is a power of 2. Then $k = 4$ and n is either 8 or 16. If $n = 16$ then G has an epimorphic image isomorphic to $C_5 \rtimes_2 C_8$ in contradiction with (P1). Thus $n = 8$ and G satisfies the conditions of (2)(a) in Theorem 1.1.

Assume that $p \equiv -1 \bmod 4$. Since $\frac{n}{k}$ divides $p-1$, if n is even then $v_2(k) = v_2(n) - 1$. Moreover, $v_q(p-1) \leqslant v_q(k)$ for every odd prime divisor q of n and if 2 divides n then either $v_2(k) = 1$ or $v_2(k) > v_2(p+1)$. If $v_q(p-1) < v_q(k)$ for some odd prime divisor of n or $v_2(p+1) + 1 < v_2(k)$ then the argument of the previous paragraph yields a contradiction. Thus $v_q(p-1) = v_q(k)$ if q is an odd prime divisor of n and if n is

even then $v_2(k)$ is either 1 or $v_2(p+1)+1$. If n is odd then $k = \gcd(p-1, n)$ and G satisfies the conditions of (2)(a) in Theorem 1.1. Assume otherwise that $n = 2^v n_1$, with $v \geqslant 1$ and $2 \nmid n_1$. If $v_2(k) = 1$ then $k = \gcd(p-1, n)$ and $v_2(n) = 2$. So G verifies the conditions of (2)(b). Suppose $k = 2^{v-1}\gcd(p-1, n_1)$ with $v = v_2(p+1)+2$. Hence $v \geqslant 4$. Let $\overline{G} = G/\langle b^{2^{v-2}}\rangle = C_p \rtimes_{2\gcd(p-1,n_1)} C_{4\gcd(p-1,n_1)}$. Then $\overline{G}$ satisfies the conditions of (Z)(c). Hence $\mathbb{Q}(\overline{G}, \overline{A})$ is a division algebra of degree $2\gcd(p-1, n_1)$ in the Wedderburn decomposition of $\mathbb{Q}\overline{G}$. By hypothesis $\mathbb{Q}(\overline{G}, \overline{A})$ is a totally definite quaternion algebra. Then $\gcd(p-1, n_1) = 1$ and $n_1 \mid m_0 = 1$. Hence $n = 2^{v_2(p+1)+2}$ and $k = 2^{v_2(p+1)+1}$. Thus, G satisfies the conditions of (2)(c) of Theorem 1.1. This finishes the proof. □

In order to prove Theorem 1.1 for the metabelian groups not covered by Proposition 4.2 we start describing the SSP exceptional components of type (EC2).

Proposition 4.3. *Let (H, K) be a strong Shoda pair of G such that $\lambda_{H,K}^G$ is faithful and let $A = \mathbb{Q}Ge(G, H, K)$ and $N = N_G(K)$. If A is an exceptional component of type* (EC2) *then one of the following conditions holds*:

(1) $A \cong M_2(\mathbb{Q})$ *and* $G \cong \mathcal{D}_m$ *with* $m = 6, 8$ *or* 12.
(2) $A \cong M_2(\mathbb{Q}(\zeta_4))$ *and one of the following conditions holds*:
  (a) *Either* $G \cong \mathcal{D}_{16}^+$, *or* $G \cong C_4 \times \mathcal{D}_6$, *or* $G \cong C_3 \rtimes_4 C_8$.
  (b) $[H : K] = 4$, $[G : H] = 2$, $N = H$ *and* $|K| \in \{2, 4\}$.
(3) $A = M_2(\mathbb{Q}(\sqrt{-2}))$ *and* $G \cong \mathcal{D}_{16}^-$.
(4) $A \cong M_2(\mathbb{Q}(\zeta_3))$ *and one of the following conditions holds*:
  (a) $G \cong C_3 \times \mathcal{D}_8$ *or* $G \cong C_3 \times \mathcal{Q}_8$.
  (b) $[G : H] = 2$, $N = H$, $[H : K] = 3$ *or* 6 *and* $1 \neq |K| \mid [H : K]$.
(5) $A \cong (\mathbb{Q}(\zeta_5)/\mathbb{Q}, -1)$ *and* $G = C_5 \rtimes_2 C_8$.
(6) $A \cong M_2(\mathbb{H}(\mathbb{Q}))$ *and one of the following conditions holds*:
  (a) $G = \langle i, j\rangle_{\mathcal{Q}_{16}} \rtimes \langle a\rangle_2$ *with* $j^a = j^3$ *and* $i^a = i$.
  (b) $[G : N] = 2$, $[H : K] = 4$, $N/K \cong \mathcal{Q}_8$ *and* $|K| \in \{2, 4\}$.
(7) $A \cong M_2(\frac{-1,-3}{\mathbb{Q}})$, $[G : N] = 2$, $[H : K] = 6$, $N/K \cong \mathcal{Q}_{12}$ *and* $1 \neq |K| \mid [H : K]$.
(8) $K = 1$, $|H| = 12$ *and* G/H *is elementary abelian of order* 4.

In particular, $|G| \in \{6, 8, 12, 16, 18, 24, 32, 36, 40, 48, 64, 72, 144\}$.

Proof. Let $n = [G : N]$, $k = [H : K]$, and $F = Z(A)$. By (2.3), $A \cong M_n(\mathbb{Q}(\zeta_k) *_\tau^\alpha N/H)$ and α is faithful. Hence the degree of A is $[G : H]$ and $[\mathbb{Q}(\zeta_k) : F] = [N : H]$. Thus

$$\varphi(k) = \big[\mathbb{Q}(\zeta_k) : \mathbb{Q}\big] = [N : H][F : \mathbb{Q}]. \tag{4.5}$$

Since A is an exceptional component of type (EC2), either $[G : H] = 2$ and $D = \mathbb{Q}$ or $[G : H] = 2$ and D is a quadratic imaginary extension of $\mathbb{Q}$, or $[G : H] = 4$, $n \leqslant 2$ and

D is a totally definite quaternion algebra over $\mathbb{Q}$. Moreover $\mathrm{Core}_G(K) = \ker \lambda^G_{H,K} = 1$. So, if $K = 1$ then $N = G \neq H$ and otherwise $[G : N] = 2$ and $K \cap K^g = 1$ for each $g \in G \setminus N$. In both cases $N \trianglelefteq G$. Thus $K^g \leqslant N$ and $|K|$ divides $[N : K]$. We consider separately the following cases:

(A) $K = 1$, $[G : H] = 2$ and $F = \mathbb{Q}$. Then $G = N$ and $A = M_2(\mathbb{Q})$.
(B) $K = 1$, $[G : H] = 2$ and $F \neq \mathbb{Q}$. Then $G = N$, F is an imaginary quadratic extension of $\mathbb{Q}$ and $A = M_2(F)$.
(C) $K = 1$ and $[G : H] = 4$. Then $G = N$, $F = \mathbb{Q}$ and $A = M_2(D)$ with D a totally definite quaternion algebra over $\mathbb{Q}$.
(D) $K \neq 1$ and $[N : H] = 2$. Then $[G : N] = 2$, $F = \mathbb{Q}$ and $A = M_2(D)$ with D a totally definite quaternion algebra over $\mathbb{Q}$.
(E) $K \neq 1$, $N = H$ and $F = \mathbb{Q}$. Then $[G : H] = 2$ and $A = M_2(\mathbb{Q})$.
(F) $K \neq 1$, $N = H$ and $F \neq \mathbb{Q}$. Then $[G : H] = 2$, F is an imaginary quadratic extension of $\mathbb{Q}$ and $A = M_2(F)$.

(A) In this case H is a cyclic subgroup of order k and index 2 in G. Moreover, (4.5) reads $\varphi(k) = 2$. Hence either $G = \mathcal{D}_{2k}$ with $k = 3, 4$ or 6 or $G = \mathcal{Q}_{2k}$ with $k = 4$ or 6. However the only non-commutative simple component of $\mathbb{Q}\mathcal{Q}_8$ is isomorphic to $\mathbb{H}(\mathbb{Q})$ and if $G = \mathcal{Q}_{12}$ then $A = (\frac{-1,-3}{\mathbb{Q}})$. ($\mathbb{Q}\mathcal{Q}_{12}$ has also an SSP simple component $\mathbb{Q}\mathcal{Q}_{12}e(\mathcal{Q}_{12}, \langle j\rangle, \langle j^3\rangle) \cong M_2(\mathbb{Q})$ coming from the strong Shoda pair $(\langle j\rangle, \langle j^3\rangle)$ but $\lambda^{\mathcal{Q}_{12}}_{\langle j\rangle,\langle j^3\rangle}$ is not faithful.) Thus G satisfies the conditions of (1).

(B) In this case (4.5) reads $\varphi(k) = 4$. Hence $k = 5, 10, 8$ or 12. Moreover, F is an imaginary quadratic extension of $\mathbb{Q}$ contained in $\mathbb{Q}(\zeta_k)$ and this excludes the cases $k = 5$ and 10. Therefore either $k = 8$ and $F \subseteq \mathbb{Q}(\zeta_8)$ or $k = 12$ and $F \subseteq \mathbb{Q}(\zeta_{12})$. Let a be a generator of H and let $b \in G \setminus H$. Then $G = \langle a, b\rangle$, $a^b = a^i$ and $b^2 = a^j$ with $i = -1, 5$ or -5 and $k \mid j(i-1)$. However, if $i = -1$ then $F = \mathbb{Q}(\zeta_k + \zeta_k^{-1})$, a real quadratic extension of $\mathbb{Q}$, contradicting the assumptions.

Assume that $k = 8$. If $i = 5$ then $F = \mathbb{Q}(\zeta_4)$, j is even and $(a^{\frac{j}{2}}b)^2 = 1$. Replacing b by $a^{\frac{j}{2}}b$ one may assume that $b^2 = 1$. Then $G \cong \mathcal{D}^+_{16}$ and the conditions of (2)(a) hold. If $i = -5$ then $F = \mathbb{Q}(\sqrt{-2})$, $4 \mid j$ and $(a^{\frac{j}{4}}b)^2 = 1$. Again one may assume that $b^2 = 1$. Now $G \cong \mathcal{D}^-_{16}$ and the conditions of (3) hold.

Assume that $k = 12$. Suppose that $i = 5$. Then $F = \mathbb{Q}(\zeta_4)$ and $3 \mid j$. If $6 \mid j$ then, $(a^{-\frac{j}{6}}b)^2 = 1$ and we may assume that $b^2 = 1$. Then $G = C_4 \times \mathcal{D}_6$ and G satisfies the conditions of (2)(a). Otherwise, we may assume that $b^2 = a^3$. Then $G = \langle a^4\rangle \rtimes_4 \langle b\rangle_8 = C_3 \rtimes_4 C_8$ and G satisfies the conditions of (2)(a). Suppose that $i = -5$. Then $F = \mathbb{Q}(\zeta_3)$, $2 \mid j$ and $(a^{-\frac{j}{2}}b)^2 = a^{3j}$. By changing b one may assume that $b^2 = 1$ or $b^2 = a^6$. In the first case $G = C_3 \times \mathcal{D}_8$ and in the second case $G = C_3 \times \mathcal{Q}_8$. Thus G satisfies the conditions of (4)(a).

(C) Again in this case $\varphi(k) = 4$ and hence $k = 5, 10, 8$ or 12. Moreover $N/H \cong \mathrm{Gal}(\mathbb{Q}(\zeta_k)/\mathbb{Q})$. If $k = 5$ then $G = C_5 \rtimes C_4$ and $\mathbb{Q}G \cong 2\mathbb{Q} \oplus \mathbb{Q}(i) \oplus M_4(\mathbb{Q})$, which does not have any exceptional component. Thus $k \neq 5$. If $k = 10$ then $G = C_{10} \rtimes C_4 =$

$C_2 \times (C_5 \rtimes C_4)$ or $G = C_{10} \natural_2 C_4 = C_5 \rtimes_2 C_8$. However $\mathbb{Q}(C_2 \times (C_5 \rtimes C_4)) = 2\mathbb{Q}(C_5 \rtimes C_4)$ does not have any exceptional component. Then $G = C_5 \rtimes_2 C_8$ and the unique exceptional component of $\mathbb{Q}G$ is $(\mathbb{Q}(\zeta_5)/\mathbb{Q}, -1)$. Thus G satisfies the conditions of (5).

Assume that $k = 8$. Then $G = \langle j, i, a\rangle$ with $|j| = 8$, $j^i = j^{-1}$, $j^a = j^3$, $i^2, a^2, (i,a) \in \langle j^4\rangle$ and $(ia)^2 \in \langle j^2\rangle$. If $a^2 = j^4$ then $(aj)^2 = 1$ and hence we may assume that $a^2 = 1$. Suppose that $i^2 = j^{4x}$ and $(ia)^2 = j^{2y}$. Then $(i,a) = i^{-2}(ia)^2 = j^{4x+2y}$. Thus $i^a = ij^{4x+2y} = j^{4x-2y}i$. Therefore $(j^{y-2x}i)^a = j^{y-2x}i$. Thus replacing i by $j^{y-2x}i$ we may assume that $(i,a) = 1$. If $i^2 = 1$ then $G \cong \mathcal{D}_{16} \rtimes C_2 = \langle i, j\rangle_{\mathcal{D}_{16}} \rtimes \langle a\rangle$ and if $i^2 = j^4$ then $G \cong \mathcal{Q}_{16} \rtimes C_2 = \langle i, j\rangle_{\mathcal{Q}_{16}} \rtimes \langle a\rangle$. In both cases, $|j| = 8$, $j^a = j^3$ and $(i,a) = 1$. Using Wedderga we obtain

$$\mathbb{Q}(\mathcal{D}_{16} \rtimes C_2) = 8\mathbb{Q} \oplus 2M_2(\mathbb{Q}) \oplus M_4(\mathbb{Q}).$$

$$\mathbb{Q}(\mathcal{Q}_{16} \rtimes C_2) = 8\mathbb{Q} \oplus 2M_2(\mathbb{Q}) \oplus M_2\big(\mathbb{H}(\mathbb{Q})\big).$$

Therefore $G = \mathcal{Q}_{16} \rtimes C_2$, $A = M_2(\mathbb{H}(\mathbb{Q}))$ and G satisfies (6)(a).

If $k = 12$ then the conditions of (8) hold.

(D) In this case, $|K|$ divides $[N : K] = 2k$. Thus $|G|$ divides $8k^2$. Moreover $(\overline{H} = H/K, \overline{K} = 1)$ is a strong Shoda pair of $\overline{N} = N/K$ satisfying the conditions of (A) (with G, H and K replaced by $\overline{N}, \overline{H}$ and $\overline{K}$ respectively), except that now $\mathbb{Q}Ge(\overline{N}, \overline{H}, \overline{K})$ is a totally definite algebra over $\mathbb{Q}$. By the calculations in case (A), $\overline{N} = \mathcal{Q}_{2k}$ with $k = 4$ or 6. In the first case $A = M_2(\mathbb{H}(\mathbb{Q}))$, so G satisfies the conditions of (6)(b). In the second case $A = M_2(\frac{-1,-3}{\mathbb{Q}})$ and G satisfies the conditions of (7).

(E) In this case (4.5) reads $\varphi(k) = 1$, and hence $k = 2$. Moreover $|K|$ divides $[H : K] = k$ and hence $|K| = 2$ and $|G| = 8$. Since $\mathcal{Q}_8$ does not have any exceptional component, $G \cong \mathcal{D}_8$. Therefore G satisfies (1).

(F) Arguing as the previous case we deduce that $\varphi(k) = 2$. Hence $k = 3$, 4 or 6, $F = \mathbb{Q}(\zeta_k)$ and $|K|$ divides k. Hence either $k = 4$ and $A = M_2(\mathbb{Q}(\zeta_4))$ or $k = 3$ or 6 $A \cong M_2(\mathbb{Q}(\zeta_3))$. In the first case G satisfies (2)(b) and in the second case it satisfies (4)(b). □

The following proposition classifies the metabelian CSP'-critical groups not included in Proposition 4.2.

Proposition 4.4. *The following conditions are equivalent for a finite group G.*

(1) *G is CSP'-critical, it is not a subgroup of a division ring and $\mathbb{Q}G$ has an exceptional SSP component of type* (EC2).
(2) *G is metabelian and CSP'-critical, it is not a subgroup of a division ring and $\mathbb{Q}G$ has an exceptional component of type* (EC2).
(3) *G is one of the groups in items* (6)–(13) *of Theorem 1.1.*

Proof. (3) implies (2). Let G be one of the groups of types (6)–(13) from Theorem 1.1. Clearly G is metabelian. By Proposition 3.2, G is CSP'-critical. Moreover, in all the cases $\mathbb{Q}G$ has an exceptional component of type (EC2) (see Table 1). It remains to prove that G is not a subgroup of a division ring. Otherwise, one of the simple components of $\mathbb{Q}G$ is a division ring containing G as a spanning set over $\mathbb{Q}$. We have calculated the Wedderburn decomposition of $\mathbb{Q}G$ for all the groups G in the proof of Proposition 3.2. The only non-commutative division algebra occurring in one of these Wedderburn decompositions is $\mathbb{H}(\mathbb{Q})$ in the Wedderburn decomposition of $\mathbb{Q}(\mathcal{Q}_8 \times C_3)$. However $\mathcal{Q}_8 \times C_3$ cannot be contained as a spanning set of $\mathbb{H}(\mathbb{Q})$ over $\mathbb{Q}$ because the centre of $\mathbb{H}(\mathbb{Q})$ does not have elements of order 3.

(2) implies (1) is a direct consequence of the fact that every metabelian group is strongly monomial (Theorem 2.1).

(1) implies (3). We use the notation of Proposition 4.3. Suppose that G is CSP'-critical and (H, K) is a strong Shoda pair of G such that $A = \mathbb{Q}Ge(G, H, K)$ is an exceptional component of type (EC2). Then $\lambda^G_{H,K}$ is a faithful character of G, because A is also a simple component of $\mathbb{Q}(G/\ker \lambda^G_{H,K})$. This implies that one of the conditions of Proposition 4.3 hold. In particular, the order of G is bounded and hence the problem of deciding which groups satisfies (1) can be done in a finite number of computations. Using this it is easy to write a program which calculates the list `L` of finite groups G satisfying one of the conditions of Proposition 4.3. We have done this using GAP [5] and Wedderga [3] (see Appendix A). The list `L` contains all the groups satisfying (1) but it contains some groups not satisfying (1). For example, if $G \in$ `L` and G/N satisfies (3) for some non-trivial normal subgroup N of G then G is not CSP'-critical. So we calculate, using GAP, a second list `R` excluding from `L` all the elements having a proper quotient satisfying (3). The groups forming `R` are precisely the groups of types (6)–(13) from Theorem 1.1. This finishes the proof. □

Now we deal with the case where G is an imprimitive subgroup of an exceptional component of type (EC2). For that we need the following lemma from [2] and three additional lemmas.

Lemma 4.5. *(See [2, Lemma 2.2].) Let D be a division algebra and let G be a subgroup of $\mathrm{GL}_2(D)$ spanning $M_2(D)$ over $\mathbb{Q}$. Then G is imprimitive if and only if there is a group homomorphism $\theta : N \to \mathrm{GL}_1(D)$ for N a subgroup of index 2 of G and $g \in G \setminus N$ such that if $K = \ker \theta$ then $K \cap K^g = 1$.*

Observe that the hypothesis that G spans $M_2(D)$ is not present in the statement of [2, Lemma 2.2] while it is used in its proof. This hypothesis is necessary because otherwise G could be included diagonally on $M_2(D)$. For example, if G is a subgroup of a division ring then it can be embedded diagonally in $\mathrm{GL}_2(D)$. This is an imprimitive representation and if the order of G is odd then the existence of the subgroup N mentioned in the lemma is not possible.

Lemma 4.6. *Assume that G is an imprimitive subgroup of an exceptional component $M_2(D)$ of type* (EC2) *of $\mathbb{Q}G$ and let $\theta : N \to \mathrm{GL}_1(D)$, $g \in G$ and $K = \ker\theta$ satisfy the conditions of Lemma 4.5. If D is an SSP component of $\mathbb{Q}(N/K)$ then $M_2(D)$ is an SSP component of $\mathbb{Q}G$.*

Proof. The rules

$$n \in N \to \begin{pmatrix} \theta(n) & 0 \\ 0 & \theta(g^{-1}ng) \end{pmatrix}, \qquad g \to \begin{pmatrix} 0 & \theta(g^2) \\ 1 & 0 \end{pmatrix}$$

define an injective group homomorphism $\bar{\theta} : G \to \mathrm{GL}_2(D)$. Moreover, D is generated over $\mathbb{Q}$ by $\theta(N)$, since $M_2(D)$ is spanned over $\mathbb{Q}$ by $\bar{\theta}(G)$. Thus D is spanned over $\mathbb{Q}$ by a subgroup isomorphic to N/K and hence D is a simple component of $\mathbb{Q}(N/K)$. Suppose that $(H/K, K_1/K)$ is a strong Shoda pair of N/K such that $D = \mathbb{Q}(N/K)e(N/K, H/K, K_1/K)$. Then θ is an irreducible representation of N affording the character λ^N_{H,K_1}. As $K = \ker\theta$, θ lifts to a faithful representation ρ of N/K affording the character $\lambda^{N/K}_{H/K,K_1/K}$. Using (2.3) and the fact that D is a division algebra, we deduce that K_1/K is normal in N/K. Thus $K_1/K = \mathrm{Core}_{N/K}(K_1/K) = \ker\lambda^{N/K}_{H/K,K_1/K} = 1$ so that $K_1 = K$. As $K \trianglelefteq N$ and H/K is cyclic and maximal abelian and normal in N/K, we deduce from [9, Corollary 3.6] that (H, K) is a strong Shoda pair of N and $e(N, H, K) = \varepsilon(H, K)$ is a primitive central idempotent of $\mathbb{Q}N$. Since $N \trianglelefteq G$, the G-conjugates of $\varepsilon(H, K)$ are primitive central idempotents of $\mathbb{Q}N$ and hence they are orthogonal. If $N_G(K) = N$ then (H, K) is a strong Shoda pair of G. Then $\mathbb{Q}Ge(G, H, K) \cong M_2(D)$, by (2.3). Otherwise, $K \trianglelefteq G$ and hence $K = K \cap K^g = 1$. If H is maximal abelian in G then again (H, K) is strong Shoda pair of G. Moreover $\bar{\theta}$ affords the character $\lambda^G_{H,1}$ and hence $M_2(D) = \mathbb{Q}Ge(G, H, K)$. Assume otherwise that H is not maximal abelian in G. Then there is $n \in N$ such that $n^{-1}g \in \mathrm{C}_G(H)$. As $(H, 1)$ is a strong Shoda pair of N, H is normal in N and therefore $h^g = h^n \in H$ for every $h \in H$. Therefore $H \trianglelefteq G$. Moreover $[N : H]$ is the degree of D which is either 1 or 2. Thus G/H is abelian. Since H is cyclic, we deduce that G is metabelian and hence every simple component of $\mathbb{Q}G$ is SSP. So in all the cases $M_2(D)$ is an SSP component of $\mathbb{Q}G$. □

Lemma 4.7. *Let N be a finite group containing two normal subgroups K_1 and K_2 such that $K_1 \cong K_2$, $K_1 \cap K_2 = 1$ and $N/K_i \cong \mathrm{SL}(2, 3)$. Then N is isomorphic to one of the following groups*:

(1) $\mathrm{SL}(2, 3)$.
(2) $\mathrm{SL}(2, 3) \times \mathrm{SL}(2, 3)$.
(3) $(\mathcal{Q}_8 \times \mathcal{Q}_8) \rtimes C_3 = (\langle i_1, j_1\rangle_{\mathcal{Q}_8} \times \langle i_2, j_2\rangle_{\mathcal{Q}_8}) \rtimes \langle c\rangle$, *with $i_k^c = j_k$ and $j_k^c = i_k j_k$ for every $k = 1, 2$.*
(4) $\mathrm{SL}(2, 3) \times C_2$.

Proof. Clearly if $K_1 = 1$ then $N \cong \mathrm{SL}(2,3)$. So we assume that $K_1 \neq 1$. The assumption of the lemma implies that $K_1 \times K_2$ is a normal subgroup of N. Then K_1 is isomorphic to a non-trivial normal subgroup of $N/K_2 \cong \mathrm{SL}(2,3)$. Thus K_1 is isomorphic to either C_2, Q_8 or $\mathrm{SL}(2,3)$. We discuss each case separately.

If $K_1 \cong \mathrm{SL}(2,3)$ then $|N| = 576 = |K_1 \times K_2|$. Thus $N = K_1 \times K_2 \cong \mathrm{SL}(2,3) \times \mathrm{SL}(2,3)$.

Assume $K_1 \cong \mathcal{Q}_8$. Then $|N| = 192$ and $[N : K_1 \times K_2] = 3$. Hence $N/(K_1 \times K_2) \cong \langle \bar{c} \rangle_3$ for some $c \in N$. As $N/K_k \cong \mathrm{SL}(2,3)$, one can choose generators i_k and j_k of K_k such that the action of c on $K_k = \langle i_k, j_k \rangle$ is given by $i_k^c = j_k$ and $j_k^c = i_k j_k$. Therefore $N \cong (\mathcal{Q}_8 \times \mathcal{Q}_8) \rtimes C_3$ and the conditions of (3) hold.

Finally suppose that $K_1 = \langle z_1 \rangle_2$. Then $|N| = 48$ and $K_i \leqslant Z(N)$. Let P be a Sylow 2-subgroup of N and c a generator of a Sylow 3-subgroup of N. Since $N/K_i \cong \mathrm{SL}(2,3) = \mathcal{Q}_8 \rtimes C_3$, we have $\mathcal{Q}_8 \cong P/K_i \trianglelefteq N/K_i$. Thus $P \trianglelefteq N$ P is non-abelian of order 16 and $K_1 \times K_2 \subseteq Z(P) \subset P$. As $P/Z(P)$ is not cyclic, necessarily $Z(P) = K_1 \times K_2 \cong C_2^2 \cong P/Z(P)$. Let $a, b \in P$ be such that $\langle aK_1, bK_1 \rangle = P/K_1$. Then $P = \langle a, b, z_1 \rangle$ where a and b have order 4 and $a^2, b^2, (a,b) \in (K_1 \times K_2) \setminus (K_1 \cup K_2) = \{z_1 z_2\}$. Thus $a^2 = b^2 = (a,b) = z_1 z_2$ and this implies that $\langle a, b \rangle \cong \mathcal{Q}_8$ and $\langle a, b \rangle \cap \langle z_1 \rangle = 1$. Hence $P = \langle a, b \rangle \times K_i \cong \mathcal{Q}_8 \times C_2$. Now it is easy to check that P has exactly four subgroups isomorphic to $\mathcal{Q}_8$. Namely $\langle a, b \rangle, \langle az_1, b \rangle, \langle a, bz_1 \rangle$ and $\langle az_1, bz_1 \rangle$. The action of $\langle c \rangle_3$ on P permutes these groups and hence it leaves invariant one of them. So let $\mathcal{Q}_8 \cong Q \leqslant P$ with $Q^c = Q$. Observe $Q \cap K_1 = Q \cap K_2 = 1$, so after a suitable change of generators we may assume that $Q = \langle a, b \rangle$. Since $z_2^c = 1$, we necessarily have that the action of c on Q has order 3 and hence $\langle Q, c \rangle = \mathrm{SL}(2,3)$ and $N = \langle Q, c \rangle \times K_1 \cong \mathrm{SL}(2,3) \times C_2$. □

Lemma 4.8. *Let G be a group and let $N = K_1 \times K_2$ be a subgroup of index 2 of G with $K_1 \cong K_2 \cong \mathrm{SL}(2,3)$. If the action of G on N permutes K_1 and K_2 then $G = (\mathrm{SL}(2,3) \times \mathrm{SL}(2,3)) \rtimes \langle g \rangle_2$ with $(x,y)^g = (y,x)$, for every $(x,y) \in \mathrm{SL}(2,3) \times \mathrm{SL}(2,3)$.*

Proof. We may assume that $N = \mathrm{SL}(2,3) \times \mathrm{SL}(2,3)$, $K_1 = \mathrm{SL}(2,3) \times 1$ and $K_2 = 1 \times \mathrm{SL}(2,3)$. For every $s \in \mathrm{SL}(2,3)$, let c_s denote the inner automorphism of $\mathrm{SL}(2,3)$ given by $c_s(x) = x^s$.

Let $g_1 \in G \setminus N$ and suppose $g_1^2 = (s_1, s_2)$. By assumption, there are $\tau, \sigma \in \mathrm{Aut}(\mathrm{SL}(2,3))$ such that $(x,y)^{g_1} = (\tau(y), \sigma(x))$ for every $(x,y) \in N$. Then

$$\big(c_{s_1}(x), c_{s_2}(y)\big) = (x,y)^{g_1^2} = \big(\tau\sigma(x), \sigma\tau(y)\big),$$

or equivalently $c_{s_1} = \tau\sigma$ and $c_{s_2} = \sigma\tau$. Therefore $(x,y)^{g_1} = (\sigma^{-1}(y)^{s_1}, \sigma(x)) = (\sigma^{-1}(y^{s_2}), \sigma(x))$ for every $x, y \in \mathrm{SL}(2,3)$.

We claim that $s_2 = \sigma(s_1)$. Indeed, if $x \in \mathrm{SL}(2,3)$ then $\tau(x) = \sigma^{-1} c_{s_2}(x) = \sigma^{-1}(s_2^{-1} x s_2) = c_{\sigma^{-1}(s_2)} \sigma^{-1}(x)$. Therefore $c_{\sigma^{-1}(s_2)} = \tau\sigma = c_{s_1}$ and hence if $z = s_1^{-1}\sigma^{-1}(s_2)$ then $z \in \mathrm{SL}(2,3)$ and $s_2 = \sigma(s_1 z)$. Consequently $(s_1, \sigma(s_1 z)) = g_1^2 = (g_1^2)^{g_1} = (c_{s_1}(s_1 z), \sigma(s_1)) = (s_1 z, \sigma(s_1))$. Thus $z = 1$ and the claim follows.

Let $g_2 = g_1(s_1^{-1}, 1)$. Then

$$g_2^2 = g_1^2(s_1^{-1}, 1)^{g_1}(s_1, 1) = (s_1, \sigma(s_1))(1, \sigma(s_1^{-1}))(s_1^{-1}, 1) = 1.$$

Therefore, one may assume without loss of generality that $g_1^2 = 1$. Hence, by the previous paragraphs $(x, y)^{g_1} = (\sigma^{-1}(y), \sigma(x))$. Let $K = (\mathrm{SL}(2,3) \times \mathrm{SL}(2,3)) \rtimes \langle g \rangle_2$, with $(x, y)^g = (y, x)$. Then the map $\alpha : (x, y)g^i \in K \mapsto (x, \sigma(y))g_1^i \in G$ is an isomorphism because $\alpha(g(x, y)) = \alpha((y, x)g) = (y, \sigma(x))g_1 = g_1(x, \sigma(y)) = \alpha(g)\alpha(x, y)$. □

We are ready to prove Theorem 1.1 for non-metabelian imprimitive subgroups of two-by-two matrix rings over division rings.

Proposition 4.9. *Let G be a non metabelian CSP'-critical group which is an imprimitive subgroup of an exceptional component of type* (EC2) *of $\mathbb{Q}G$. Then G is one of the groups in items* (14)–(15) *of Theorem 1.1.*

Proof. Let G satisfy the hypothesis of the proposition, and let D be a division ring such that $M_2(D)$ is an exceptional component of $\mathbb{Q}G$ and G is an imprimitive subgroup of $M_2(D)$. Let $\theta : N \to \mathrm{GL}_1(D)$, K and $g \in G$ be as in Lemma 4.5. By Lemma 4.6, N/K is a subgroup of $\mathrm{GL}_1(D)$ and D is a simple component of $\mathbb{Q}(N/K)$. We claim that G is not a subgroup of a division ring. Otherwise, by Proposition 4.2, G is one of the groups of types (1)–(5) of Theorem 1.1. However, the first three types are metabelian while the other two groups do not have a subgroup of index 2. This proves the claim. Since G is not metabelian, by Proposition 4.4, the exceptional component $M_2(D)$ of $\mathbb{Q}G$ is not SSP. Then, by Lemma 4.6, D is not an SSP component of $\mathbb{Q}(N/K)$. Therefore N/K is not strongly monomial. In particular, N/K is non-abelian. Thus D is not commutative and hence it is a totally definite quaternion algebra over $\mathbb{Q}$. Moreover, N/K is not a Z-group and therefore it is one of the groups in item (NZ) of Theorem 2.2. However the groups in (NZ)(b) and (NZ)(c) are metabelian and, in particular, strongly monomial, while the only non-commutative division algebra in the Wedderburn decomposition of $\mathbb{Q}\mathcal{O}^*$ is $\mathbb{H}(\mathbb{Q}(\sqrt{2}))$ and the only division algebra in the Wedderburn decomposition of $\mathbb{Q}\,\mathrm{SL}(2,5)$ is $(\mathbb{Q}(\zeta_5)/\mathbb{Q}(\sqrt{5}), -1)$. Hence $N/K = \mathrm{SL}(2,3) \times M$ with M a Z-group of odd order. If M is non-abelian then every Wedderburn component containing N/K should have degree greater than 2. Hence M is cyclic. If $M \neq 1$ then the centre of D should contain a root of unit of order greater than 2, in contradiction with the fact that $Z(D) = \mathbb{Q}$. Thus $N/K \cong \mathrm{SL}(2,3)$. This implies that $D = \mathbb{H}(\mathbb{Q})$ and hence the order of the centre of G is at most 2. Moreover, $K \cap K^g = 1$ and hence the subgroups $K_1 = K$ and $K_2 = K^g$ satisfy the hypothesis of Lemma 4.7. Thus one may assume that one of the following conditions holds: (1) $N = \mathrm{SL}(2,3) \times \mathrm{SL}(2,3)$ and $K = \mathrm{SL}(2,3) \times 1$ and $K^g = 1 \times \mathrm{SL}(2,3)$; (2) $N = \mathrm{SL}(2,3)$ and $K = 1$; (3) $N = \mathrm{SL}(2,3) \times \langle z \rangle_2$ and $K = \langle z \rangle_2 \neq K^g$; (4) $N = (\mathcal{Q}_8 \times \mathcal{Q}_8) \rtimes C_3$, $K = \mathcal{Q}_8 \times 1$ and $K^g = 1 \times \mathcal{Q}_8$.

(1) Assume first that $N = \mathrm{SL}(2,3) \times \mathrm{SL}(2,3)$. Then, by Lemma 4.8, $G \cong N \rtimes \langle g \rangle_2$ with $(x, y)^g = (y, x)$. Let $H = \langle P_2, b_1 b_2 \rangle$, where P_2 is the Sylow 2-subgroup of N and

$\langle b_1, b_2\rangle \cong C_3^2$ is a Sylow 3-subgroup of N. Then $P_2^g = P_2$ and $(b_1b_2)^g = b_1b_2$. Then H is a normal subgroup of G and $G/H \cong \mathcal{D}_6$ in contradiction with (P1).

(2) Suppose now that $N \cong \mathrm{SL}(2,3) = \langle i,j\rangle_{\mathcal{Q}_8} \rtimes \langle a\rangle_3$ and let $g \in G \setminus N$ and $Q = \langle i,j\rangle$. Then Q is a characteristic subgroup of $\mathrm{SL}(2,3)$ and hence $Q \lhd G$. One may assume without loss of generality that $g^2 \in Q$. Then N has eight elements of order 3 in two conjugacy classes $a^N = \{a, ia, ja, ija\}$ and $(a^2)^N = \{a^2, i^{-1}a^2, j^{-1}a^2, i^{-1}ja^2\}$. If $a^g \in (a^2)^N$ then $G/N_2 \cong Q$, in contradiction with (P1). Therefore $a^g = a^q$ for some $q \in N$ and, as Q contains a transversal of $C_N(a)$, we may assume that $q \in Q$. Replacing g by gq^{-1}, one may assume that $(a,g) = 1$. Let α be the restriction to Q of the inner automorphism defined by ag. Since the order of a is 3 and the order of g is a power of 2, the order of α is multiple of 3. Moreover $\mathrm{Aut}(Q) \cong S_4$ and therefore the order of α is 3. Then $(g,Q) = 1$ and hence $g \in Z(G)$. Thus $g^2 = 1$ and $G/\langle g\rangle \cong \mathrm{SL}(2,3)$ in contradiction with (P1).

(3) Suppose now that $N = \mathrm{SL}(2,3) \times C_2 = (\langle i,j\rangle_{\mathcal{Q}_8} \rtimes \langle a\rangle_3) \times \langle z\rangle_2$ and $K = \langle z\rangle_2$. The Sylow 2-subgroup of N is $N_2 = \langle i,j,z\rangle \cong \mathcal{Q}_8 \times C_2$. Hence N_2 is characteristic in N it has three elements of order 2, namely i^2, z and i^2z, and i^2 is the only one which is a square. Thus $z^g = i^2z$ because $K \neq K^g$. As in the previous case N has eight elements of order 3 in two conjugacy classes $a^N = \{a, ia, ja, ija\}$ and $(a^2)^N = \{a^2, i^{-1}a^2, j^{-1}a^2, i^{-1}ja^2\}$ and if $a^g \in (a^2)^N$ then $G/N_2 \cong \mathcal{D}_6$, in contradiction with (P1). Therefore $(a,g) = 1$ and thus $g^2 \in \langle i^2\rangle$. If $g^2 = 1$ then $(gz)^2 = i^2$. Hence we may assume that $g^2 = i^2$. Then $g^z = zgz = gi^2 = g^3$ and hence $\langle g,z\rangle \cong \mathcal{D}_8$. Moreover N_2 has 4 subgroups isomorphic to $\mathcal{Q}_8$: $\langle i,j\rangle, \langle i,jz\rangle, \langle iz,j\rangle$ and $\langle iz,jz\rangle$.

We claim that $(g,i) = (g,j) = 1$. If $\langle i,j\rangle^g = \langle i,j\rangle$ then conjugation by ag induces an automorphism of $\langle i,j\rangle \cong \mathcal{Q}_8$ of order a multiple of 3. As $\mathrm{Aut}(\mathcal{Q}_8) \cong S_4$ this implies that g commutes with i and j and the claim follows. Otherwise, i.e. if $\langle i,j\rangle^g \neq \langle i,j\rangle$, the intersection of $\langle i,j\rangle$ and $\langle i,j\rangle^g$ is a cyclic subgroup of order 4 and, by symmetry, one may assume that $\langle i,j\rangle \cap \langle i,j\rangle^g = \langle i\rangle$. Then $\langle i,j\rangle^g = \langle i,jz\rangle$. If $j^g \in \langle i\rangle$ then $\langle i^g\rangle = \langle j^{g^2}\rangle = \langle j\rangle$ and hence $\langle i,j\rangle^g = \langle i,j\rangle$, contradicting the assumption. Thus $j^g \in \{jz, j^{-1}z, ijz, i^{-1}jz\}$ and $j^{g^2} = j^{i^2} = j$. If $j^g = jz$ or $j^g = j^{-1}z$ then $j = j^{g^2} = (jz)^g = jzi^2z = i^2j$ or $j = j^{g^2} = (j^{-1}z)^g = jzi^2z = i^2j$, a contradiction. Thus $j^g = ijz$ or $j^g = i^{-1}jz$ and, replacing i by i^{-1} if necessary one may assume that $j^g = ijz$. Then $j = j^{g^2} = (ijz)^g = i^gijzi^2z = i^gi^{-1}j$ and therefore $i^g = i$. Thus $i^{ag} = j^g = ijz \neq j = i^a = i^{ga}$, in contradiction with $ga = ag$. This finishes the proof of the claim.

We conclude that $(\langle g,z\rangle, \mathrm{SL}(2,3)) = 1$, $\langle g,z\rangle \cong \mathcal{D}_8$ and $\langle g,z\rangle \cap \mathrm{SL}(2,3) = \langle g^2\rangle = \langle i^2\rangle$. Thus $G = \mathrm{SL}(2,3) \curlyvee_2 \mathcal{D}_8$ i.e. G is the group of item (14) in Theorem 1.1.

(4) Finally suppose that $N \cong (\mathcal{Q}_8 \times \mathcal{Q}_8) \rtimes C_3 = (\langle i_1,j_1\rangle_{\mathcal{Q}_8} \times \langle i_2,j_2\rangle_{\mathcal{Q}_8}) \rtimes \langle c\rangle$, with $i_k^c = j_k$, $j_k^c = i_kj_k$ and $\langle i_1,j_1\rangle^g = \langle i_2,j_2\rangle$. As in the previous case N has two conjugacy classes formed by elements of order 3 represented by c and c^2. If c and c^2 are conjugate in G and $N_2 = \langle i_1,j_1,i_2,j_2\rangle$ then $G/N_2 \cong \mathcal{D}_6$, contradicting (P1). As in the previous case this implies that we may assume that $(c,g) = 1$ and, in particular, $g^2 \in Z(N) = \langle i_1^2, i_2^2\rangle$. However $((i_1)^2)^g = i_2^2$ and therefore $g^2 \notin \{i_1^2, i_2^2\}$. If $g^2 = i_1^2i_2^2$ then $(i_1^2g)^2 = 1$, so we may

assume also that $g^2 = 1$. On the other hand N has eight normal subgroups isomorphic to $\mathcal{Q}_8$, namely

$$Q_{11} = \langle i_1, j_1 \rangle, \quad Q_{12} = \langle i_1 i_2^2, j_1 \rangle, \quad Q_{13} = \langle i_1, j_1 i_1^2 \rangle, \quad Q_{14} = \langle i_1 i_2^2, j_1 i_2^2 \rangle,$$
$$Q_{21} = \langle i_2, j_2 \rangle, \quad Q_{22} = \langle i_1^2 i_2, j_2 \rangle, \quad Q_{23} = \langle i_2, i_1^2 i_2 \rangle, \quad Q_{24} = \langle i_1^2 i_2, i_1^2 i_2 \rangle.$$

Observe that $Q_{1x} \cap Q_{2y} = 1$ and $(Q_{1x}, Q_{2y}) = 1$ for every $x, y \in \{1, 2\}$. Moreover, N has three elements of order 2, namely i_1^2, i_2^2 and $i_1^2 i_2^2$. Furthermore $i_x^2 \in Q_{1x}$ and $i_x^2 \in Q_{2x}$ for every $x = 1, 2, 3, 4$. As $i_1^g = i_2$, we deduce that the action of g by conjugation interchanges the Q_{1x}'s with the Q_{2x}'s. Therefore, if $b = c^2 g$ then b has order 6 and the action of b by conjugation interchanges the Q_{1x}'s with the Q_{2x}'s. Since the action of c permutes transitively the three cyclic subgroups of order 4 of each Q_{ix}, after renaming the generators we may assume that $i_2 = i_1^b$ and $j_2 = j_1^b$. As $c = b^2$, we have $i_2^b = j_1$ and $j_2^b = i_1 j_1$ and $G = (\langle i_1, j_1 \rangle \times \langle i_2, j_2 \rangle) \rtimes \langle b \rangle_6$. Thus G is the group of item (15) in Theorem 1.1. □

The following proposition completes the proof of Theorem 1.1.

Proposition 4.10. *Let G be a CSP'-critical group which does not satisfy the hypothesis of neither Proposition 4.2, nor Proposition 4.4 nor Proposition 4.9. Then G is one of the groups in items* (16)–(22) *of Theorem 1.1.*

Proof. By the hypothesis, G satisfies (P1) and (P2). Moreover we may assume that G is a primitive subgroup of an exceptional component $M_2(D)$ of type (EC2) of $\mathbb{Q}G$. In particular D is either $\mathbb{Q}$, an imaginary quadratic extension of $\mathbb{Q}$ or a totally definite quaternion algebra over $\mathbb{Q}$. Moreover, G satisfies the following properties:

(P3) G is not strongly monomial. In particular, G is not abelian-by-supersolvable.
(P4) If n is the order of an element g of G then $\varphi(n) \leqslant 4$ and if $g \in Z(G)$ then $\varphi(n) \leqslant 2$.

(P3) is a consequence of Proposition 4.4. To prove (P4) suppose $F = Z(D)$ and let $g \in G$. Then F is either $\mathbb{Q}$ or an imaginary quadratic extension of $\mathbb{Q}$. If $g \in Z(G)$ then F has a root of unity of order n and then $\varphi(n) \leqslant [F : \mathbb{Q}] \leqslant 2$. Assume that $D = F$. Consider g as an element of $M_2(F)$ and let f be the characteristic polynomial of g. Then g is conjugate in $M_2(\mathbb{C})$ to a diagonal matrix $\operatorname{diag}(\alpha_1, \alpha_2)$ where α_1 and α_2 are roots of unity. Let m_1 and m_2 be the orders of α_1 and α_2. Then $n = \operatorname{lcm}(m_1, m_2)$. Furthermore $f(\alpha_1) = f(\alpha_2) = 0$ and hence $F(\zeta_n) = F(\alpha_1, \alpha_2)$ is contained in the splitting field K of f over F. Thus $[F(\zeta_n) : F] \leqslant 2$ and hence $\varphi(n) = [\mathbb{Q}(\zeta_n) : \mathbb{Q}] \leqslant [F(\zeta_n) : \mathbb{Q}] \leqslant [F(\zeta_n) : F][F : \mathbb{Q}] \leqslant 4$. Suppose otherwise that $D \neq F$. Then D is a totally definite quaternion algebra over $\mathbb{Q}$ and $M_2(D)$ is embedded in $M_4(\mathbb{C})$. Consider g as an element of $M_4(\mathbb{C})$ and let f be the characteristic polynomial of g. Then g is conjugate in $M_4(\mathbb{C})$ of a diagonal matrix $\operatorname{diag}(\alpha_1, \alpha_2, \alpha_3, \alpha_4)$ where each α_i a root of unity, say

of order m_i, and $n = \operatorname{lcm}(m_1, m_2, m_3, m_4)$. Then f is multiple of the least common multiple of the minimal polynomials of the α_i and $\mathbb{Q}(\zeta_n) = \mathbb{Q}(\alpha_1, \alpha_2, \alpha_3, \alpha_4)$. As f has degree 4, either $\mathbb{Q}(\zeta_n) = \mathbb{Q}(\alpha_i)$ for some i or $\mathbb{Q}(\zeta_n) = \mathbb{Q}(\alpha_i, \alpha_j)$, with $\mathbb{Q}(\alpha_i) \neq \mathbb{Q}(\alpha_j)$ and $\varphi(m_1) = \varphi(m_2) = 2$. In the first case $\varphi(n) = \varphi(m_i) \leqslant 4$ and in the second case $\varphi(n) = \varphi(m_i)\varphi(m_2) = 4$.

In the remainder of the proof our main tool is the classification of the primitive subgroups of two-by-two matrix rings over division rings obtained by Banieqbal in [2]. This classification is contained in Theorems 3.8, 4.4, 4.5, 4.6, 4.7 and 5.8 of [2]. So G is one of the groups appearing in these theorems and we will consider each case separately.

We start observing that the groups of [2, Theorem 3.8] are all supersolvable and hence they do not satisfy (P3).

In the description of many of the remaining groups the group $G_{m,r} = \langle a\rangle_m \rtimes_s \langle b\rangle_n$ from (2.1) with m, r, s, t and n satisfying the conditions of (2.2) has a relevant role.

Let G be one of the groups of [2, Theorem 4.4] and let $N = O_2(G)\mathrm{C}_G(O_2(G))$. The statement of the theorem considers eight types for G denoted (a_1), (a_2), (b_1), (b_2), (c), (d_1), (d_2), and (e). An inspection of the proof of [2, Theorem 4.4] shows that if G satisfies conditions (b_1), (b_2), (c) or (e) then $G/N \cong \mathcal{D}_6$ in contradiction with (P1). If G satisfies (a_1) or (a_2) then G contains T_α^* with $\alpha \geqslant 1$. Therefore G has an element of order 3^α and hence (P4) implies that $\alpha = 1$. Since $T_1^* \cong \mathrm{SL}(2,3)$, in case (a_1), $G = \mathrm{SL}(2,3) \times N$ for some N. Then (P1) implies that $G = \mathrm{SL}(2,3)$, a subgroup of a division ring. This excludes this case. If G is of type (a_2) then $G = \mathrm{SL}(2,3) \curlyvee_2 G_{m,r}$, with $v_2(s) = v_2(n) = 1$. Then $1 \neq n = o_m(r)$ and therefore $m > 2$. Then $a^2 \neq 1$ and $G/\langle a^2, b^4\rangle \cong \mathrm{SL}(2,3) \curlyvee_2 C_4$ in contradiction with (P1). If G is of type (d_1) or (d_2) then $G \cong \mathcal{Q}_8 \rtimes G_{m,r}$ with m odd, $3 \mid n$, $(\mathcal{Q}_8, a) = 1$, $i^b = j$ and $j^b = ij$. Then $G/\langle a, b^3\rangle \cong \mathrm{SL}(2,3)$ in contradiction with (P1).

Suppose now that G is one of the groups of [2, Theorem 4.5] and let again $N = O_2(G)\mathrm{C}_G(O_2(G))$. In this case Banieqbal considers 13 cases denoted (a), (b), …, (h), (i_1), (i_2), (j), …, (l). As in the previous paragraph for some of these cases, namely all but the first three, $G/N \cong \mathcal{D}_6$ in contradiction with (P1). Hence G satisfies either (a), (b) or (c). In case (a), $G = T_\beta^* \curlyvee_2 G_{m,r}$ with $2 \leqslant v_2(s)$. By (P4), $\beta = 1$ and hence $G = \mathrm{SL}(2,3) \curlyvee_2 G_{m,r}$ with $4 \mid s$ and t odd. Moreover, by (P4), $4 \geqslant \varphi(m) \geqslant 2\varphi(t)$. Hence $\varphi(t) \leqslant 2$ and, as t is odd, necessarily $t = 1$ or 3. If $t = 3$ then $\gcd(r-1, m) = s = 4$ and hence $m = 12$. This implies that $r \equiv 5 \bmod 12$ and we may assume that $r = 5$ and $n = o_{12}(5) = 2$. Then $G/\langle \mathrm{SL}(2,3), a^3\rangle \cong \mathcal{D}_6$ in contradiction with (P1). Thus $t = 1$ and hence $G_{m,r}$ is cyclic of order m with $4 \mid m$. Then $\varphi(m) = 2$, by (P4), and therefore $m = 4$. We conclude that $G = \mathrm{SL}(2,3) \curlyvee_2 C_4$, i.e. G is as in item (16) of Theorem 1.1. In case (b), $G = \mathrm{SL}(2,3) \curlyvee_2 \mathcal{D}_{2^{\alpha+1}m}$ with $\alpha \geqslant 2$ and m is odd and greater than 1. Let a be an element of $\mathcal{D}_{2^{\alpha+1}m}$ of order $2^\alpha m$. Then $a^4 \neq 1$ and $G/\langle a^4\rangle \cong \mathrm{SL}(2,3) \curlyvee_2 \mathcal{D}_8$, a contradiction with (P1). Finally, in case (c), $G = \mathcal{Q}_8 \rtimes_2 G_{m,r}$ with $4 \nmid s$ and $3 \mid n = o_m(r) \mid \varphi(m) \leqslant 4$. This implies that $3 = \varphi(m)$ which is not possible because 3 is not in the image of the Euler function.

Assume that G is one of the groups of [2, Theorem 4.6] and take now $N = O_2(G)$. Now there are three types (a), (b) and (c) to consider. In case (a), $G = \mathrm{SL}(2,3) \curlyvee_2 \mathcal{D}_{2^\alpha}$ with $\alpha \geqslant 4$. Then a proper quotient of G is isomorphic to $\mathcal{D}_8$, in contradiction with (P1). Moreover, from the proof of the theorem one has that for types (b) and (c), we have $G/N \cong \mathcal{D}_6$, again a contradiction with (P1).

Suppose that G satisfies the conditions of [2, Theorem 4.7]. Then $G = R \times G_{m,r}$ with $\gcd(mn, 30) = 1$ and R is a subgroup of $\mathcal{B}^*$ containing $O_2(\mathcal{B}^*)$ where $\mathcal{B}^*$ is the following extension of $\mathcal{B}$:

$$\mathcal{B}^* = \mathcal{B} \rtimes C_2 = \left(\left(\langle i,j\rangle_{\mathcal{Q}_8} \curlyvee_2 \langle a,b\rangle_{\mathcal{D}_8}\right) \downharpoonright_2 \langle u,v\rangle_{\mathrm{SL}(2,5)}\right) \rtimes \langle h\rangle_2$$

where i, j, a, b, u and v satisfy the relations of $\mathcal{B}$ and the action of h on $\mathcal{B}$ is given by

$$j^h = ij, \quad i^h = i^{-1}, \quad a^h = a, \quad b^h = b^{-1}, \quad u^h = u^3, \quad v^h = u^{vu}v^2.$$

By (P4) we deduce that $G_{m,r} = 1$ and hence $O_2(\mathcal{B}^*) \subseteq G \subseteq \mathcal{B}^*$. Moreover, [2, Theorem 4.7] also states that either $G \subseteq \mathcal{B}$ and $G/O_2(G)$ is isomorphic to $\mathcal{D}_6, C_5$ or $\mathcal{D}_{10}$ or $G \nsubseteq \mathcal{B}$ and $G/O_2(G) \cong C_5 \rtimes C_4$. The case $G/O_2(G) \cong \mathcal{D}_6$ contradicts (P1) and inspecting the proof [2, Theorem 4.7] one observes that in the last case the only two-by-two matrix algebra containing G is $M_2(\mathbb{H}(\mathbb{Q}(\sqrt{2})))$, contradicting (P2). Therefore we have $O_2(\mathcal{B}^*) \subseteq G \subseteq \mathcal{B}$ and $G/O_2(G)$ is isomorphic to either C_5 or $\mathcal{D}_{10}$. Moreover, $O_2(\mathcal{B}^*) = O_2(\mathcal{B}) = \langle i,j,a,b\rangle$, $\mathcal{B}/\mathcal{O}_2(\mathcal{B}) \cong A_5$ and $\mathcal{B}^*/O_2(\mathcal{B}^*) \cong S_5$. Furthermore all the subgroups H of S_5 with $H/O_2(H) \cong C_5$ (respectively, $H/O_2(H) \cong \mathcal{D}_{10}$) are conjugate in A_5 to $\langle (1,2,3,4,5)\rangle$ (respectively, $\langle (1,2,3,4,5), (2,5)(3,4)\rangle$). This implies that $O_2(G) = O_2(\mathcal{B})$ and there are exactly two conjugacy classes of subgroups G of $\mathcal{B}^*$ satisfying the conditions $O_2(\mathcal{B}) \leqslant G$ and $G/O_2(\mathcal{B}) \cong C_5$ or $\mathcal{D}_{10}$. A computer calculation using GAP shows that if $G/O_2(G) \cong C_5$ then G is the group of item (20) in Theorem 1.1 and if $G/O_2(G) \cong \mathcal{D}_{10}$ then G is the group of item (21) in Theorem 1.1. This finishes this case.

Finally assume that G satisfies one of the conditions (a)–(i) in [2, Theorem 5.8]. In case (e), G contains an element of order 20 and, in case (i), G contains an element of order 24. In case (d), G contains $\mathrm{SL}(2,5) \curlyvee_2 C_m$ with $4 \mid m$ and thus G has an element of order 20. These three cases are hence excluded by (P4). In case (a), $G = \mathrm{SL}(2,5) \curlyvee_2 \mathcal{D}_{2^\alpha m}$ with either $m = 1$ and $\alpha \geqslant 4$ or $m > 1$ odd and $\alpha \geqslant 2$. However, by (P4), $m = 1, 3$ or 5 and as $\mathrm{SL}(2,5)$ has elements of order 3 and 5, if $m \neq 1$ then G has an element of order 15, in contradiction with (P4). Therefore $m = 1$ and, again using (P4) we deduce that $\alpha = 4$. Then $G/\mathrm{SL}(2,5) \cong \mathcal{D}_8$, in contradiction with (P1). In case (c), $G = \mathcal{A}^{\pm} \times G_{m,r}$. By (P1), $G = \mathcal{A}^{\pm}$ and hence G is as in item (18) or item (19) of Theorem 1.1. The same argument shows that in case (f), $G = \mathrm{SL}(2,9)$ and in case (h), $G = \mathcal{B}$. So in these cases G either is as in item (17) or as in item (22) of Theorem 1.1. Assume that G satisfies condition (b). Then, $G = \mathrm{SL}(2,5) \curlyvee_2 G_{m,r}$ with $2 \mid s$. Assume that $M_2(D)$ is an exceptional component of $\mathbb{Q}G$. As G is an epimorphic image of the

direct product $\mathrm{SL}(2,5) \times G_{m,r}$, there are simple components A of $\mathbb{Q}\,\mathrm{SL}(2,5)$ and B of $\mathbb{Q}G_{m,r}$ such that $M_2(D)$ is an epimorphic image of $A \otimes_{\mathbb{Q}} B$ and $\mathrm{SL}(2,5)$ is contained in A and $G_{m,r}$ is contained in B. A dimension argument compared with the Wedderburn decomposition of $\mathbb{Q}\,\mathrm{SL}(2,5)$ obtained in the proof of Proposition 3.2, shows that A is either $M_2(\frac{-1,-3}{\mathbb{Q}})$ or $(\mathbb{Q}(\zeta_5)/\mathbb{Q}(\sqrt{5}), -1)$. However, in the second case the centre of D contains $\mathbb{Q}(\sqrt{5})$ in contradiction with the fact that $M_2(D)$ is an exceptional component. Thus $A = M_2(\frac{-1,-3}{\mathbb{Q}})$ and hence $B = \mathbb{Q}$. Therefore $G_{m,r}$ is contained in $\mathbb{Q}$ and hence it is C_2. Thus $G = \mathrm{SL}(2,5)$ in contradiction with the assumption that G is not contained in a division algebra. Suppose finally that G is of type (g). Then G contains a subgroup N of index 2 isomorphic to $\mathrm{SL}(2,9)$ and an element $g \in G \setminus N$ such that $g^2 \in Z(N)$ and g acts on the entries of the elements of $\mathrm{SL}(2,9)$ as the Frobenius automorphism $x \mapsto x^3$. This is the group identified with $[1440, 4591]$ in the GAP library of small group. Using Wedderga we obtain the Wedderburn decomposition

$$\begin{aligned}\mathbb{Q}G = {} & 2\mathbb{Q} \oplus 4M_5(\mathbb{Q}) \oplus M_3\big(\mathbb{Q}(\zeta_3)\big) \oplus M_2\big(\mathbb{H}\big(\mathbb{Q}(\sqrt{3})\big)\big) \oplus 2M_9(\mathbb{Q}) \\ & \oplus 2M_{10}(\mathbb{Q}) \oplus M_4\big(\mathbb{Q}(\zeta_5)/\mathbb{Q}, -1\big) \oplus M_{16}(\mathbb{Q}) \oplus M_{10}\big(\mathbb{H}(\mathbb{Q})\big),\end{aligned}$$

which does not have any exceptional component, in contradiction with the hypothesis. This finishes the proof of the Proposition and of Theorem 1.1. □

Appendix A. GAP programs used in the proof of Proposition 4.4

In this appendix we include the GAP code used in the proof of Proposition 4.4. The following GAP program implements the function `Propiedad` with three arguments G, H and K. If (H, K) is a strong Shoda pair of a finite group G then `Propiedad(G,H,K)` returns true if one of the conditions (1)–(7) of Proposition 4.3 holds. The groups are identified using the terminology of the GAP library of small groups.

```
    Propiedad := function(G,H,K)
local id,N;
if G=H then
  return false;
fi;
id := IdSmallGroup(G);
N:=Normalizer(G,K);
if Size(K)=1 and id in [[6,1] , [8,3] , [12,4]] then
  return true;
fi;
if Size(K)=2 and id = [8,3]  then
  return true;
fi;
```

```
if Size(K)=1 and id in [[16,6] , [24,1] , [24,5]] then
  return true;
fi;
if Size(H)=4*Size(K) and Size(G)=2*Size(N) and N=H and
            (Size(K)=2 or Size(K)=4) then
  return true;
fi;
if Size(K)=1 and id = [16,8] then
  return true;
fi;
if Size(K)=1 and id in [[24,10] , [24,11] ] then
  return true;
fi;
if (Size(H) = 3*Size(K) or Size(H)=6*Size(K)) and
        Size(G)=2*Size(H) and N=H and Size(K) <> 1 and
        Size(H) mod Size(K)^2 = 0 then
  return true;
fi;
if Size(K)=1 and id = [40,3] then
  return true;
fi;
if Size(K)=1 and id = [32,42] then
  return true;
fi;
if Size(H) = 4*Size(K) and Size(G)=2*Size(N) and
        IdSmallGroup(N/K) = [8,4] and (Size(K)=2 or Size(K)=4) then
  return true;
fi;
if 6*Size(K) mod Size(H) = 0 and Size(G)=2*Size(N) and
        IdSmallGroup(N/K) = [12,1] and Size(K) <> 1 and
        Size(H) mod Size(K)^2 = 0 then
  return true;
fi;
if Size(K)=1 and Size(H)=12 and IdSmallGroup(G/H)=[4,2] then
  return true;
fi;
return false;
end;
```

The program below computes the list `L` formed by the groups G of orders 6, 8, 12, 16, 18, 24, 32, 36, 40, 48, 64, 72 or 144 for which `Propiedad(G,H,K)` returns true for some strong Shoda pair (H, K) of G and another list `R` with the groups in `L` with no proper

quotient isomorphic to any of the groups in items (6)–(13) of Theorem 1.1. The list `L` contains 127 groups while the resulting list `R` contains the 8 groups in items (6)–(13) of Theorem 1.1.

```
LoadPackage("wedderga");
D := [6,8,12,16,18,24,32,36,40,48,64,72,144];
csp := [[6,1],[8,3],[16,6],[16,13],[24,11],[32,50],[40,3],[72,19]];
L := [];
R := [];

for n in D do
 m:=NumberSmallGroups(n);
 for i in [1..m] do
  G:=SmallGroup(n,i);
  if not IsAbelian(G) then
   prop := false;
   ssp := StrongShodaPairs(G);
   nssp := Length(ssp);
   j:=0;
   while not prop and j<nssp do
    j:=j+1;  x:=ssp[j];
    H:=x[1]; K:=x[2];
    prop := Propiedad(G,H,K);
   od;
   if prop then
    Add(L,[n,i]);
    NS := Filtered(NormalSubgroups(G),x->Size(x)>1);
    IdNS := SSortedList(NS,x->IdSmallGroup(G/x));
    if Intersection(IdNS,csp)=[] then
     Add(R,[n,i]);
    fi;
   fi;
  fi;
 od;
od;
```

References

[1] S.A. Amitsur, Finite subgroups of division rings, Trans. Amer. Math. Soc. 80 (2) (1955) 361–386 (in English).

[2] B. Banieqbal, Classification of finite subgroups of 2×2 matrices over a division algebra of characteristic zero, J. Algebra 119 (2) (1988) 449–512.

[3] O. Broche Cristo, A. Konovalov, A. Olivieri, G. Olteanu, Á. del Río, I. Van Gelder, Wedderga — Wedderburn decomposition of group algebras, version 4.5.3, 2013.

[4] H. Bass, J. Milnor, J.-P. Serre, Solution of the congruence subgroup problem for SL_n ($n \geqslant 3$) and Sp_{2n} ($n \geqslant 2$), Inst. Hautes Études Sci. Publ. Math. (33) (1967) 59–137, MR 0244257 (39 #5574).
[5] The GAP Group, GAP – Groups, Algorithms, and Programming, version 4.5.6, 2012.
[6] E. Jespers, G. Leal, Generators of large subgroups of the unit group of integral group rings, Manuscripta Math. 78 (3) (1993) 303–315, MR 1206159 (94f:20010).
[7] B. Liehl, On the group SL_2 over orders of arithmetic type, J. Reine Angew. Math. 323 (1981) 153–171, MR 611449 (82h:10034).
[8] C. Moser, Repr'esentation de -1 comme somme de carr'es dans un corps cyclotomique quelconque, J. Number Theory 5 (1973) 139–141, MR 0316423 (47 #4970).
[9] A. Olivieri, Á. del Río, J.J. Simón, On monomial characters and central idempotents of rational group algebras, Comm. Algebra 32 (4) (2004) 1531–1550, MR 2100373 (2005i:16054).
[10] G. Olteanu, Computing the Wedderburn decomposition of group algebras by the Brauer–Witt theorem, Math. Comp. 76 (258) (2007) 1073–1087 (electronic), MR 2291851 (2008b:16036).
[11] D.S. Passman, Infinite Crossed Products, Pure Appl. Math., vol. 135, Academic Press Inc., Boston, MA, 1989, MR 979094 (90g:16002).
[12] G. Prasad, A. Rapinchuk, Developments on the congruence subgroup problem after the work of Bass, Milnor and Serre, in: Hyman Bass, T.Y. Lam (Eds.), Collected Papers of John Milnor. V. Algebra, American Mathematical Society, Providence, RI, 2010, pp. 307–325, MR 2841244 (2012h:01022).
[13] I. Reiner, Maximal Orders, London Math. Soc. Monogr. Ser., vol. 5, Academic Press [A subsidiary of Harcourt Brace Jovanovich, Publishers], London, New York, 1975, MR 0393100 (52 #13910).
[14] J. Ritter, S.K. Sehgal, Construction of units in integral group rings of finite nilpotent groups, Trans. Amer. Math. Soc. 324 (2) (1991) 603–621, MR 987166 (91h:20008).
[15] M. Shirvani, B.A.F. Wehrfritz, Skew Linear Groups, London Math. Soc. Lecture Note Ser., vol. 118, Cambridge University Press, Cambridge, 1986.
[16] L.N. Vaserštein, The group SL_2 over Dedekind rings of arithmetic type, Mat. Sb. (N. S.) 89 (131) (1972) 313–322, 351, MR 0435293 (55 #8253).
[17] T.N. Venkataramana, On systems of generators of arithmetic subgroups of higher rank groups, Pacific J. Math. 166 (1) (1994) 193–212, MR 1306038 (95k:22016).