JOURNAL OF ALGEBRA 119, 449–512 (1988)

Classification of Finite Subgroups of 2×2 Matrices over a Division Algebra of Characteristic Zero*

BEHNAM BANIEQBAL

Department of Computer Science, University of Manchester, Oxford Road, Manchester M13 9PL, England

Communicated by Walter Feit

Received June 25, 1987

INTRODUCTION

The aim of the present paper is a complete classification of the finite groups G which can be embedded in $M_2(D)^\times$ for some division algebra D. We will make the assumption that G is primitive and its rational span is $M_2(D)$. The reason for this assumption is that the structure of other groups is easily deducible from the results of [1] (cf. 2.1). We begin by surveying the literature on the finite multiplicative subgroups of a simple algebra. In [12] B. Hartley and M. A. Shahabi obtain a general structure theorem on such groups: there exists a function $f(n)$ such that any finite subgroup of $M_n(D)$ has a metabelian subgroup of index bounded by $f(n)$. S. A. Amitsur gives a classification of finite subgroups of $D^\times$ in [1]. The problem of embeddability of Amitsur's groups in a given division algebra is considered by B. Fein and M. Schacher in [9]. M. Hikari considers the same problem as ours in [13–15]. In the first two papers, by appealing to powerful group theoretic results, the insoluble composition factors of G are determined. This is also done in [11]. In the third paper, partial results on soluble groups with an abelian Sylow 2-subgroup are obtained. Finally, in [27], J. Tits shows among other results that the double cover of the Hall–Janko simple group J_2 embeds in 3×3 matrix ring over quaternions over $\mathbb{Q}(\sqrt{5})$.

Now we give a brief indication of the contents of this work. Section 1 contains information on the norm residue symbol and the Brauer group.

* Taken from the author's Ph.D. thesis, University of Manchester, 1984.

0021-8693/88 $3.00

Also we expand on the results of [1] in 1.5. By the inclusion of this material, we hope to make the present work more accessible. In a recent book [26], a different treatment of results of [1] on the classification of finite subgroups of $D^\times$ is presented. In Section 2, we gather some miscellaneous results. In particular we show that the odd Sylow subgroups of G are abelian and determine the Fitting subgroup $F(G)$ of G. Here Lemmas 2.3, 2.4, and 2.6 are the important tools to enable us to describe the structure of $\mathbb{Q}\{G\}$, the rational span of G. The book of T. Yamada [28] contains calculations on the line of Lemma 2.3. In Sections 3 and 4 we investigate G when it is soluble. First we consider the cases when the automorphism group of $O_2(G)$ is a 2-group. Then the structure of G is determined once that of a Sylow 2-subgroup S of G is known. A long case by case argument on the possible actions of S on $F(G)$, which makes $\mathbb{Q}\{SF(G)\}$ to have size at most 2, leads to the determination of S. The balance of the section contains presentations for the various types of G. We note here the factorisability property of G when S itself does. The remaining possibilities for $O_2(G)$ are considered in Section 4. Various modifications on G lead to a new group $\bar{G}$ which renders itself to the treatment of Section 3. Thus G is retrieved by reversal of this procedure. In Section 5, we study an insoluble group G. We start off by showing that there are only three perfect groups embeddable in some $M_2(D)^\times$. For that, we have recourse to the result of [11] on quasi-simple subgroups of $M_2(D)$. However, when D is locally compact, an independent classification, using the properties of the maximal order of D, is possible. Incidentally those three groups are obtainable here as well. For the general case, our method is to analyse the possible extensions of the perfect radical of G in $M_2(D)^\times$ in the light of the Noether–Skolem theorem and our information on the soluble groups. Thus Theorem 5.8 concludes the group theoretic classification of G. In this part of the paper, the types of G are given by presentations involving integer parameters. Also the structure of $\mathbb{Q}\{G\}$ as a cyclotomic crossed product is explicitly described. It remains to find the conditions on the parameters to ensure that that algebra has size 2. This is carried out for a (representative) sample of three groups in the final section. When $\mathbb{Q}\{G\}$ does have size 2, then G is primitively represented in it, as proved during the investigation in Sections 2–5.

Notation

D	division algebra
G	finite primitive spanning subgroup of $M_2(D)^\times$ for some D
$\mathrm{Aut}(R)$, $\mathrm{Inn}(R)$	the automorphism, inner automorphism group of the group R

$\mathrm{Out}(R) = \mathrm{Aut}(R)/\mathrm{Inn}(R)$	
${}^hg = hgh^{-1}$, ${}^\sigma a = \sigma(a)$, $h: g \to g'$	means $hgh^{-1} = g'$
S_h	conjugation map by h
$Z(R)$, $Z(A)$	centre of the group R, algebra A
$\mathbb{Q}\{T\}$	the $\mathbb{Q}$-subalgebra of A generated by the subset T
$R \,Y_m\, S$	central product of R and S with a subgroup of order m in their centres identified
$R \downarrow_m S$	split extension with central subgroups of order m identified
$\mathscr{D}^n R$	terms of the derived series of R
$\mathscr{D}_{2m} = \langle g, h \rangle$	$g^m = 1,\ h^2 = 1,\ hgh^{-1} = g^{-1},\ m > 1$
$\mathscr{Q}_{2m} = \langle g, h \rangle$	$g^m = 1,\ h^2 = g^{m/2},\ hgh^{-1} = g^{-1},\ 2 \mid m$
$\mathscr{S}_{2^{\alpha+1}} = \langle g, h \rangle$	$g^{2^\alpha} = 1,\ h^2 = 1,\ hgh^{-1} = g^{-1+2^{\alpha-1}},\ \alpha \geqslant 3$
$\mathscr{E}_{2^{\alpha+1}} = \langle g, h \rangle$	$g^{2^\alpha} = 1,\ h^2 = 1,\ hgh^{-1} = g^{1+2^{\alpha-1}},\ \alpha \geqslant 2$
$\mathscr{C}_n$	cyclic group of order n
$T^*_\alpha = \langle i, j, g \rangle$	$i^4 = 1,\ i^2 = j^2,\ jij^{-1} = i^{-1},\ g^{3^\alpha} = 1,\ g: i \to j,\ j \to ij,\ \alpha \geqslant 1$
$T^* = T^*_1$	
$\mathscr{O}^*$	binary octahedral group
$N_{E/F}(x)$	norm of $x \in E$
$(\alpha, E/F)$	the norm residue value of $\alpha \in F$, E local field
$\mathscr{N}_{E/F} = \langle N_{E/F}(x);\ x \in E^\times \rangle$	
$\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{H}$, $\mathbb{Z}_p$, $\mathbb{Q}_p$	integer, rational, real, complex, quaternion, p-adic integer, or rational numbers
(m, n), $\mathrm{lcm}(m, n)$	greatest common divisor, least common multiple of m, n
$\gamma(r, m)$	minimal integer $n > 0$ such that $r^n \equiv 1 (m)$ $((r, m) = 1)$
$\beta(p, m)$	exact power of p dividing m
$n \mid m$	n divides m
$p^\alpha \parallel m$	p^α exactly divides m
$\langle E/F, G, \alpha \rangle$	crossed product algebra
$\mathscr{A}$	the rational quaternions

1. Background Material

1. *Completions of Number Fields*

The material in this section is treated in most books on algebraic number theory, e.g., [18] or [20]. Let E/K be a relatively Galois extension with the group G. Let $\mathfrak{P}$ be a prime of E lying over the prime $\mathfrak{p}$ of K. $\mathfrak{P}$

may be finite or infinite. In the finite case $\mathfrak{P}$ will denote a prime ideal or a non-archimedean valuation of E. In the infinite case $\mathfrak{P}$ denotes the equivalence class of an embedding of E in $\mathbb{C}$. We denote the $\mathfrak{P}$-adic additive valuation of E with value group $\mathbb{Z}$ by $v_{\mathfrak{P}}$. Now G acts on the prime divisors of $\mathfrak{p}$ in E. Define

$$D_{\mathfrak{P}}(E/K) = \{g \in G; g\mathfrak{P} = \mathfrak{P}\} \text{ the decomposition group of } \mathfrak{P}$$

$$I_{\mathfrak{P}}(E/K) = \{g \in G;\ gx \equiv x \bmod \mathfrak{P} \text{ for all integers } x \in E\}$$

$$\text{the inertia group of } \mathfrak{P},$$

which we often abbreviate to $D_{\mathfrak{P}}$, $I_{\mathfrak{P}}$. In the definition above if $\mathfrak{P}$ is an infinite prime, we put $g\mathfrak{P}(x) = \mathfrak{P}(g^{-1}(x))$, $g \in G$, $x \in E$, so that $D_{\mathfrak{P}}$ consists of 1 and complex conjugation relative to the embedding $\mathfrak{P}$: $E \to \mathbb{C}$. In addition, we put $I_{\mathfrak{P}} = D_{\mathfrak{P}}$.

These two groups behave well with respect to subgroups and quotients of G. Namely, let F/K be a subextension of E/K with $\mathrm{Gal}(E/F) = H$ and let $\mathfrak{P}$ induce the prime $\wp$ on F. We can indicate the latter by $\mathfrak{P} \mid \wp \mid \mathfrak{p}$. We have

$$D_{\mathfrak{P}}(E/F) = D_{\mathfrak{P}}(E/K) \cap H, \quad I_{\mathfrak{P}}(E/F) = I_{\mathfrak{P}}(E/K) \cap H.$$

When H is normal in G,

$$D_{\wp}(F/K) = D_{\mathfrak{P}}(E/K)H/H, \quad I_{\wp}(F/K) = I_{\mathfrak{P}}(E/K)H/H.$$

Now when $\mathfrak{p}$ is finite, denote the ramification and residue degree of $\mathfrak{P} \mid \mathfrak{p}$ by $e = e_{\mathfrak{p}}(E/K)$ and $f = f_{\mathfrak{p}}(E/K)$. In the infinite case, put $e = f = 1$ unless $\mathfrak{p}$ is real and $\mathfrak{P}$ is complex whereby $e = 2$, $f = 1$. Now we always have $|I_{\mathfrak{P}}(E/K)| = e$, $|D_{\mathfrak{P}}(E/K)| = ef$.

The completion of E under $\mathfrak{P}$ will be denoted by $E_{\mathfrak{P}}$ in which E and $K_{\mathfrak{p}}$ are naturally embedded. If $\mathfrak{p}$ is finite, then $v_{\mathfrak{P}}(x) = ev_{\mathfrak{p}}(x)$ for all $x \in K$. Now $E \cap K_{\mathfrak{p}}$ is the fixed field of $D_{\mathfrak{P}}$ in E so by restriction $\mathrm{Gal}(E_{\mathfrak{P}}/K_{\mathfrak{p}})$ is isomorphically mapped onto $D_{\mathfrak{P}}$. The subgroup corresponding to $I_{\mathfrak{P}}$ is $\mathrm{Gal}(E_{\mathfrak{P}}/Z)$, where Z is the maximal unramified subextension of $E_{\mathfrak{P}}/K_{\mathfrak{p}}$.

Actually, all the fields with which we shall deal are cyclotomic, i.e., abelian over $\mathbb{Q}$. As the groups introduced above are conjugate for different extensions of p to E, they will be the same in our case so we shall specify only a rational prime in the notation. As for completions, we shall change our emphasis and take them in a fixed algebraic closure $\bar{\mathbb{Q}}_p$ of $\mathbb{Q}_p$ (or $\mathbb{C}/\mathbb{R}$). Thus an embedding $\sigma_{\mathfrak{P}}$: $E \to \bar{\mathbb{Q}}_p$ gives rise to a prime ideal of E: $\mathfrak{P} = \{x$ integer in E; $v(\sigma_{\mathfrak{P}}(x)) > 0\}$, where v is the additive valuation of $\bar{\mathbb{Q}}_p$. Since $E/\mathbb{Q}$ is now Galois, $\sigma_{\mathfrak{P}}(E)$ is independent of the embedding. We denote it by E_p or $E\mathbb{Q}_p$. In the infinite case we will say E is (totally) real or complex according as the completion of E at ∞ is $\mathbb{R}$ or $\mathbb{C}$. The reason for this modification of viewpoint is that the properties of the completions concerning us will be independent of the prime of E in question.

Let us explicitly describe the groups introduced above for $E=\mathbb{Q}(\zeta_m)$, $K=\mathbb{Q}$, where ζ_m is a primitive mth root of 1 and $m>2$. The Galois group G consists of all automorphisms σ of E of the form $\sigma\colon \zeta_m \to \zeta_m^i$, $(i, m)=1$. So $|G|=\phi(m)$. $I_\infty = D_\infty = \langle\tau\rangle$, where $\tau\colon \zeta_m \to \zeta_m^{-1}$. Now suppose that p is a finite prime, $p^l \| m$, $l \geqslant 0$. Put $m'=mp^{-l}$ and $f=\gamma(p, m')$, the order of $p \bmod m'$. Then $I_p = \{\sigma\in G;\ \sigma(\zeta_{m'})=\zeta_{m'}\}$; $D_p=\{\sigma\in G;\ \sigma(\zeta_{m'})=\zeta_{m'}^{p^i}$ for some integer $i\}$; $|I_p|=1$ if $l=0$, $p^{l-1}(p-1)$ if $l\geqslant 1$, and $|D_p|=f|I_p|$.

2. *The Norm Residue symbol*

Excellent references for this section are [2, 22]. By a local field we shall understand a finite extension of $\mathbb{Q}_p$ or $\mathbb{R}$. Let K be a local field. The main theorem of local class field theory is that an abelian extension E of K is characterised by $\mathcal{N}_{E/K}=\{N_{E/K}(x);\ 0\neq x\in E\}$, which is an open subgroup of $K^\times$ of finite index, and there exists a canonical isomorphism between $K^\times/\mathcal{N}_{E/K}$ and $G=\mathrm{Gal}(E/K)$. The map is the norm residue symbol $(\cdot, E/K)$: $K^\times \to G$. Thus $(\alpha, E/K)=1 \Leftrightarrow \alpha\in\mathcal{N}_{E/K}$, where $\alpha\in K^\times$. Now let F/K be a subextension of E/K. The norm residue map enjoys the following properties:

(a) $(\alpha, F/K)=(\alpha, E/K)|_F$, where $\alpha\in K^\times$. Thus $(\alpha, E/K)\in \mathrm{Gal}(E/F) \Leftrightarrow \alpha\in\mathcal{N}_{F/K}$.

(b) $(\beta, E/F)=(N_{F/K}(\beta), E/K)$, where $\beta\in F^\times$.

(c) If K is real or complex, then $(\alpha, E/K)=1$ unless $K=\mathbb{R}$, $E=\mathbb{C}$, $\alpha<0$ whereupon $(\alpha, E/K)=$ the complex conjugation τ.

(d) Suppose E/K is unramified of degree n. Let π be a prime element of K and U its units, i.e., elements of K with value 0. We know $\mathrm{Gal}(E/K)$ is cyclic with a distinguished generator χ, the Frobenius automorphism. We have $\mathcal{N}_{E/K}=U\times\langle\pi^n\rangle$, $(\pi, E/K)=\chi$.

Finally, we state the explicit formula of the norm residue symbol for $E=\mathbb{Q}_p(\zeta_m)$, $K=\mathbb{Q}_p$, where $m=p^lm'$, $l\geqslant 0$, $(p, m')=1$. If $l=0$, then E/K is unramified of degree $f=\gamma(p, m)$ so it is covered by (d). Suppose that $l\geqslant 1$. We have $E=E_1E_2$, where $E_1=\mathbb{Q}_p(\zeta_{p^l})$, $E_2=\mathbb{Q}_p(\zeta_{m'})$. We have $E_1\cap E_2=\mathbb{Q}_p$, $\mathrm{Gal}(E/K)\cong\mathrm{Gal}(E_1/K)\times\mathrm{Gal}(E_2/K)$. Thus by (a) and the first case we may confine our attention to E_1/K. Put $\zeta=\zeta_{p^l}$. Then E_1/K is totally ramified of degree $p^{l-1}(p-1)$. $1-\zeta$ is a prime element of E_1, $N_{E_1/K}(1-\zeta)=p$. Furthermore $\mathcal{N}_{E_1/K}=\langle u\in\mathbb{Z}_p^\times;\ u\equiv 1(p^l)\rangle\times\langle p\rangle$ and for $\alpha\in\mathbb{Z}_p^\times$, $(\alpha, E_1/K)\colon \zeta\to\zeta^\beta$, where $\beta\in\mathbb{Z}$, $\beta\equiv\alpha^{-1}(p^l)$.

3. *Central Simple Algebras and the Brauer Group*

An almost complete reference volume for the results here is [24]. Let K be an arbitrary field. By a simple algebra A over K we understand a finite-dimensional algebra over K such that any two-sided idea of A is 0 or A.

The centre $Z(A)$ of A is then a field containing K which we can take as coefficient field. Thus we say A is central over K when $Z(A) = K$. On the structure of A, we have the famous

THEOREM (Wedderburn). *Let A be a simple algebra over K. Then $A \cong M_m(D)$, where D is a division algebra over K. Moreover m and the K-isomorphism type of D are uniquely determined.*

If A, B are central simple algebras over K, then so is $A \otimes_K B$. This operation allows us to define an abelian group $\mathrm{Br}(K)$, the Brauer group of K, on the set of division algebras central over K. Namely if D, D' are two and $D \otimes_K D' = M_*(D'')$, put $D \cdot D' = D''$. Equivalently, we can form $\mathrm{Br}(K)$ out of equivalence classes of central simple algebras over K where we say A is equivalent to B, $A \sim B$, if their division algebra parts are K-isomorphic. When $A \sim K$, we say that A is split.

Let A be a central simple algebra over K and E an arbitrary extension of K. $\mathrm{Dim}_K A$ is a square, and its square root is called the *index* of A. If $A \cong M_m(D)$ for a division algebra D, then m is called the *size* of A (nonstandard). Finally, the *exponent* of A is that in $\mathrm{Br}(K)$. Now $A \otimes_K E$ is a central simple algebra over E. So we have a homomorphism $\cdot \otimes_K E$: $\mathrm{Br}(K) \to \mathrm{Br}(E)$. If A is in the kernel, i.e., $A \otimes_K E \sim E$, then we say E splits A. If A is a division algebra but $A \otimes_K E$ is not, we will say that E splits A partially (nonstandard). Now let E/K be a (finite) Galois extension with the group G. Let α: $G \times G \to E^\times$ be a factor set, i.e.,

$$\alpha(g, h)\,\alpha(gh, j) = \alpha(g, hj) \cdot {}^g\alpha(h, j), \quad g, h, j \in G.$$

Then the crossed product algebra A of E/K with G has an E-basis S_g, $g \in G$, such that

$$S_g S_h = \alpha(g, h) S_{gh}, \quad S_g x = g(x) S_g, \quad g, h \in G, x \in E.$$

It is denoted by $\langle E/K, G, \alpha \rangle$. The algebra A is central simple over K with index $|G|$. Cohomologous factor sets produce K-isomorphic algebras. Thus when $\mathrm{Gal}(E/K) = \langle g \rangle$ is cyclic of order n, we can take the E-basis to be 1, S_g, ..., $(S_g)^{n-1}$ with the relations $S_g x = g(x) S_g$ and $(S_g)^n = \beta$ for some $\beta \in K^\times$. Often we write g instead of S_g. The resulting algebra denoted by $\langle E/K, g, \beta \rangle$ is called cyclic.

In the following two theorems, let A be central simple over K.

THEOREM (Noether–Skolem). *Let B, B' be simple subalgebras of A containing K and let σ: $B \to B'$ be a K-isomorphism of B onto B'. Then there exists $x \in A^\times$ such that $\sigma(y) = xyx^{-1}$ for all $y \in B$.*

THEOREM (Double Centraliser). *Let B be a simple subalgebra of A*

central over K. Put $B' = C_A(B)$. *Then* B' *is central simple over K,* $C_A(B') = B$ *and* $A = B \otimes_K B'$.

If $Z \leqslant K$ and B is a simple subalgebra of A central over Z, then $B \cdot K \cong B \otimes_Z K$ is a simple subalgebra of A central over K to which the above may be applied.

LEMMA. *Let A be a simple algebra over K.*

(a) *Let B be a simple subalgebra of A which need not be a vector space over K or have the same identity as A. Then* $\text{size}(B) \leqslant \text{size}(A)$.

(b) *Let B be a simple subalgebra of A containing K. Then* $\text{index}(B) \leqslant \text{index}(A)$.

Proof. (a) Let V be the faithful irreducible left A module over K. Let $D = \text{End}_A(V)$ act on the right of V. D is a division algebra. Putting $m = \dim_D V$, we have $A = \text{End}_D V \cong M_m(D)$, $\text{size}(A) = m$ and V can be regarded as the set of column vectors of size m over D. Put $m' = \text{size}(B)$. So B has m' orthogonal idempotents $e_1, ..., e_{m'}$. Now $\bigoplus_{i=1}^{m'} e_i V$ is a nontrivial D-space decomposition. Hence $m' \leqslant m$.

(b) Let $\bar{K}$ be an algebraic closure of K. Set $n = \text{index}(A)$, $n' = \text{index}(B)$. Then $M_{n'}(\bar{K}) \leqslant B \otimes_K \bar{K} \leqslant A \otimes_K \bar{K} =$ direct sum of copies of $M_n(\bar{K})$. Projecting on some summand of the right-hand side, we get a $\bar{K}$ embedding of $M_{n'}(\bar{K})$ into $M_n(\bar{K})$ (not necessarily respecting the identities). So by (a), $n' \leqslant n$.

Now we specialise K to be a number field. There is a complete description of $\text{Br}(K)$ with the theory of the Hasse invariant. Familiarity with this theory will be usefull. However, we will briefly summarise the actual results we need. Thus for a central simple algebra A over K and every prime divisor $\mathfrak{p}$ of K, $\text{inv}_\mathfrak{p} A$ is a rational number mod 1 satisfying the following properties.

(a) $\text{inv}_\mathfrak{p} A \equiv 0(1)$ for all but a finite number of primes. If $\mathfrak{p}$ is infinite, $\text{inv}_\mathfrak{p} A \equiv 0(1)$ unless $\mathfrak{p}$ is real and $A \otimes_K K_\mathfrak{p} \sim \mathbb{H}$, where $\mathbb{H}$ is the Quaternions over $\mathbb{R}$. In that case $\text{inv}_\mathfrak{p} A \equiv \frac{1}{2}(1)$.

(b) The denominator of $\text{inv}_\mathfrak{p} A$ in the reduced form is the exponent of $A_\mathfrak{p} = A \otimes_K K_\mathfrak{p}$. The exponent of A is the least common multiple of them over $\mathfrak{p}$.

(c) $A \sim K \Leftrightarrow \text{inv}_\mathfrak{p} A \equiv 0(1)$ for all $\mathfrak{p} \Leftrightarrow A_\mathfrak{p} \sim K_\mathfrak{p}$ for all $\mathfrak{p}$.

(d) $\text{inv}_\mathfrak{p} A \otimes_K B \equiv \text{inv}_\mathfrak{p} A + \text{inv}_\mathfrak{p} B(1)$, where B is central simple over K.

(e) $\text{inv}_\mathfrak{P} A \otimes_K E \equiv |E_\mathfrak{P} : K_\mathfrak{p}| \cdot \text{inv}_\mathfrak{p} A(1)$, where E is a finite extension of K with the prime $\mathfrak{P} \mid \mathfrak{p}$.

If D is a division algebra central over K, then $\text{index}(D) = \text{exponent}(D)$. Thus $\text{index}(A) = \text{size}(A) \times \text{exponent}(A)$. Now let $A = \langle E/K, g, \alpha \rangle$ be a cyclic algebra, $\text{Gal}(E/K) = \langle g \rangle$ of order n, $g^n = \alpha \in K$. The algebra A is split $\Leftrightarrow \alpha \in \mathcal{N}_{E/K}$. Part (b) above in this context becomes

HASSE'S NORM THEOREM. *Let E/K be a cyclic extension of number fields and $\alpha \in K$. Then $\alpha \in \mathcal{N}_{E/K} \Leftrightarrow \alpha \in \mathcal{N}_{E_\mathfrak{P}/K_\mathfrak{p}}$ for every prime divisor $\mathfrak{P} \mid \mathfrak{p}$ of E/K. In fact suppose that $(\alpha, E_\mathfrak{P}/K_\mathfrak{p}) = g^r$. Then $\text{inv}_\mathfrak{p} A \equiv r/n(1)$; see* [22, *Teil* II, *Lemma* 1.10].

Defining $\mathcal{A} = \langle \mathbb{Q}(i), j, -1 \rangle$, $i = \sqrt{-1}$, j: $i \to -i$ (the rational quaternions; the quaternion over K will be denoted by $\mathcal{A}_K = \mathcal{A} \otimes_\mathbb{Q} K$) we have $\text{inv}_\infty \mathcal{A} = \frac{1}{2}$, $\text{inv}_2 \mathcal{A} = \frac{1}{2}$, and $\text{inv}_p \mathcal{A} = 0$ for any odd prime p.

LEMMA. *Let D, D' be central division algebras over K with indices n, n'. Then for a prime p, $p \mid \text{size}(D \otimes_K D') \Leftrightarrow p \mid n$ and $p \mid n'$. Thus $D \otimes_K D'$ is a division algebra if and only if $(n, n') = 1$.*

Proof. Clearly $\text{index}(D \otimes_K D') = nn'$. It is easily established that $nn'/(n, n')^2 \mid \text{exponent}(D \otimes_K D') \mid nn'/(n, n')$. The assertion then follows from the fact that index = size × exponent as above.

In the context of the lemma above, if $D \otimes_K D'$ is not a division algebra, we shall say that it is split partially (nonstandard terminology). Finally, we remark that the central simple algebras we shall deal with turn out to be cyclotomic, i.e., are of the form $A = \langle E/K, G, \alpha \rangle$, where $E/\mathbb{Q}$ is cyclotomic and α: $G \times G \to \langle \zeta \rangle$, where $\zeta \in E$ is some root of unity. Set $|G| = n$, $\text{exponent}(A) = m$. It is proved in [27, Theorem 6.1] that then a primitive mth root ξ of 1 belongs to K. Moreover if $\mathfrak{p}$ and $\mathfrak{p}'$ are two prime divisors of the rational prime p in K, then $\text{inv}_\mathfrak{p} A \equiv r \cdot \text{inv}_{\mathfrak{p}'} A(1)$, where $\mathfrak{p}' = \theta\mathfrak{p}$ for some $\theta \in \text{Gal}(K/\mathbb{Q})$ and $\theta(\xi) = \xi^r$. Thus the local exponent of A at $\mathfrak{p}$ and $\mathfrak{p}'$ are the same and we can talk of the local exponent or the denominator of the Hasse invariant of A at p.

4. *Rational Group Rings*

Let G be a finite group. The structure of $\mathbb{Q}G$ is well known: $\mathbb{Q}G = A_1 \oplus \cdots \oplus A_r$, where $A_i = \mathbb{Q}Ge_i$ is a simple algebra; $e_1, \ldots, e_r$ are the central primitive idempotents of $\mathbb{Q}G$. Put $A_i = M_{d_i}(D_i)$. The irreducible complex characters of G can be broken into $\mathbb{Q}$-conjugacy classes which will correspond to the simple components above. That is, we can order the classes such that, picking χ_i from the ith class, we have $\chi_i(A_i) \neq 0$, $\chi_i(A_j) = 0$, $i \neq j$. In fact $Z(D_i) \cong \mathbb{Q}(\chi_i)$ the character field. Now $\mathbb{C}G = \mathbb{C} \otimes_\mathbb{Q} \mathbb{Q}G = \bigoplus_{i=1}^r \mathbb{C} \otimes_\mathbb{Q} M_{d_i}(D_i)$ and $\mathbb{C} \otimes_\mathbb{Q} M_{d_i}(D_i) =$ direct sum of $|\mathbb{Q}(\chi_i) : \mathbb{Q}|$ copies of $M_{d_i m_i}(\mathbb{C})$, where $m_i = \text{index}(D_i)$. These components arise from the various embeddings of $Z(D_i)$ in $\mathbb{C}$. Thus $d_i m_i = \chi_i(1)$ and if

ρ_i: $\mathbb{Q}G \to A_i$ is the projection on A_i, then by the definition of the reduced trace $\chi_i(g) = \mathrm{tr}(\rho_i(g))$, $g \in G$, where a suitable embedding of $Z(D_i)$ in $\mathbb{C}$ has to be taken. Proofs can be found in [5].

5. *Review on Finite Subgroups of a Division Algebra*

Amitsur completely classifies the finite subgroups of a division algebra in [1]. Understanding the methods employed in that paper will be very useful though not essential here. However, later in our work Theorems 5 and 7 of [1] will be required. We remark that the calculations for the $G_{m,r}$ groups of type (3D) can be avoided by the use of our techniques. We now expand and comment on the results of [1]. The references are to that paper.

(a) Let $G = \langle a, b \rangle$ be a $G_{m,r}$ group of type (3C) so $(r, m) = 1$, $a^m = 1$, $b^n = a^t$, $bab^{-1} = a^r$; $n = \gamma(r, m)$, $s = (r-1, m)$, $st = m$, $(ns, t) = 1$, t odd. We have $Z(G) = \langle a^t \rangle$, $\mathscr{D}G = \langle a^s \rangle$, $F(G) = \langle a \rangle$, and $G = \langle a^s \rangle \rtimes \langle b \rangle$. Observe that $G_{m,r} \cong G_{m',r'} \Leftrightarrow m' = m$ and $r' \equiv r^x(m)$ for some $x \in \mathbb{Z}$, $(x, n) = 1$. Actually a more general expression of $G \cong G_{m,r}$ as a cyclic extension of $F(G)$ is $G = \langle a, h \rangle$, $a^m = 1$, $h^{n'} = a^{t'}$, $hah^{-1} = a^r$, where $n = \gamma(r, m)$, $s't' = m$, $s' \mid s = (r-1, m)$, $st = m$, $(s/s', n) = 1$, and $(ns, t) = 1$.

(b) Now let G as in (a) be a subgroup of $D^\times$ for some division algebra D. By Theorem 5 either $G = \mathscr{Q}_{2m}$ with $2 \| m$ or 5.2 holds. Let the latter be the case and put $t = \prod_1^k p_i^{\alpha_i}$, p_i odd primes, $v_i = \gamma(r, p_i^{\alpha_i})$. In 5.2 if $p = p_i$, then $n_p = \mathrm{lcm}_{j \neq i}(v_j)$. It follows from 5.2 that $v_1, \ldots, v_k$ are pairwise coprime and $n = \prod_1^k v_i$. Observe that $v_i \neq 1$ otherwise $p_i \mid (s, t) = 1$, a contradiction. Now we obtain a factorisation of G. We have $G = L \rtimes H$, where $L = \langle a^s \rangle$ has order t and $H = \langle b \rangle$ has order ns. We know $n \mid s$ by Lemma 5. Write $ns = \mu \prod_1^k \mu_i$, where v_i and μ_i have exactly the same prime divisors and $(\mu, n) = 1$. Thus $v_i \mid \mu_i$ and $\mu \mid s$. It follows from pairwise coprimality of v_i that $\langle b \rangle = \langle b^{ns/\mu} \rangle \times \bigtimes_{i=1}^k \langle b^{ns/\mu_i} \rangle$ and $G = C \times G_1 \times \cdots \times G_k$, where $C = \langle b^{ns/\mu} \rangle$, $G_i = \langle a^{m/p_i^{\alpha_i}}, b^{ns/\mu_i} \rangle$. Thus to any factorisation $L = L_1 \times L_2$ of L we have one $H = H_1 \times H_2$ for H such that $G = (L_1 H_1) \times (L_2 H_2)$.

(c) Now consider a $G_{m,r}$ subgroup of $D^\times$ of type (3D). By Theorem 5 either $G = \mathscr{Q}_{2m}$ with $4 \mid m$ or condition 5.2(c) holds as 2(a), 2(b) deal with the (3C) types. It follows from 5.2 that $b^{n/2}$ centralises $O_{2'}(\langle a \rangle)$. Hence $O_2(G) \cong \mathscr{Q}_8$ is the Sylow 2-subgroup of G and $G \cong \mathscr{Q}_8 \times G_{m/4,r}$. The rest of 5.2(c) says that 2 has odd order mod $m/4$.

(d) Now we reformulate Theorem 7 of [1] in the light of (c) above. A finite group G can be embedded in $D^\times$ for some division algebra D if and only if G is of the following types:

(1) A $G_{m,r}$ group satisfying (3C) (i.e., with cyclic Sylow subgroups) and 5.2(a) or 5.2(b). Cyclic groups are included for $r \equiv 1(m)$.

(2) $\mathscr{Q}_{2m}$ a quaternion group, $2|m$.

(3) $\mathscr{Q}_8 \times R$, $T^* \times R$, $\mathscr{O}^*$, where $R \cong G_{m,r}$ is of type (1) and mn, $\gamma(2, m)$ are odd.

(4) $\mathscr{T}^* \cong SL(2, 5)$.

The classification of primitive finite subgroup of $M_2(D)^\times$ to follow will to some extent reflect this pattern. That is, the groups in Sections 3, 4, and 5 correspond in some way to the types (1), (2), (3), and (4) above.

2. Preliminary Results

1. We suppose that $G \leqslant M_2(D)$ is a finite group with the identity element $\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$ and D is a division algebra of characteristic zero. G is primitive if there is no nonsingular 2×2 matrix A over D such that AgA^{-1} is monomial for all $g \in G$. In particular this means that G is irreducible. We can reformulate this in the following way. Let V be the set of column vectors over D. V is a (G, D) bimodule. The group G is primitive iff we cannot write $V = V_1 \oplus V_2$ as D modules such that $gV_1 = V_1$ or V_2 and $gV_2 = V_2$ or V_1 for all $g \in G$. In the classification of finite subgroups of $M_2(D)$ we can restrict our attention to primitive groups as the imprimitive ones are really expressible in terms of subgroups of D. Namely

2. Lemma. *Let $G < M_2(D)^\times$ be an imprimitive finite group. Then there is a subgroup H of G with index 2 and a normal subgroup N of H such that if $G = H \cup Hg$ then $N \cap {}^gN = 1$ and H/N embeds in D. Conversely, if we have the groups H, N as above and θ: $H \to D$ is a representation with kernel N, then*

$$h \to \begin{pmatrix} \theta(h) & 0 \\ 0 & \theta(g^{-1}hg) \end{pmatrix}, \qquad g \to \begin{pmatrix} 0 & \theta(g^2) \\ 1 & 0 \end{pmatrix}$$

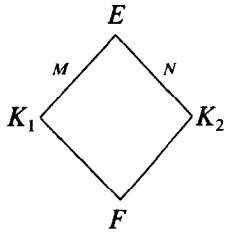
is a faithful representation of G in $M_2(D)$.

Proof. In the imprimitive representation of G, let H be the diagonal matrices and N be those of the form $\left(\begin{smallmatrix} 1 & 0 \\ 0 & * \end{smallmatrix}\right)$.

Now we make another restriction on G. There is an obvious map $\mathbb{Q}G \to \mathbb{Q}\{G\}$. So $\mathbb{Q}\{G\}$ is semisimple, $\mathbb{Q}\{G\} \cong D_1$ or $D_1 \oplus D_2$ or $M_2(D_1)$. In the second case, let e_1, $e_2 \in \mathbb{Q}\{G\}$ be the central idempotents corresponding to D_1, D_2. The decomposition $V = e_1V \oplus e_2V$ of V into (G, D) modules contradicts the irreducibility of G. We will now assume that the first case does not hold, as that is covered by the paper of Amitsur [1]. So henceforth $\mathbb{Q}\{G\} = M_2(D)$, i.e., G is assumed to span $M_2(D)$ and D is a rational division algebra.

Our main tools are the following two lemmas.

3. LEMMA. *Let E/F be a Galois extension of fields with the group $H = M \times N$ and let K_1, K_2 be the fixed fields of M and N.*



Let α: $H \times H \to E^\times$ be a factor set of H such that $\alpha(y, y') \in K_1$ for all y, $y' \in N$. Then

$$\langle E/F, H, \alpha\rangle \cong \langle K_1/F, N, \alpha|_N\rangle \otimes_F \langle K_2/F, M, \beta\rangle$$

for some factor set β: $M \times M \to K_2^\times$.

Proof. Let S_h, $h \in H$, be an E-basis for $\langle E/F, H, \alpha\rangle$. For a fixed $x \in M$ and all $y \in N$, ${}^{S_y}S_x = f_x(y)S_x$ for some f_x: $N \to E^\times$. In fact f_x is a crossed homomorphism for

$$\begin{aligned} {}^{S_yS_{y'}}S_x &= {}^{S_y}(f_x(y')S_x) = {}^{y}f_x(y')\, f_x(y)S_x \\ &= {}^{\alpha(y,\,y')S_{yy'}}S_x = {}^{\alpha(y,\,y')}(f_x(yy')S_x) \\ &= f_x(yy')S_x \end{aligned}$$

so $f_x(yy') = f_x(y) \cdot {}^{y}f_x(y')$. Since $H^1(N, E^\times) = 0$, by [22, Teil II, 2.2] there is $0 \neq a_x \in E$ such that $f_x(y) = a_x/{}^{y}a_x$. Now ${}^{S_y}(a_xS_x) = {}^{y}a_x f_x(y)S_x = a_xS_x$ $(y \in N)$. Let β be the factor set of a_xS_x, $x \in M$: $(a_xS_x)(a_{x'}S_{x'}) = \beta(x, x')(a_{xx'}S_{xx'})$, $\beta(x, x') = (a_x \cdot {}^{x}a_{x'}/a_{xx'})\,\alpha(x, x')$. We have $\beta(x, x') \in K_2$, $E = K_1 \otimes_F K_2$ and

$$\sum_{h \in H} ES_h = \left(\sum_{y \in N} K_1S_y\right) \otimes_F \left(\sum_{x \in M} K_2a_xS_x\right).$$

4. LEMMA. *Let H, L be finite subgroups of $M_2(D)$ and suppose that H and L commute. Exactly one of the following holds, where A_*, B_* denote simple algebras with the centres E_*, F_*.*

(a) *$\mathbb{Q}\{H\} = A$, $\mathbb{Q}\{L\} = B$, E and F generate a subfield EF of $M_2(D)$. Then $\mathbb{Q}\{HL\} \cong (A \otimes_E EF) \otimes_{EF} (B \otimes_F EF)$.*

(b) $\mathbb{Q}\{H\} = A$, $\mathbb{Q}\{L\} = B$, *and* E *and* F *do not generate a subfield of* $M_2(D)$. *Then* $\mathbb{Q}\{E, F\} = K_1 \oplus K_2$ *for two fields* K_1 *and* K_2 *which are composites of* E *and* F *and*

$$\mathbb{Q}\{HL\} \cong \bigoplus_{i=1}^{2} (A \otimes_E K_i) \otimes_{K_i} (B \otimes_F K_i).$$

(c) $\mathbb{Q}\{H\} = A$, $\mathbb{Q}\{L\} = B_1 \oplus B_2$. Then $\mathbb{Q}\{Ef_i, F_i\} \cong EF_i$ *is a field and* $\mathbb{Q}\{HL\} = \bigoplus_{i=1}^{2} (A \otimes_E EF_i) \otimes_{EF_i} (B_i \otimes_{F_i} EF_i)$, *where* $1 = f_1 + f_2$, $f_i \in F_i$.

(d) *The same as* (c) *with* H *and* L *interchanged.*

(e) $\mathbb{Q}\{H\} = A_1 \oplus A_2$, $\mathbb{Q}\{L\} = B_1 \oplus B_2$. *Then by suitable numbering of* B_i, *identities of* A_i *and* B_i *coincide and* $\mathbb{Q}\{HL\} = \bigoplus_{i=1}^{2} (A_i \otimes_{E_i} E_i F_i) \otimes_{E_i F_i} (B_i \otimes_{F_i} E_i F_i)$.

Clearly, except for case (a), *the algebras* A_i *and* B_i *and the tensor product summands of* $\mathbb{Q}\{HL\}$ *must be division algebras.*

Proof. Note that the identities of H and L are taken to be $\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$. Clearly the five cases are mutually exclusive. Since the proof is elementary, we illustrate case (e) only. Let us denote the matrix $\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$ by 1. Put $1 = e_1 + e_2$, $1 = f_1 + f_2$, $e_i \in A_i$, $f_i \in B_i$. e_i and f_i are the identities of A_i and B_i. Note that A_i and $B_{i'}$ commute. Since $1 = \sum_{i,i'=1}^{2} e_i f_{i'}$ and $M_2(D)$ has at most the sum of two orthogonal idempotents, two of the above summands are zero. Both of these two cannot involve e_1. Hence, by renumbering the B_i, we can take $e_1 f_2 = e_2 f_1 = 0$. Then $e_1 = e_1(f_1 + f_2) = e_1 f_1 = (e_1 + e_2) f_1 = f_1$ and $e_2 = f_2$. The commutative semisimple algebra $\mathbb{Q}\{E_i, F_i\}$ must be a field otherwise $M_2(D)$ would contain at least three orthogonal idempotents, a contradiction. Put $K_i = \mathbb{Q}\{E_i, F_i\}$ a composite of E_i and F_i, $X_i = (A_i \otimes_{E_i} K_i) \otimes_{K_i} (B_i \otimes_{F_i} K_i)$ a simple algebra. There is an obvious nontrivial homomorphism of X_i onto $\mathbb{Q}\{A_i, B_i\}$ which sends $1 \otimes 1$ to $e_i f_i = e_i \neq 0$. So it is an isomorphism. Since $\mathbb{Q}\{HL\} = \sum_{i=1}^{2} \mathbb{Q}\{A_i, B_i\}$, the assertion is proved.

In our investigation, it is the case (a) which is most often applicable, because of either the concluding remark in the lemma or Lemma 9 in the sequel.

5. At this point we stop to prove a theorem which in its less general form is proved by Jacobson [19] and used by Amitsur [1]. We do this as it illustrates a situation occurring a few times in the later part of this investigation.

PROPOSITION. *Let* A *be a central simple algebra over* K *and* H *be a group*

of outer automorphisms of A, that is, a nontrivial $h \in H$ induces a nontrivial automorphism on K.

Then $A = B \otimes_F K$, where $B = C_A(H)$, $F = B \cap K$ is the fixed field of H in K. So the automorphisms in H are really Galois automorphisms of K/F which are extended to A.

Proof. Following Jacobson's idea, we form the algebra of formal sums $X = \sum_{h \in H} AS_h$, where the S_h are symbols satisfying the relations

$$S_h S_{h'} = S_{hh'}, \qquad S_1 = 1 \qquad \text{of} \quad A,\ S_h a = h(a) S_h.$$

for all h, $h' \in H$, $a \in A$. The algebra X, a form of a skew group ring, is a central simple algebra over F. For let I be a nonzero two-sided ideal of X. Pick a nonzero x in I. If x involves at least two symbols, i.e., $x = aS_h + bS_g + \cdots$, $a, b \in A$ nonzero, $g \neq h$ in H, then choose $\alpha \in K$ so that $gh^{-1}(\alpha) \neq \alpha$. The element

$$xS_{h^{-1}}\alpha - \alpha x S_{h^{-1}} = b(gh^{-1}(\alpha) - \alpha) S_{gh^{-1}} + \cdots$$

is nonzero, belongs to I, and involves one less symbol than x. Repeating this procedure, we see that $aS_h \in I$ for some nonzero $a \in A$ and $h \in H$. It follows that $a \in I$ for some $a \in A$. Hence $I = X$ and X is simple. Now $C_X(K) = A$ for if $a = \sum_{h \in H} a_h S_h \in C_X(K)$, it follows from $ax = xa$ that $a_h h(x) = a_h x$ for all $x \in K$. Hence $a_h = 0$ for $h \neq 1$, and $a \in A$. If furthermore $a \in Z(X)$ then $ab = ba$ and $aS_h = S_h a$ for all $b \in A$, $h \in H$ so that $a \in F$.

Now $Y = \sum_{h \in H} KS_h \cong \langle K/F,\ H,\ 1 \rangle$ is a central simple subalgebra of X. By the double centralizer theorem $X = Y \otimes_F C_X(Y)$. Now $C_X(K) = A$. So $C_X(Y) = B$ and $X = Y \otimes_F B = \sum_{h \in H} (K \otimes_F B) S_h$. Comparing coefficients, we get $A = K \otimes_F B$.

The following lemma is essentially contained in Amitsur's paper [1]:

6. LEMMA. *Let the finite group H have a self-centralising normal cyclic subgroup $C = \langle c \rangle$ of order m so that $\bar{H} = H/C$ acts faithfully on C. Let $h_1 \cdots h_s$ be right coset representatives of C in H and α be their factor set. Suppose that H is a subgroup of the simple algebra $A = M_n(D)$. If C is a p group then $\langle \mathbb{Q}(\zeta_m), \bar{H}, \alpha \rangle$ is a direct summand of $\mathbb{Q}\{H\}$, where c projects on ζ_m. If the representation of H in A is irreducible (in the sense of* 2.1) *or $\mathbb{Q}\{C\}$ is known to be a field, then $\mathbb{Q}\{H\} = \langle \mathbb{Q}(\zeta_m), \bar{H}, \alpha \rangle$.*

Proof. Let $\mathbb{Q}C = \bigoplus_{i=1}^{r} F_i$ with the idempotents e_i. By conjugation, H operates on $\mathbb{Q}C$. e_i are fixed under H because e_i is characterised by $\mathrm{Ker}_C e_i = \{g \in C;\ ge_i = e_i\}$ and for $h \in H$, $\mathrm{Ker}_C e_i = \mathrm{Ker}_C he_i h^{-1}$. If $|\mathrm{Ker}_C e_i| = d$ then $F_i = e_i \mathbb{Q}C \cong \mathbb{Q}(\zeta_{m/d})$.

Now suppose that under the natural map ϕ: $\mathbb{Q}C \to \mathbb{Q}\{C\}$, $e_1 \cdots e_k$ alone do not go to zero. So $F_i = \mathbb{Q}\{C\}\,\phi(e_i)$ and $\sum_{i=1}^k \phi(e_i) = 1$ of A. $\bigcap_{i=1}^k \mathrm{Ker}_C\, e_i = 1$ for if g is in this intersection then $\phi(g) = \phi(g)\sum_{i=1}^k \phi(e_i)$ $= \sum_{i=1}^k \phi(ge_i) = \sum_{i=1}^k \phi(e_i) = 1$. Thus $g = 1$. Suppose C is a p-group. This implies that, say, $\mathrm{Ker}_C\, e_1 = 1$. So $\mathbb{Q}\{C\}\,\phi(e_1) \cong \mathbb{Q}(\zeta_m)$ and $\bar{H}$ is represented faithfully on $\mathbb{Q}\{C\}\,\phi(e_1)$ by Galois automorphisms. Now

$$\mathbb{Q}\{H\} = \mathbb{Q}\{\mathbb{Q}\{C\}, h_1, \ldots, h_s\}$$
$$= \bigoplus_{i=1}^{k} \mathbb{Q}\{\mathbb{Q}\{C\}\,\phi(e_i), h_1\phi(e_i), \ldots, h_s\phi(e_i)\}.$$

These components are orthogonal to each other and the first one is a homomorphic image of the simple algebra $\langle \mathbb{Q}(\zeta_m), \bar{H}, \alpha \rangle$ hence isomorphic to it.

When $\mathbb{Q}\{C\}$ is a field, then $k = 1$ and $\mathbb{Q}\{H\} \cong \langle \mathbb{Q}(\zeta_m), \bar{H}, \alpha \rangle$. If H is represented irreducibly and V is the (H, D) bimodule then $V = \bigoplus_{i=1}^k \phi(e_i)V$ is a (H, D) decomposition. Hence $k = 1$ as above.

This lemma will be constantly applied in this investigation. To simplify notation for the crossed product algebra, we will often write H with $\bar{H}$ in mind and we may sometimes replace ζ_m with c. These abuses of notation should not cause any confusion.

7. LEMMA. *Let $C = \langle c \rangle$ be a cyclic group of order m and $C' = \langle c^d \rangle$ for some $d \mid m$, $d > 1$. Suppose that $C \leqslant M_2(D)$. Clearly if $\mathbb{Q}\{C\}$ is a field, then so is $\mathbb{Q}\{C'\}$. If every prime divisor of d divides m/d, then the converse holds. In particular this is the case when m is a prime power and $d < m$.*

Proof. We need to show the converse. Assume that $\mathbb{Q}\{C\}$ is not a field and we prove that $\mathbb{Q}\{C'\}$ is not a field either. Adopting the notation of the start of the proof of Lemma 6, we have two idempotents e_1 and e_2 in $\mathbb{Q}C$ such that $\phi(e_1)$ and $\phi(e_2)$ are nonzero, $A_i = \mathbb{Q}\{C\}\,\phi(e_i) \cong \mathbb{Q}(\zeta_{m_i})$, where $\mathrm{lcm}(m_1, m_2) = m$ and $m_1 \neq m_2$. In the above isomorphism, $\phi(c)$ $(= c)$ is mapped onto ζ_{m_i}. Letting V be the $(M_2(D), D)$ bimodule, it follows that on a basis of V adapted to the decomposition $V = A_1V \oplus A_2V$, we have $c = \left(\begin{smallmatrix} a_1 & 0 \\ 0 & a_2 \end{smallmatrix}\right)$, where a_i is a primitive m_ith root of 1 in D. Conversely, with c of the above form and $m_1 \neq m_2$, we can show that $\mathbb{Q}\{c\} \cong \mathbb{Q}(\zeta_{m_1}) \oplus \mathbb{Q}(\zeta_{m_2})$. For suppose $m_1 \nmid m_2$, then

$$c^{m_2} = \begin{pmatrix} a_1^{m_2} & 0 \\ 0 & 1 \end{pmatrix},$$

where $a_1^{m_2}$ is a primitive l root of 1 for some $l \neq 1$. Putting $f(t) = (t^l - 1)/(t - 1) \in \mathbb{Z}[t]$, we have $e = f(c^{m_2})/l = \left(\begin{smallmatrix} 0 & 0 \\ 0 & 1 \end{smallmatrix}\right)$, $ce = \left(\begin{smallmatrix} 0 & 0 \\ 0 & a_2 \end{smallmatrix}\right)$, $c(1 - e) =$

$\left(\begin{smallmatrix} a_1 & 0 \\ 0 & 0 \end{smallmatrix}\right)$ so that $\mathbb{Q}\{c\} = \mathbb{Q}\{ce\} \oplus \mathbb{Q}\{c(1-e)\}$ is the required decomposition. Now

$$c^d = \begin{pmatrix} a_1^d & 0 \\ 0 & a_2^d \end{pmatrix}$$

so by above we need to show that a_1^d and a_2^d belong to different exponents.

There is a prime p which divides m_1 and m_2 to different powers, say $p^{\alpha_1} \| m_1$, $p^{\alpha_2} \| m_2$ and $\alpha_1 > \alpha_2 \geqslant 0$. So $p^{\alpha_1} \| m$ and by assumption on d, $p^\beta \| d$, where $\beta < \alpha_1$. Hence the p-parts of the exponents of a_1^d and a_2^d are $p^{\alpha_1 - \beta}$ and $p^{\max(0, \alpha_2 - \beta)}$, which are different.

8. LEMMA. *Suppose that $R \leqslant M_2(D)$ has a self-centralising normal subgroup $C = \langle c \rangle$ of order m such that $\mathbb{Q}\{C\}$ is a field and $\mathbb{Q}\{R\} = M_2(D)$. Then R is represented imprimitively in $M_2(D)$ if and only if either of the following holds*:

(a) *$8 \mid m$ and there exists $b \in R$ such that $b^2 = 1$ and $bcb^{-1} = cz$, where $z \in C$ is of order 2.*

(b) *$4 \| m$, $O_2(R) \cong \mathscr{D}_8$, $R = R_1 \curlyvee O_2(R)$ with $F(R_1) = O_{2'}(C) \times \langle z \rangle$, and $\mathbb{Q}\{R_1\} \cong D$.*

Proof. Suppose that R is represented imprimitively in $M_2(D)$ and let H, N be the subgroups of Lemma 2. Since R consists of all the diagonal matrices H and matrices of the form $\left(\begin{smallmatrix} 0 & * \\ * & 0 \end{smallmatrix}\right)$ and $\mathbb{Q}\{R\} = M_2(D)$, we have $\mathbb{Q}\{H\} = D \oplus D$. If $C \leqslant H$, then by Lemma 6 $\mathbb{Q}\{H\}$ whould be simple, a contradiction. So $C \not\leqslant H$, $C \cap H = C^2$, and $2 \mid m$. Since $N \cap C = {}^g(N \cap C)$, $N \cap C = 1$. Also $[C^2, N] \leqslant N \cap C = 1$. Since N acts faithfully on C and centralises C^2, $|N| \leqslant 2$. If $N = 1$ then H embeds in D. Put $S = C_H(C^2)$. Since S/C^2 acts faithfully on C and centralises C^2, $|S/C^2| \leqslant 2$ and S is abelian, therefore cyclic. $\mathbb{Q}\{S\}$ is a field if $|S : C^2| = 2$, as then $4 \mid m$ and Lemma 7 applies to $C^2 < S$. Clearly $C_H(S) = S$. Thus by Lemma 6, $\mathbb{Q}\{H\}$ is simple, a contradiction. We have shown that $N = \langle b \rangle$ is of order 2, forcing $4 \mid m$ and $bcb = cz$. This is (a) if $8 \mid m$. Suppose that $4 \| m$ and write $c = c_1 c_2 = c_2 c_1$, c_1 of odd order, c_2 of order 4; c_1, $c_2 \in C$ and $bc_1 = c_1 b$, $bc_2 b^{-1} = c_2^{-1}$. Put $T = \langle b, c_2 \rangle \cong \mathscr{D}_8$.

Since R/C is abelian, $\langle c, b \rangle \lhd R$ so $T \lhd R$. Also $\langle b \rangle \leqslant Z(H)$ so the only automorphisms which are induced by conjugation from R on T are inner. Hence $R = R_1 \curlyvee T$, where $R_1 = C_G(T)$, $\langle c_1 \rangle \leqslant R_1$. We have $C_{R_1}(c_1) = R_1 \cap C_R(c) = \langle c_1 \rangle \times \langle z \rangle$. Clearly $\mathbb{Q}\{c_1, z\}$ and $\mathbb{Q}\{c_2\}$ are fields so by Lemma 6, $\mathbb{Q}\{R_1\}$ is a simple algebra and $\mathbb{Q}\{T\} \cong M_2(\mathbb{Q})$. By Lemma 4(a), $\mathbb{Q}\{R_1 \curlyvee T\} = \mathbb{Q}\{R_1\} \otimes_{\mathbb{Q}} M_2(\mathbb{Q})$ so $\mathbb{Q}\{R_1\} \cong D$. Applying 1.5(d) to R_1, one concludes easily that R_1 has cyclic Sylow subgroups, so that $F(R_1) = \langle c_1 \rangle \times \langle z \rangle$ and $O_2(R) = O_2(R_1)T = T$. For the converse,

write $c = c_1 c_2$ as before. Then $\langle c, b\rangle = \langle c_1\rangle \times \langle c_2, b\rangle$ and $\langle c_2, b\rangle \lhd R$. In both bases $\langle c_2^2, b\rangle$ is an abelian noncyclic normal subgroup of R. Therefore R is imprimitive by Lemma 9 below.

9. LEMMA. *If N is normal in H and $H \leqslant M_2(D)$ is a primitive group then $\mathbb{Q}\{N\}$ is simple. So if N is abelian as well then it is cyclic.*

Proof. $\mathbb{Q}\{N\}$ is semisimple. If not simple, then $\mathbb{Q}\{N\} = A_1 \oplus A_2$ with the central idempotents e_1, e_2. These are the only primitive central idempotents in $\mathbb{Q}\{N\}$. Let $h \in H$. Then $he_ih^{-1} \in \mathbb{Q}\{N\}$ is a central primitive idempotent of $\mathbb{Q}\{N\}$ so $he_ih^{-1} = e_j$ $i, j = 1$ or 2. Hence $V = e_1V \oplus e_2V$ gives an imprimitive representation of H, a contradiction (as usual V is the (H, D) bimodule).

The idea of this lemma extends to other situations. For instance, if N_1, $N_2 \lhd H$ and $[N_1, N_2] = 1$ then $Z_1 = Z(\mathbb{Q}\{N_1\})$ and $Z_2 = Z(\mathbb{Q}\{N_2\})$ generate a field so that case (a) of Lemma 4 applies to $\mathbb{Q}\{N_1N_2\}$.

Now we give some information on special subgroups of $M_2(D)$.

10. LEMMA. (a) *An abelian subgroup C of $M_2(D)$ has rank at most* 2.

(b) *A p-subgroup P of $M_2(D)$ is abelian for odd p.*

(c) *A 2-subgroup S of $M_2(D)$ is abelian or has an abelian subgroup of index* 2 *or is a subdirect product of 2 groups or $|Z(S)| = 2$ and there is an abelian normal subgroup L of S with $S/L \cong \mathscr{D}_8$. Hence the rank of any abelian section of S is at most* 4.

Proof. (a) Since $M_2(D)$ has at most two orthogonal idempotents, $\mathbb{Q}\{C\}$ is at most the direct sum of two fields. So $\operatorname{rank}(C) \leqslant 2$.

(b) As above $\mathbb{Q}\{P\}$ is at most the direct sum of two components. These occur in $\mathbb{Q}P$. By [25], $\mathbb{Q}P$ is the direct sum of matrix algebras over fields, and their sizes are character degrees of P, i.e., odd numbers. So $\mathbb{Q}\{P\}$ is the direct sum of fields and P is abelian.

(c) Again we apply [25]. So either S has a cyclic subgroup of index 2 or the representation of S is imprimitive. If S is reducible, then the two diagonal entries form two subgroups of $D^\times$ which are therefore cyclic or 2 groups. So S is abelian or has an abelian subgroup of index 2 or is a subdirect product of 2 groups. Now suppose that S is monomial and let H, N be the subgroups of Lemma 1. $H/N \subsetneq D$ so it is cyclic or 2. If cyclic, then $H \subsetneq H/N \times H/{}^gN$ is abelian. So suppose $H/N \cong 2$. If $Z(S) \leqslant H$ then $Z(S) \cap N = 1$ and $Z(S) \to Z(H/N)$ of order 2. Therefore $|Z(S)| = 2$. Let H_1/N be a cyclic subgroup of index 2 in H/N. Then $L = H_1 \cap gH_1g^{-1}$ is abelian with $S/L \cong \mathscr{D}_8$. If $Z(S) \not\leqslant H$ then we can take $g \in Z(S)$ so $N = 1$ and H is cyclic or quaternion. Hence $S = \langle Z(S), H\rangle$ is abelian or has an abelian subgroup of index 2.

The classification of G in the soluble case is based on the following lemma. Recall that G is a primitive subgroup of $M_2(D)$ which spans $M_2(D)$ over $\mathbb{Q}$.

11. LEMMA. *$O_{2'}(F(G))$ is cyclic. $O_2(G)$ is one of the groups*

$$\mathscr{C},\ \mathscr{D},\ \mathscr{S},\ \mathscr{Q},\ \mathscr{Q}_8 \Upsilon \mathscr{C} \cong \mathscr{D}_8 \Upsilon \mathscr{C},\ \mathscr{Q}_8 \Upsilon \mathscr{D}_{2^n} \cong \mathscr{D}_8 \Upsilon \mathscr{Q}_{2^n},\ n \geqslant 3.$$

Proof. $O_{2'}(F(G))$ is cyclic by Lemmas 9 and 10. By Lemma 9 any characteristic abelian subgroup of $O_2(G)$ is cyclic. By a result of P. Hall [18, Chap. III, 13.10], $O_2(G)$ is the central product of an extraspecial group with a $\mathscr{C}$, $\mathscr{Q}$, $\mathscr{D}$, or $\mathscr{S}$ group. Since any abelian section of $O_2(G)$ has rank at most 4, it can be seen easily that there are at most two factors in a complete central decomposition of $O_2(G)$. Consideration of the various possibilities with the use of Lemmas 4 and 6 leaves the above possibilities only. Note that $\mathbb{Q}\{O_2(G)\}$ is simple by Lemma 9 so that by Lemma 4, the enveloping algebra of each factor of $O_2(G)$ is simple. We illustrate a typical calculation. Let $O_2(G) = C \Upsilon C'$, where $C \cong \mathscr{Q}_8$, $C' \cong \mathscr{S}_{2^{n+1}}$, $n \geqslant 3$. By Lemma 6, $\mathbb{Q}\{C\} \cong \mathscr{A}$, $\mathbb{Q}\{C'\} \cong \langle \mathbb{Q}(\zeta_{2^n}), \sigma, 1 \rangle \cong M_2(K)$, where $\sigma\colon \zeta_{2^n} \to -\zeta_{2^n}^{-1}$ and $K = \mathbb{Q}(\zeta_{2^n} - \zeta_{2^n}^{-1})$. Hence $\mathbb{Q}\{O_2(G)\} \cong (\mathscr{A} \otimes_{\mathbb{Q}} K) \otimes_K M_2(K)$. Now K splits $\mathscr{A}$ since the nonzero invariants of $\mathscr{A}$ are at ∞ and 2, but K is complex and $|K\mathbb{Q}_2 : \mathbb{Q}| = 2^{n-2}$ is even. So $\mathbb{Q}\{O_2(G)\} \cong M_4(K)$, a contradiction.

12. For reasons which will be clarified in Sections 3 and 4, below, we divide the isomorphism types of $O_2(G)$ into the following two classes which will require different techniques for the classification of a soluble group G:

(1) $O_2(G) \cong \mathscr{C}$, $\mathscr{D}$, $\mathscr{S}$, $\mathscr{Q}$ including $\mathscr{Q}_8$ provided that no element of G induces an automorphism of order 3 on $O_2(G)$.

(2) $O_2(G) \cong \mathscr{Q}_8 \Upsilon \mathscr{C}$, $\mathscr{Q}_8 \Upsilon \mathscr{D}_{2^{n+1}}$, $n \geqslant 3$, $\mathscr{Q}_8 \Upsilon \mathscr{D}_8$ or $\mathscr{Q}_8$, where G induces an automorphism of order 3 on $O_2(G)$.

In the next two sections the group theoretic structure of G in the soluble case will be completely determined.

13. We need to know about the automorphism groups of the 2-groups T occurring in 2.12 as well as the groups $SL(2, 5)$, $SL(2, 9)$. Employing the notation described following the Introduction, we have:

(a) $T = \langle a, b \rangle \Upsilon_2 \langle c \rangle \cong \mathscr{Q}_8 \Upsilon \mathscr{C}_{2^\alpha}$. $\langle a, b \rangle$ and $\langle c \rangle$ are characteristic in T. Thus $\mathrm{Aut}(T) = \mathrm{Aut}\langle a, b \rangle \times \mathrm{Aut}\langle c \rangle$.

(b) $T = \langle a, b \rangle \Upsilon_2 \langle c, d \rangle \cong \mathscr{Q}_8 \Upsilon \mathscr{D}_{2^{\alpha+1}}$, $\alpha \geqslant 3$. $\langle a, b \rangle \Upsilon \langle c \rangle = \langle g \in T;$ g has order $2^\alpha \rangle$. It follows that $\langle a, b \rangle$, $\langle c \rangle$, $\langle c, d \rangle$ are characteristic in T. Thus $\mathrm{Aut}(T) = \mathrm{Aut}\langle a, b \rangle \Upsilon \mathrm{Aut}\langle c, d \rangle$.

(c) $T = \langle a, b \rangle \Upsilon_2 \langle c, d \rangle \cong \mathscr{Q}_8 \Upsilon \mathscr{D}_8$.

Any automorphism of T induces an automorphism on $\bar{T} = T/Z(T)$. By [8, Lemma 34.5] the inner automorphisms are precisely the ones which are identity on $\bar{T}$. Now $\bar{T}$ is a 4-dimensional $\mathbb{F}_2$-space, with the basis $\bar{a}, \bar{b}, \overline{cd}, \bar{d}$, where for $g \in T$, denote $gZ(T)$ by $\bar{g}$. Put $Z(T) = \langle z \rangle$. For $\bar{g}, \bar{h} \in \bar{T}$, let $g^2 = z^\alpha$, $[g, h] = z^\beta$ and put $\mathrm{q}(\bar{g}) = \alpha$, $(\bar{g}, \bar{h}) = \beta$. Then q: $\bar{T} \to \mathbb{F}_2$; $(*,*)$: $\bar{T} \times \bar{T} \to \mathbb{F}_2$ are a nonsingular quadratic form and its symplectic bilinear form. In fact $\mathrm{q}(\bar{a}^x \bar{b}^y (\overline{cd})^u \bar{d}^v) = x^2 + xy + y^2 + uv$, where $x, y, u, v \in \mathbb{F}_2$. This quadratic form is sufficient to specify the multiplication of T [16, Chap. 3, Satz 13.8]. It is clear now that the outer automorphism group of T is isomorphically mapped onto the orthogonal group $O(\bar{T}, \mathrm{q})$ of q ($O_4^-(2)$ in the notation of [4]). Dickson shows [7, p. 205] that $|O_4^-(2)| = 120$. In fact $O_4^-(2) \cong \mathrm{Sym}_5$. It is enough to show that Sym_5 can be embedded in $O_4^-(2)$. Put $e_1 = a$, $e_2 = b$, $e_3 = abd$, $e_4 = abcd$. Then $T = \langle e_i;\ 1 \leqslant i \leqslant 4 \rangle$ with the relations $e_i^2 = z$, $e_i e_j = z e_j e_i$, $i \neq j$. Let $V' = \sum_1^5 \mathbb{F}_2 v_i$ be the permutation module for Sym_5 over $\mathbb{F}_2$ and let $V = \{\sum_1^5 a_i v_i;\ a_i \in \mathbb{F}_2,\ \sum_1 a_i = 0\}$ be its nontrivial summand. It is easily verified that under the map ϕ: $\bar{T} \to V$, ϕ: $e_i \to v_i + v_5$, $1 \leqslant i \leqslant 4$, the group Sym_5 can be pulled back to a subgroup of $O_4^-(2)$. This shows $\mathrm{Out}(T) \cong \mathrm{Sym}_5$ and moreover $\mathrm{Inn}(T) \cong \bar{T} \cong V$ as an $\mathbb{F}_2$-module over $\mathrm{Out}\, T \cong \mathrm{Sym}_5$. We remark that V is a projective Alt_5 module. If S is the Sylow 2-subgroup of Alt_5 which fixes the letter 5, we need only to prove that V is a projective $\mathbb{F}_2 S$-module [17, Chap. VII, Theorem 7.11]. But that is clear, for $V \cong \mathbb{F}_2 S$. Now we show that $R = \mathrm{Aut}(T)$ is split over $N = \mathrm{Inn}(T)$. Put $\bar{R} = R/N \cong \mathrm{Sym}_5$ and let $\alpha \in H^2(\bar{R}, N)$ denote the cohomology class of the extension $1 \to N \to R \to \bar{R} \to 1$. For $\sigma \in \mathrm{Sym}_4$, define $h_\sigma \in R$ by $h_\sigma(e_i) = e_{\sigma(i)}$ and put $H_1 = \{h_\sigma;\ \sigma \in \mathrm{Sym}_4\}$, $R_1 = NH_1$. H_1 is a group of outer automorphisms of T. Now $\alpha|_{\bar{R}_1} = 0$ for R_1 is split over N. Since $|R : R_1|$ is coprime to 2, Res: $H^2(\bar{R}, N) \to H^2(\bar{R}_1, N)$ is a monomorphism. Thus $\alpha = 0$ as required. Explicitly, one can verify that $H = \langle H_1, \chi \rangle$ is a complement to N, where χ: $e_1 \to e_1^{-1}$, $e_2 \to e_1 e_2$, $e_3 \to e_1 e_3$, $e_4 \to e_1 e_4$ represents (15). In future sections, we will take the action of Sym_5 on T to be via H.

(d) $T \cong SL(2, 5)$ or $SL(2, 9)$.

Observe that $\bar{T} = T/Z(T) \cong \mathrm{Alt}_5$ or Alt_6. Since T is perfect, $\mathrm{Out}(T) \supsetneq \mathrm{Out}(\bar{T}) \cong \mathscr{C}_2$ or $\mathscr{C}_2 \times \mathscr{C}_2$ by [23, Chap. 1, 3.7]. Conversely one can verify that conjugation from $GL(2, 5)$ or $GL(2, 9)$ on T in addition to the extension of the Galois automorphism of $\mathbb{F}_9$ to $SL(2, 9)$ are outer automorphisms of T. Thus $\mathrm{Out}(T) \cong \mathscr{C}_2$ or $\mathscr{C}_2 \times \mathscr{C}_2$.

14. LEMMA. *Let H_i $(i = 1, 2)$ be a finite subgroup of the simple algebra A_i (with the same identity) and span it over $\mathbb{Q}$. Put $C_i = Z(H_i)$, $K_i = Z(A_i)$.*

(a) *K_i is a cyclotomic field. C_i is cyclic and $C_i \leqslant K_i$.*

(b) *Putting* $K = K_1K_2$ *the composite of* K_1 *and* K_2 *and* $m = (|C_1|, |C_2|)$, *the group* $H = H_1 \Upsilon_m H_2$, *is a subgroup of the simple algebra* $A = (A_1 \otimes_{K_1} K) \otimes_K (A_2 \otimes_{K_2} K)$ *and spans it over* $\mathbb{Q}$. *Here* Υ_m *denotes that the subgroups of order* m *of* C_1 *and* C_2 *are to be identified.*

Proof. (a) The epimorphism $\mathbb{Q}H_i \to A_i$ identifies A_i as a simple component of $\mathbb{Q}H_i$. Hence K_i is cyclotomic by 1.4. Clearly $C_i \leqslant K_i$. Thus C_i is cyclic.

(b) Let $Z = K_1 \cap K_2$. Since K/Z is Galois, $|K : K_2| = |K_1 : Z|$ and $K = K_1 \otimes_Z K_2$. In a natural way, therefore $A = A_1 \otimes_Z A_2$. Now regard A_1 and A_2 and their subgroups H_1, H_2 inside A. Clearly H_1 and H_2 commute and $\mathbb{Q}\{H_1H_2\} = A$. We need to show $|H_1 \cap H_2| = m$. Note that $A_1 \cap A_2 = Z$, $H_1 \cap H_2 = C_1 \cap C_2$. Since $m \mid |C_i|$, $\mathbb{Q}(\zeta_m)$ is a subfield of K_1 and K_2 by (a). So $\mathbb{Q}(\zeta_m) \leqslant Z$. Hence the subgroups of order m in C_1 and C_2 are the group of mth roots of 1 in Z. Thus they coincide and $m \mid |C_1 \cap C_2|$. Clearly $|C_1 \cap C_2| \mid m$. This proves $|C_1 \cap C_2| = m$ so that $H = H_1 \Upsilon_m H_2$.

As an application we see that $\mathscr{Q}_8 \Upsilon \mathscr{D}_8$ is a spanning subgroup of $M_2(\mathscr{A})$.

3. Soluble Groups I

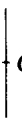
1. In this section we assume that G is a soluble group and $O_2(G)$ is of type (1) in 2.12. The aim is to determine the group theoretic structure of G. It turns out that G is 2-nilpotent and belongs to one of four different classes, each consisting of a few different types. Class 1 groups are metacyclic with each type depending on two integer parameters. Class 2 groups have a metacyclic subgroup of index 2 and depend on three integer parameters for each type. Class 3 groups can be factored into the central (or direct) product of two groups of class 1 except for one type where one factor is of class 2. Finally, there are two very specific types in class 4 and they depend on two parameters. In each type a necessary set of conditions on the parameters of G will be given. The complete set of conditions on these parameters, ensuring that $\mathbb{Q}\{G\}$ is a 2×2 matrix ring over a division algebra, is worked out for some illustrative examples in Section 6. Suffice it to remark that for each type in the four classes, there exist integer values for the parameters ensuring that the above holds.

We begin by obtaining the structure of a Sylow 2-subgroup of G. Let $C = \langle c \rangle$ be $O_2(G)$ if it is cyclic, the cyclic subgroup of index 2 in $O_2(G)$ if it is $\mathscr{D}$, $\mathscr{S}$, $\mathscr{Q}_{2^{\alpha+1}}$, $\alpha \geqslant 3$, and a 4 cycle in $O_2(G)$ which is normal in G if $O_2(G) \cong \mathscr{Q}_8$. So $C \lhd G$. Put $M = C \times O_{2'}(F(G))$. M is a cyclic self-centralising normal subgroup of G. For if $G_1 = C_G(C)$, then $F(G_1) = F(G) \cap G_1 = M$. Therefore by a theorem on Fitting subgroups of soluble

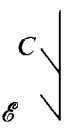
groups $C_{G_1}(M) = M$. Hence $C_G(M) = C_{G_1}(M) = M$. The structure of a Sylow 2-subgroup of G is determined in the following lemma.

2. LEMMA. *Let $R \leqslant M_2(D)$ be a finite group with the cyclic self-centralising normal subgroup M. Suppose that $\mathbb{Q}\{M\}$ is a field. Put $O_2(M) = C = \langle c \rangle$, $|C| = 2^\alpha$, $\alpha \geqslant 0$, and $|O_{2'}(M)| = m$. Then a Sylow 2-subgroup S of R has one of the following types:*

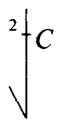
Class 1: $S \cong \mathscr{C}$, $\mathscr{D}$, $\mathscr{Q}$, $\mathscr{S}$, $\mathscr{E}$; S/C *is cyclic.*

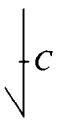
(a) $\mathscr{C}$ 

(b) $\mathscr{D}$, $\mathscr{Q}$, $\mathscr{S}$ 

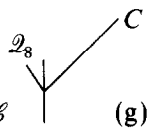
(c) $\mathscr{E}$ 

Class 2: $S = \mathscr{D}$, $\mathscr{Q}$, $\mathscr{S}$, $\mathscr{E}$; S/C *of rank* 2.

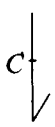
(d) $\mathscr{D}$, $\mathscr{Q}$, $\mathscr{S}$ 

(e) $\mathscr{E}$ 

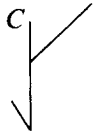
Class 3: *S is the direct or central product of class* 1 *groups except for case* (f), *where $\mathscr{Q}_8$ belongs to class* 2.

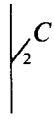
(f) $\mathscr{Q}_8 \mathbin{Y} \mathscr{C}$ 

(g) $\mathscr{Q} \times \mathscr{C}_2$ 

(h) $\mathscr{C} \times \mathscr{C}_2$ 

(i) $\mathscr{D}$, $\mathscr{Q}$, $\mathscr{S} \mathbin{Y} \mathscr{C}_4$ 

(j) $\mathscr{E} \mathbin{Y} \mathscr{C}$ 

(k) $\mathscr{C} \times \mathscr{C}_2$ 

Class 4: $S = \langle a, b, c \rangle$.

$aca^{-1} = c^{-1}$, $bcb^{-1} = cz$, $a^2 = z$, $ab = ba$, $c^{2^\alpha} = 1$ $(\alpha \geqslant 3)$, $z \in \langle c \rangle$ *of order* 2, $(l_1)b^2 = 1$, $(l_2)b^2 = z$.

Proof. The following fact is easily established.

Suppose that $X = \langle a \rangle$ is cyclic of order 2^n, $n \geqslant 3$, and σ: $a \to a^{\pm(1+2^k)}$, $2 \leqslant k < n$, is an automorphism of X of order 2^{n-k}. Then any extension of X by $\langle \sigma \rangle$ is split. (*)

We observe that S enjoys the following two properties.

P1. S/C acts faithfully on the cyclic group M and is abelian.

P2. There is no subgroup H of S with $|H| \geqslant 4$ and $H \cap C = 1$, otherwise by Lemma 2.6, $\mathbb{Q}\{H, M\} \cong \langle \mathbb{Q}(\zeta_m), H, 1 \rangle \cong M_{|H|}(*)$, a contradiction.

If $m = 1$, i.e., $M = C$, then $R = S$ and by $(*)$ and P2, $|S/C| \leqslant 2$. Clearly then S is one of the groups in (a), (b), or (c). Thus we can assume from now on that $m > 1$. If $\alpha = 0$, then by P2, $|S| \leqslant 2$. This gives (a). Let $\alpha = 1$. Let $S_1/C = \Omega_1(S/C)$, $C = \langle z \rangle$. $\mathbb{Q}\{S_1, M\} \cong \langle \mathbb{Q}(\zeta_m), S_1/C, * \rangle$, which by Lemma 2.3 is the tensor product of algebras of index 2. So the exponent is at most 2 and therefore its index is at most 4. So $\operatorname{rank}(S/C) \leqslant 2$. If this rank is 1, then S is cyclic or $S \cong C \times \text{Cyclic}$. In the first case, $A = \mathbb{Q}\{S, M\} \cong \langle \mathbb{Q}(\zeta_m), S/C, -1 \rangle$ is a cyclic algebra of exponent at most 2, since $A^2 \sim \langle \mathbb{Q}(\zeta_m), S/C, 1 \rangle$ is split. Hence $|S| \leqslant 8$. For the second case by P2, $S = C \times C_2$. These two groups are covered under (a) and (h). Now suppose that $\operatorname{rank}(S/C) = 2$ and H is a maximal abelian subgroup of S. So $C \leqslant H$ and $C_S(H) = H$. By a reasoning similar to that above, one sees that either H is cyclic of size $\leqslant 8$ or $H = \langle a \rangle \times \langle b \rangle$, where $|\langle a \rangle| \leqslant 4$, $b^2 = 1$ and $C \leqslant \langle a \rangle$. $S = H$ is covered under (h). So suppose that $H < S$. If $H \cong \mathscr{C}_4$ then $S \cong \mathscr{D}_8$ or $\mathscr{Q}_8$. If $H \cong \mathscr{C}_8$ then by P1 $S \cong \mathscr{E}_{16}$. If $H \cong C \times \mathscr{C}_2$ then clearly $S \cong \mathscr{D}_8$. Finally, if $H = \langle a \rangle \times \langle b \rangle$ is of order 8, then $|S/H| \leqslant 4$ for S/H acts faithfully on H and centralises H/C. If we have $d \in S$, d: $a \to az$ $b \to b$ (recall that this means ${}^d a = az$, ${}^d b = b$), then $d^2 \in H$ and in fact $d^2 \in \langle z, b \rangle$. We must have $d^2 = b$ or zb as rank $(S/C) = 2$. But then $|\langle d \rangle| = 4$ and $\langle d \rangle \cap C = 1$, a contradiction to P2. Hence $|S/H| = 2$ and $d \in S \backslash H$ induces $a \to a$, $b \to bz$ (if we have d: $a \to az$, $b \to bz$, then replace a by ab). Now $d^2 \in \langle a \rangle$. By replacing d by $a^* d$, we can make $d^2 = 1$ or a. As $\operatorname{rank}(S/C) = 2$, we have $d^2 = a$ so that $S \cong \mathscr{E}_{16}$. Actually, we can rule out $\mathscr{E}_{16}$ as follows. Let $S = \langle a, b; a^8 = 1, b^2 = 1, bab^{-1} = az \rangle$. Choose $g, g' \in M$ to be of prime order p, q such that $\bar{S} = S/C$ acts faithfully on $\langle g, g' \rangle$. In $\mathbb{Q}(\zeta_{pq})$, let E, K be the fixed fields of b, $\bar{S}$ and $A = \mathbb{Q}\{S, g, g'\}$. By renaming g and g' if needed, one sees that one of the following must hold:

1. b inverts g and a acts with order $\leqslant 2$ on g, that is, $[a^2, g] = 1$. By the technique of Lemma 2.3, b and $a' = a(\zeta_p - \zeta_p^{-1})$ commute in A and $\gamma = a'^4 = -(\zeta_p - \zeta_p^{-1})^4$. Now $A = M_2(K) \otimes_K \langle E/K, a', \gamma \rangle$ and the latter algebra has exponent $\leqslant 2$ because $\gamma^2 = (\zeta_p^2 + \zeta_p^{-2} - 2)^4$ is a 4th power in K. So A has size 4 or 8, a contradiction.

2. b inverts g and a acts on both g, g' with order 4 so that $p \equiv q \equiv 1(4)$. Let δ be a 4th root of 1 mod p. Thus a: $\zeta_p \to \zeta_p^\delta$. Again b and $a' = a(\zeta_p - \zeta_p^{-1})$ commute and $\gamma = a'^4 = -(\zeta_p^\delta - \zeta_p^{-\delta})^2 (\zeta_p - \zeta_p^{-1})^2$. The

algebra $\langle E/K, a', \gamma \rangle$ has again exponent $\leqslant 2$, for γ^2 is the norm of $(\zeta_p^{\delta} - \zeta_p^{-\delta})(\zeta_p - \zeta_p^{-1}) \in E$. Contradiction.

Now we consider the case when $\alpha \geqslant 2$. Put $T = C_S(C)$ and $z = c^{2^{\alpha-1}}$. We begin by finding the structure of T. It will turn out that there are five types possible, listed in (A)–(E) below. Once this is done, the structure of S will be determined for each case. To start with, let T be abelian. Then $\operatorname{rank}(T) \leqslant 2$ and T does not have a $\mathscr{C}_4 \times \mathscr{C}_4$ subgroup by P2. Thus there are three possibilities for $C \leqslant T$:

(A) $T = \langle a \rangle \cong \mathscr{C}_{2^\beta}$,

(B) $T = \langle a \rangle \times \langle b \rangle = \mathscr{C}_{2^\beta} \times \mathscr{C}_2$, $\beta \geqslant \alpha + 1$, $C = \langle a^{2^{\beta-\alpha}} b \rangle$,

(C) $T = \langle a \rangle \times \langle b \rangle \cong \mathscr{C}_{2^\beta} \times \mathscr{C}_2$, $\beta \geqslant \alpha$, $C = \langle a^{2^{\beta-\alpha}} \rangle$.

Now assume that T is not abelian. Let H be a maximal abelian subgroup of T. So $C \leqslant H$, $H \lhd T$, and $C_T(H) = H$. Clearly H can be of the types in (A), (B), (C) above. First let $H = \langle a \rangle$ be cyclic. Then $|T/H| = 2$ by (*) and the automorphism on H is $a \to az$ (for $C \leqslant Z(T)$) and we get

(D) $T = \mathscr{E}_{2^{\beta+1}} = \langle a, b \rangle$, $a^{2^\beta} = 1$, $b^2 = 1$, $bab^{-1} = az$, and $C \leqslant \langle a \rangle$.

Next, let $H = \langle a \rangle \times \langle b \rangle$; $a^{2^\beta} = 1$, $b^2 = 1$, $C = \langle a^{2^{\beta-\alpha}} b \rangle$, $\beta > \alpha$ and pick $d \in T$ to be of order 2 mod H. Then d: $a \to ax$, $b \to bx'$; $x, x' \in C$ and $x^2 = x'^2 = 1$. Since d centralises C, $x' = 1$ so d: $a \to az$, $b \to b$. We can make $d^2 \in \langle b \rangle$ but then $\langle d, b \rangle$ gives a contradiction to P2. So this case is not possible. Finally, let $H = \langle a \rangle \times \langle b \rangle$; $a^{2^\beta} = 1$, $b^2 = 1$; $C \leqslant \langle a \rangle$. We want to show that $|T/H| = 2$. If $d \in T$ has order 4 mod H and d: $a \to ax$, $b \to bx'$ $x, x' \in C$, then $x^4 = x'^2 = 1$ and $x^2 \neq 1$. Hence $e = d^2$: $a \to az$, $b \to b$. Similarly if $T/H \cong \mathscr{C}_2 \times \mathscr{C}_2$, then we can again find $e \in T$ such that e: $a \to az$, $b \to b$. But then we can make $e^2 \in \langle b \rangle$ so $\langle e, b \rangle$ gives a contradiction to P2. So $|T/H| = 2$ and $d \in T \backslash H$ induces $a \to a$, $b \to bz$ (if d: $a \to az$, $b \to bz$, then $\beta \geqslant \alpha + 1$ and replace a by ab). Make $d^2 = a$ or 1. In the first case we get (D) again. For the second we get $T = \langle a \rangle \curlyvee \mathscr{D}_8$. If $\langle a \rangle > C$, then take $a' \in \langle a \rangle$ such that $a'^2 = a$. Then $\mathbb{Q}\{a', b, d, M\}$ is by Lemma 2.3 of exponent $\leqslant 2$ and index 8, a contradiction. So in fact

(E) $T \cong C \curlyvee \mathscr{D}_8 \cong C \curlyvee \mathscr{Q}_8$. (Here $\mathscr{Q}_8 = \langle c^{2^{\alpha-2}} b, c^{2^{\alpha-2}} d \rangle$.)

Now we consider the whole of S for each type (A)–(E). Note that S/T is a group of automorphisms of C and $|C| = 2^\alpha \geqslant 4$.

(A) If $\langle a \rangle > C$, then $a \to az$ induces the identity on C, hence it is not induced from S. So $|S/T| \leqslant 2$ and is of order 2 only if $T : C| = 2$ for T/C must be centralised by S. Thus in this case we get the groups (a) or (d). Now suppose $T = C$. By (*) and P2, S/C is elementary abelian of order at most 4. If $|S/C| = 2$ then $S \cong \mathscr{D}$, $\mathscr{Q}$, $\mathscr{S}$, $\mathscr{E}$ given in (b) and (c). Note that

when $S=\langle a, b\rangle \cong \mathscr{E}$; $a^{2^\alpha}=1$, $b^2=1$, $\alpha \geqslant 3$, we do indeed get (c) because $S=\langle a, b'\rangle$; $b'=a^{1+2^{\alpha-2}}b$, $b'^2=a^2$. Now suppose $|S/C|=4$, $\alpha \geqslant 3$. We can find a, $b \in S$ such that $aca^{-1}=c^{-1}$, $bcb^{-1}=cz$, $a^2=1$ or z, $b^2=1$ and $aba^{-1}=xb$, $x \in C$. Then $1=ab^2a^{-1}=xbxb=x\cdot {}^b x$. So $x=1$ or z. If $x=z$, then replace b by $c^{2^{\alpha-2}}b$. Then $ab=ba$, $b^2=1$ or z. If $a^2=1$, then using Lemma 2.3 and that $\mathbb{Q}\{C\}$ is a field, we see that

$$\mathbb{Q}\{S\}=\langle \mathbb{Q}(\zeta^2)/K,\ a,\ 1\rangle \otimes_K \langle E/K,\ b,\ \pm 1\rangle,$$

where $\zeta=\zeta_{2^\alpha}$, $E=\mathbb{Q}(\zeta+\zeta^{-1})$, and $K=\mathbb{Q}(\zeta^2+\zeta^{-2})$. Now $-1 \in \mathscr{N}_{E/K}$. To prove that, by Hasse's norm theorem we must show that $-1 \in \mathscr{N}_{E_\mathfrak{P}/K_\mathfrak{p}}$ for each prime divisor $\mathfrak{P} \mid \mathfrak{p}$ of E/K. Since E/K is unramified outside 2 and -1 is a unit, we need to consider $\mathfrak{p} \mid 2$ only. There, using the standard properties of the norm residue symbol, we have

$$(-1, E_\mathfrak{P}/K_\mathfrak{p})=(N_{K_\mathfrak{p}/\mathbb{Q}_2}(-1),\ \mathbb{Q}_2(\zeta)/\mathbb{Q}_2)|_{E_\mathfrak{P}}=1,$$

since $(\pm 1,\ \mathbb{Q}_2(\zeta)/\mathbb{Q}_2)$: $\zeta \to \zeta^{\pm 1}$. This shows that $\mathbb{Q}\{S\}=M_4(K)$, a contradiction. Hence $a^2=z$ and we get the two groups of class 4.

(B) Again, we show that $|S/T| \leqslant 2$. Let $d \in S$ be order 2 mod T and suppose d: $b \to b$. We get a contradiction. Let $r=\beta-\alpha$, $c=a^{2^r}b$, and d: $a \to ax$, $x \in C$. Then d: $c \to cx^{2^r}$ and $x\cdot {}^d x=1$ because $d^2 \in T$. Now consider the possible automorphisms induced on C.

(1) d: $c \to c^{-1}$. So $x^{2^r}=c^{-2}$, $r=1$, and $x=c^{-1}$ or $c^{-1}z$. Now $d^2 \in \langle a, b\rangle$ is fixed by d so $d^2 \in \langle z, b\rangle$. If we have $d^2=1$ or b or zb then $\langle d, b\rangle$ gives a contradiction to P2. So $d^2=z$. Now using the technique of Lemma 2.3, d commutes with $a'=a(1+\zeta^{-1})$ or $a(1-\zeta^{-1})$, where $\zeta=c$ is a 2^αth root of 1. So $A=\mathbb{Q}\{d, T, M\}$ can be written as the tensor product of two crossed product algebras, one with d of exponent $\leqslant 2$ and the other with a' and $a'^4=\zeta^2(1\pm\zeta^{-1})^4=(\zeta+\zeta^{-1}\pm 2)^2$. Since the centre of this latter algebra contains $\mathbb{Q}(\zeta\pm\zeta^{-1})$, its exponent is $\leqslant 2$ and hence so is the exponent of A, a contradiction.

Therefore for the remaining two possibilities, we can assume that $\alpha \geqslant 3$:

(2) d: $c \to c^{-1}z$. Then $x^{2^r}=c^{-2}z$ so $r=1$ and $x^2=c^{-2}z$. Since $x\cdot {}^d x=1$, $x \in \langle c^2\rangle$. But then $x^2=c^{-2}z$ cannot hold. Contradiction.

(3) d: $c \to cz$. So $x^{2^r}=z$ and $x\cdot {}^d x=1$. If $x \in \langle c^2\rangle$ then ${}^d x=x$ and $x^2=1$, a contradiction. Otherwise ${}^d x=xz$ so $x^2=z$, $|C|=4$, a contradiction as we assumed $|C| \geqslant 8$.

It follows now that $|S/T| \leqslant 2$, because otherwise we can find $d \in S$ of order 2 mod T such that d: $b \to b$. We get the group (k) if $S=T$. So suppose that $|S/T|=2$ and $d \in S\backslash T$, d: $a \to ax$, $b \to bz$, $x \in C$. We have d:

$c \to cx^{2^r}z$, $x \cdot {}^d x = 1$. Again we distinguish the three possible automorphisms induced by d on C. For the first two, we can assume that $\alpha \geqslant 3$:

(1) d: $c \to c^{-1}$. So $x^{2^r}z = c^{-2}$, $r = 1$, and $x = c^{-1}z'$, where $z'^2 = z$, $z' \in C$. We have $d^2 \in \langle a, b \rangle$ and $(ad)^2 = a$. ${}^d ad^2 = d^2 bz'$. So we can make $d^2 \in \langle a \rangle$. Then $d^2 \in \langle z \rangle$ and like (1) previously d commutes with $a' = a(1+\zeta)$, where $\zeta = x$ is a 2^αth root of 1, $a'^4 = -\zeta^{-2}(1+\zeta)^4 = -(\zeta + \zeta^{-1} + 2)^2$ so the factors of $A = \mathbb{Q}\{d, T, M\}$ have exponent $\leqslant 2$, as $\zeta + \zeta^{-1} \in Z(A)$. Contradiction.

(2) d: $c \to c^{-1}z$. So $x^{2^r} = c^{-2}$, $r = 1$, and $x = c^{-1}$ or $c^{-1}z$. Contradiction to $x^d x = 1$.

(3) d: $c \to cz$, $b \to bz$, and $\alpha \geqslant 2$. We have $x^{2^r} = 1$, $x \cdot {}^d x = 1$. If $x \notin \langle c^2 \rangle$, then ${}^d x = xz$, $x^2 z = 1$ so $\alpha = 2$ and $r \geqslant 2$. But then $\mathbb{Q}\{a, M\}$ is a crossed product algebra with $a^{2^{r+1}} = -1$, so its exponent is $\leqslant 2$ and the index is 2^{r+1}, a contradiction. Therefore $x \in \langle c^2 \rangle$, ${}^d x = x$, and $x \in \langle z \rangle$. By replacing a with ab if needed, we get d: $a \to a$, $b \to bz$. So $d^2 \in \langle a \rangle$. We can make either $d^2 = a$ giving the group (c) or $d^2 = 1$ so that $S = \langle d, c \rangle \, Y \, \langle a \rangle$ is of type (j). Actually then $\alpha \geqslant 3$. For if $\alpha = 2$, then $\mathbb{Q}\{S, M\}$ has index $2^\beta \geqslant 8$ and is the tensor product of two crossed product algebras both of which have exponent $\leqslant 2$. Contradiction.

(C) Clearly, here $\langle a \rangle$ is normalised by S. If $S = T$ then we get the group (h). So suppose that $S > T$ and $d \in S$ is of order 2 mod T. We will show $\beta = \alpha$. If $\beta \geqslant \alpha + 2$ then d: $a \to az$ because d must centralise T/C. But d is then identity on C, a contradiction. Next, if $\beta = \alpha + 1$, then d: $a \to a^{-1}$ or $a^{-1}z$ and we have two cases to consider:

Case 1. d: $b \to b$. Then $d^2 \in \langle z, b \rangle$. So by P2, $d^2 = z$. Now by Lemma 2.3, $\mathbb{Q}\{d, T, M\}$ is of exponent $\leqslant 2$ and index 8, a contradiction.

Case 2. d: $a \to a^{-1}$, $b \to bz$ (if d: $a \to a^{-1}z$, then replace a by ab). Replace b by $a^{2^{\beta-2}}b$ to get d: $b \to b$ and $b^2 = z$. So $d^2 \in \langle b \rangle$. In $A = \mathbb{Q}\{d, T, M\}$, $a(1+\zeta^{-1})$ and $\langle d, b \rangle$ commute ($\zeta = a^2$ is a 2^α root of 1). So the exponent of A is $\leqslant 2$, a contradiction.

This shows that $\beta = \alpha$. Now we prove $|S/T| = 2$. This is the case if $\alpha = 2$. So suppose $\alpha \geqslant 3$. If $d \in S$ has order 2 mod T and d: $b \to b$, $c \to c^{-1}z$ or cz, then we can make $d^2 \in \langle b \rangle$, where $\langle d, b \rangle$ gives a contradiction to P2. Now if $g \in S$ has order 4 mod T, then g^2: $b \to b$, $c \to cz$, a contradiction as above. Next if $S/T \cong \mathscr{C}_2 \times \mathscr{C}_2$, then we can choose g, $h \in S$ such that

$$g\colon c \to c^{-1},\ b \to b;\ g^2 = z$$

(if $g^2 = 1$, then $\langle g, b \rangle$ contradicts P2)

$$h\colon c \to cz,\ b \to bz;\ ghg^{-1} = xh,\ x \in C.$$

This is because of the above, P1, and that S/T acts faithfully on C. If $h^2 \in C$ then we can make $h^2 = 1$, so $\mathbb{Q}\{S, M\}$ has exponent $\leqslant 2$, a contradiction. The other possibility, by a suitable choice of h, is $h^2 = cb$. Then $c^{-1}b = gh^2g^{-1} = x^h x h^2$. So $x \cdot {}^h x = c^{-2}$, $x = c^{-1 \pm 2^{\alpha-2}}$. We are going to rule out this group. We have

$$S = \langle g, h, c \rangle;\ g: c \to c^{-1},\ h: c \to cz;\ g^2 = z,\ h^4 = c^2$$
$$ghg^{-1} = xh;\ c^{2^\alpha} = 1,\ \alpha \geqslant 3.$$

In $A = \mathbb{Q}\{S, M\}$, g and $h' = (1+\zeta)h$ commute, where $\zeta = x$ is a primitive 2^αth root of 1. Put $E = \mathbb{Q}(\zeta_{2^\alpha m})$. We remind the reader of the comment after Lemma 2.6. By that lemma, A is a crossed product of E with S. Let the fixed fields of g, h', and S in E be F, F', and K. We have

$$A = \langle F'/K,\ g,\ -1 \rangle \otimes_K \langle F/K,\ h',\ \gamma \rangle,$$

where $\gamma = h'^4 = (1-\zeta^2)^2 h^4 = -(\zeta - \zeta^{-1})^2$. We show that $\gamma^2 \in \mathcal{N}_{F/K}$. This makes the exponent of A at most 2, giving a contradiction as the index of A is 8. By Hasse's norm theorem, we have to prove that locally. At any (possible) real prime divisor of K, γ^2 is positive and there is nothing to show. Let p be a rational prime and $\mathfrak{P} \mid p$ be a prime divisor of E. Denote the corresponding primes of F, K, $\mathbb{Q}(\zeta)$ by $\wp'$, $\wp$, $\mathfrak{P}'$. Let m' be the p' part of m. First, assume that p is odd. The inertia subgroup of p in E denoted by $I_p(E/\mathbb{Q})$ consists of automorphisms of $E/\mathbb{Q}$ which fix $\zeta_{m'}$. So $I_p(E/K) = I_p(E/\mathbb{Q}) \cap \langle g, h' \rangle \leqslant \langle h'^2 \rangle$ and $I_p(F/K) = I_p(E/K) \bmod \langle g \rangle \leqslant \langle h' |_F^2 \rangle$. Let Z be the maximal unramified subfield of $F_{\wp'}/K_\wp$, where $K_\wp$, etc., denotes the completion of K at $\wp$, etc. The inertia subgroup of $F_{\wp'}/K_\wp$, that is, $\mathrm{Gal}(F_{\wp'}/Z)$, is canonically isomorphic to $I_p(F/K)$ (by the restriction map). So $|F_{\wp'} : Z| = 1$ or 2. Thus by the local class field theory $K_\wp^\times / \mathcal{N}_{F_{\wp'}/K_\wp}$ is cyclic with the subgroup $\mathcal{N}_{Z/K_\wp}/\mathcal{N}_{F_{\wp'}/K_\wp}$ of size $\leqslant 2$. Since $N_{\mathbb{Q}(\zeta)/\mathbb{Q}}(\gamma) = 2^4$, γ is a unit of $K_\wp$. So $\gamma \in \mathcal{N}_{Z/K_\wp}$ and $\gamma^2 \in \mathcal{N}_{F_{\wp'}/K_\wp}$.

Now we consider $p = 2$. $I_2(E/K) = I_2(E/\mathbb{Q}) \cap \langle g, h' \rangle \leqslant \langle g \rangle$ since h' acts on $\zeta_{m'}$ with order 4. Hence $F_{\wp'}/K_\wp$ is unramified. Let $v_\mathfrak{P}$, $v_\wp$, etc., be the normalised additive valuations of $E_\mathfrak{P}$, $K_\wp$, etc. Normalised means that their value group is $\mathbb{Z}$. By the above, we need to show that $4 \mid v_\wp(\gamma^2)$. Now $E_\mathfrak{P}$ is unramified over $\mathbb{Q}(\zeta)_{\mathfrak{P}'}$. Hence

$$v_\mathfrak{P}(\gamma) = v_{\mathfrak{P}'}(\gamma) = v_{\mathfrak{P}'}[-\zeta^{-2}(1-\zeta)^2(1+\zeta)^2] = 4$$

and $v_\wp(\gamma) = v_{\wp'}(\gamma) = v_\mathfrak{P}(\gamma)$ or $\frac{1}{2} v_\mathfrak{P}(\gamma)$ according as $E_\mathfrak{P}/F_{\wp'}$ is unramified or not. This concludes the $p = 2$ case and the impossibility of the embedding of the group in question.

We have shown $|S/T| = 2$. If $d \in S \setminus T$, d: $b \to b$, then as we saw, we must have d: $c \to c^{-1}$ ($\alpha \geqslant 2$) giving the group (g). The remaining possibility d: $b \to bz$ gives rise to the following two cases:

(1) d: $c \to c^{-1}$ or $c^{-1}z$ and $\alpha \geqslant 3$. Replace b by $c^{2^{\alpha-2}}b$ to get d: $b \to b$ and $b^2 = z$. We must have $d^2 \in \langle b \rangle$ so that either $d^2 = 1$ or z giving (i) (note $\mathscr{D}_{2^{\alpha+1}} \Upsilon \mathscr{C}_4 \cong \mathscr{D}_{2^{\alpha+1}} \Upsilon \mathscr{C}_4$) or $d^2 = b$. In that case, $d^4 = z$, d: $c \to c^{-1}$ or $c^{-1}z$. We show that this is not possible. Let $g \in M$ be of prime order p such that d operates with order 4 on $\langle g \rangle$ (so $p \equiv 1 \bmod 4$). Let $E = \mathbb{Q}\{c, g\} \cong \mathbb{Q}(\zeta_{2^\alpha p})$ and K be the fixed field of d in E. We claim that $A = \mathbb{Q}\{S, g\} = \langle E/K, d, -1 \rangle \cong M_4(K)$. We must show $-1 \in \mathscr{N}_{E/K}$ and it is enough to do that locally. Since all our fields are cyclotomic and only relative dimension of their completions concerns us, it is enough to specify rational primes only. This remark applies to all later such calculations. Now K is complex because d^2 is not the complex conjugation of E. At a prime $q \neq 2$ or p, E_q/K_q is unramified so -1 is automatically a norm. Now consider 2. Put $f = \gamma(2, p) =$ order of 2 mod p, $\beta(2, f) =$ maximum power of 2 dividing f, and $n = \min(2, \beta(2, f))$. Recall that $D_2(E/\mathbb{Q})$, the decomposition group of 2 in $E/\mathbb{Q}$, consists of automorphisms of E which on ζ_p are of the form $\zeta_p \to \zeta_p^{2^*}$. The Galois group of E_2/K_2 is canonically isomorphic to $D_2(E/K) = D_2(E/\mathbb{Q}) \cap \langle d \rangle$, which can easily be seen to be of order 2^n. Hence $|K_2 : \mathbb{Q}_2| = 2^{\alpha-1}f/2^n$ is even, so that by the properties of the norm residue symbol $(-1, E_2/K_2) = ((-1)^{|K_2:\mathbb{Q}_2|}, E_2/\mathbb{Q}_2) = 1$ and $-1 \in \mathscr{N}_{E_2/K_2}$. Finally, consider p. We have $D_p(E/K) = D_p(E/\mathbb{Q}) \cap \langle d \rangle = \langle d^2 \rangle$ for -1 or $-1 + 2^{\alpha-1}$ when $\alpha \geqslant 3$ is not congruent to a power of p mod 2^α as $p \equiv 1(4)$. Putting $f = \gamma(p, 2^\alpha)$, we have $(-1, E_p/K_p) = ((-1)^{(p-1)f/2}, E_p/\mathbb{Q}_p) = 1$. Therefore $-1 \in \mathscr{N}_{E_p/K_p}$ and our claim is proved.

2. d: $c \to cz$, $b \to bz$. If $d^2 \notin C$ then $d^2 = c^k b$ for some odd number k, so $d^{2^{\alpha+1}} = 1$, $b^2 = 1$, ${}^b d = dz$, and $C = \langle d^2 b \rangle$. We get the group (c). If $d^2 \in C$, then make $d^2 = 1$. Replace b by ab to get $b^2 = a^2$, d: $b \to b$. We get the group (j).

(D) We want to show $S = T$, getting the group (e). So let $d \in S \setminus T$ to be of order 2 mod T, d: $a \to ax$, $x \in C$, $r = \beta - \alpha \geqslant 1$, $c = a^{2^r}$. We can take d: $b \to b$ for if d: $b \to bz$, then replace d by ad. We consider the three possible actions of d on C separately:

1. d: $c \to c^{-1}$. Then $x^{2^r} = c^{-2}$, $r = 1$, $x = c^{-1}$ or $c^{-1}z$. So d: $a \to a^{-1}$ or $a^{-1}z$, $b \to b$. Here d^2 centralises T, so $d^2 \in \langle z \rangle$. By Lemma 2.3, $\mathbb{Q}\{d, T, M\}$ has exponent $\leqslant 2$, a contradiction. For the remaining two cases we can assume $\alpha \geqslant 3$:

2. d: $c \to c^{-1}z$. So $x^{2^r} = c^{-2}z$, $r = 1$, $x = c^{-1}z'$, where $z' \in C$, $z'^2 = z$. Now d: $a \to a^{-1}z'$, $b \to b$ so d^2: $a \to az$, $b \to b$. Therefore $d^2 = b$ or zb. In either case $\langle d \rangle \cap C = 1$ contradicts P2.

3. d: $c \to cz$. Then $x^{2^r} = z$. Also d^2: $a \to ax \cdot {}^d x$. So $x \cdot {}^d x = 1$ or z, $x \in \langle c^2 \rangle$, $x^2 = 1$ or z. Therefore $r = 1$, $x^2 = z$, d^2: $a \to az$, $b \to b$. Hence $d^2 = yb$ for some $y \in \langle c^2 \rangle$. Replace d by $y'd$, where $y' \in C$, $y'^2 = y^{-1}$, to get $d^2 = b$ or zb. But now $\langle d \rangle$ gives a contradiction to P2.

(E) Again we show $S = T$ to get the group (f). Let $T = \langle a, b \rangle \curlyvee \langle c \rangle$; $a^4 = 1$, ${}^b a = a^{-1}$, $b^2 = 1$. Suppose $d \in S$ and d: $a \to ax$, $b \to bx'$: x, $x' \in C$. Now $x'^2 = 1$, ${}^{bx'}(ax) = a^{-1}x^{-1}$ so $x^2 = 1$. Therefore d is inner on $\mathscr{D}_8$ and $S = \langle a, b \rangle \curlyvee C_1$, where $C_1 = C_S(a, b)$. Let $d \in C_1$ be of order 2 mod C. Then $\mathbb{Q}\{d, T, M\}$ is of index 8 and exponent $\leqslant 2$ by Lemma 2.3, a contradiction. Therefore $C_1 = C$ and $S = T$.

This concludes the proof of the lemma. We remark that if $S = \mathscr{D}_8 \curlyvee \mathscr{C}_{2^\beta}$, $\beta \geqslant 2$, is of type (j), then one shows easily that $\mathbb{Q}\{S, M\}$ has exponent $\leqslant 2$. So its index 2^β must be $\leqslant 4$. Hence $\beta = 2$ and the group also occurs under (i).

3. Having determined the structure of a Sylow 2-subgroup of G, we obtain a complete group theoretic description of G in Subsection 8. It will be seen that G is 2-nilpotent and all its odd Sylow subgroups are cyclic. Although it is this presentation of G as a split extension of a metacyclic group by a 2-group which is most suitable for the number theoretic investigations in Section 6, here we give generators and relations for G in a way which show the dependence of G on a minimal number of integer parameters. The necessary group theoretic conditions on these parameters will be given as well. See the theorem below. We trust that the reader is able to go freely from one presentation to the other. A glance at the theorem shows that the division of the Sylow 2-subgroup into four classes is intimately reflected in G.

We require Lemma 5 below. We only need this lemma in its simplest form when all the Sylow subgroups of R are cyclic. Nevertheless we present the general form as it was its discovery in that generality which gave hope of a complete classification. In the proof of Lemma 5, we use Lemma 4, which is supplied with a proof for the reader's convenience.

4. LEMMA. *Let R be a finite group, $M \trianglelefteq R$ with R/M nilpotent. Then there is a nilpotent subgroup H of R such that $R = HM$.*

Proof. We use induction on $|M|$. If, for some prime p, $P \in \mathrm{Syl}_p M$ is not normal in R, then, putting $N = N_R(P)$, we have $M \cap N < M$, $R = MN$, $N/M \cap N \cong R/M$. So by the induction hypothesis applied to $M \cap N \trianglelefteq N$, $N = HM$ for some nilpotent subgroup H of N. Hence $R = HM$. We can therefore assume that M is nilpotent. Let $p \mid |M|$, $O_{p'}(M) \neq 1$. Then applying induction to $R/O_{p'}(M)$, we have $R = H_1 M$, where $H_1/O_{p'}(M)$ is nilpotent to which we apply induction again: $H_1 = HO_{p'}(M)$ for some

nilpotent H. Then $R = HM$. So we are left with the case that M is a p-group. Let T/M be the Sylow p-subgroup of R/M. The group R/T is a p'-group. So by the Schur–Zassenhaus theorem there exists a subgroup L of R such that $R = LT$, $L \cap T = 1$. Now L centralises T/M. By a result on p'-automorphisms of p-groups [10, Chap. 5, Theorem 3.5], $T = C_T(L)[L, T]$ and $[L, T] \leqslant M$. Thus $H = L \times C_T(L)$ is the required subgroup.

5. LEMMA. *Let R be a finite soluble group with abelian Sylow subgroups such that $F(R)$ is cyclic. Then $F(R) = Z(R) \times \mathscr{D}R$ ($\mathscr{D}R = [R, R]$), $|\mathscr{D}R|$ is odd, there is an abelian complement H to $\mathscr{D}R$, $Z(R) \leqslant H$, $N_R(H) = H$, and H is uniquely determined up to conjugacy in R.*

Proof. By transfer into Sylow subgroups one gets $Z(R) \cap \mathscr{D}R = 1$. By Lemma 4, there is a nilpotent subgroup H such that $R = H\mathscr{D}R$. So H is abelian, $\mathscr{D}R \leqslant F(R)$ is cyclic, and $H \cap \mathscr{D}R \leqslant Z(R) \cap \mathscr{D}R = 1$. $C_R(H) = H(C_R(H) \cap \mathscr{D}R) = H$ so $Z(R) \leqslant H$. Since $R/[H, \mathscr{D}R]$ is abelian, $[H, \mathscr{D}R] = \mathscr{D}R$. Hence $\mathscr{D}R$ has odd order. $F(R) = (H \cap F(R)) \times \mathscr{D}R$ and $H \cap F(R) = Z(R)$ so $F(R) = Z(R) \times \mathscr{D}R$. $[H, N_R(H)] \leqslant H \cap \mathscr{D}R = 1$ so $N_R(H) = H$. We prove the statement on the conjugacy of the complements by induction on $|H|$. Let H, H' be two completements to $\mathscr{D}R$. Let p be the smallest prime divisor of $|H|$ and let $H = L \times M$, $H' = L' \times M'$ be the decomposition into p, p' parts. $p \nmid |\mathscr{D}R|$ otherwise $|H|$ will have a prime dividing $p - 1$. So L, $L' \in \mathrm{Syl}_p R$. By conjugating, we can assume $L = L'$. Let $R_1 = C_R(L)$, $C = C_{\mathscr{D}R}(L)$ then $\mathscr{D}R = C \times [L, \mathscr{D}R]$ so $[M, C] = [M', C] = C$ and $R_1 = L \times (MC) = L \times (M'C)$. Since $|L|$ and $|MC|$ are coprime, $MC = M'C = R_2$ to which induction can be applied, since $C = \mathscr{D}R_2$ and M, M' are complements for C. So $M' = M^x$ for some $x \in R_2$ and $H' = H^x$.

6. LEMMA. *Let $R \leqslant M_2(D)$ be a soluble group with abelian Sylow subgroups such that $F(R)$ is cyclic. Suppose that $\mathbb{Q}\{F(R)\}$ is a field. Let H be as in Lemma* 5.

(a) *For an odd prime p, if $p \mid |H|$ then $p \mid |Z(R)|$.*

(b) *Sylow p-subgroups of R are cyclic for odd p.*

(c) *A sylow 2-subgroup of R is cyclic or $\mathscr{C} \times \mathscr{C}_2$.*

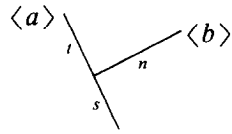
(d) $(|H|, |\mathscr{D}R|) = 1$.

Proof. If (a) or (b) were not true, then there would exist $g \in H \setminus Z(R)$ of order p so $\langle g \rangle \cap F(R) = 1$ and $\mathbb{Q}\{g, F(R)\} \cong M_p(*)$, a contradiction. If (c) were false, then there would exist a subgroup $L \cong \mathscr{C}_4$ or $\mathscr{C}_2 \times \mathscr{C}_2$ of H such that $L \cap F(R) = 1$. Then $\mathbb{Q}\{L, F(R)\} = M_4(*)$, a contradiction. Part (d) follows from (a) and the fact that $|\mathscr{D}R|$ is odd and $(|Z(R)|, |\mathscr{D}R|) = 1$.

7. *Remark.* In the context of Lemma 6, suppose that R has odd order. So all the Sylow subgroups of R and H are cyclic. $\mathbb{Q}\{R\}$ is a central simple algebra of index $|R/F(R)|$ by Lemma 2.6. Hence $\mathbb{Q}\{R\}$ is a division algebra and R is classified as a $G_{m,r}$ group in [1]. We have $R = L \rtimes H$, where $L = \mathscr{D}R$ as before. We observed in 1.5(b) that to any decomposition $L = L_1 \times L_2$, we have one for $H = H_1 \times H_2$ such that $R = (L_1 \rtimes H_1) \times (L_2 \rtimes H_2)$. These two factors are of coprime order. Presently, we will make use of this fact.

8. THEOREM. *Suppose that G is a primitive, finite soluble subgroup of $M_2(D)$ spanning it over $\mathbb{Q}$. Let $O_2(G)$ belong to* 2.12(1). *Let S be a Sylow 2-subgroup of G. G is classified into four classes each consisting of several types as follows*:

Class 1: *G is metacyclic depending on the parameters m, r. $G = \langle a, b \rangle$; $a^m = 1$, $b^n = a^t$, $bab^{-1} = a^r$; $(r, m) = 1$, $n = \gamma(r, m)$, $st = m$, (n, t) and (s, t) are powers of 2.*



(a) $S \cong \mathscr{C}$; $s = (r-1, m)$, *t odd.*

(b_1) $S \cong \mathscr{Q}_{2^{\alpha+1}}$, $\alpha \geqslant 2$;
$2^{\alpha-1} \| t$, $2 \| s$, $2 \| n$, $r \equiv -1(2^\alpha)$, $s = (r-1, m)$.

(b_2) $S \cong \mathscr{D}_{2^{\alpha+1}}$, $\alpha \geqslant 2$;
$2^\alpha \| t$, *s odd*, $2 \| n$, $r \equiv -1(2^\alpha)$, $2s = (r-1, m)$.

(b_3) $S \cong \mathscr{S}_{2^{\alpha+1}}$, $\alpha \geqslant 3$;
$2^\alpha \| t$, *s odd*, $2 \| n$, $r \equiv -1 + 2^{\alpha-1}(2^\alpha)$, $2s = (r-1, m)$.

(c) $S \cong \mathscr{E}$; $2 \| t$, $2^{\alpha-1} \| s$, $2 | n$, $r \equiv 1 + 2^{\alpha-1}(2^\alpha)$, $\alpha \geqslant 2$, $s = (r-1, m)$.

Class 2: *G has a metacyclic subgroup G_1 of index 2 and depends on the three parameters m, r, r':*

$$G_1 = \langle a, b \rangle,\ G = \langle a, b, d \rangle;$$

$$a^m = 1,\ b^n = a^t,\ bab^{-1} = a^r,\ dad^{-1} = a^{r'},\ dbd^{-1} = b^\beta;$$

$$(r, m) = (r', m) = 1,\ n = \gamma(r, m),\ r'^2 \equiv 1(m),\ st = m,\ t \text{ odd.}$$

In $d_1 - d_3$; $2^\alpha \| s$, $2 \| n$, $s/2^{\alpha-1} = (r-1,\ r'-1,\ m)$, $r \equiv 1(s)$, $r' \equiv -1(2^\alpha)$, $\beta \equiv 1(ns/2^{\alpha+1})$. In d_1, d_2; if $\alpha = 1$, then r and r' are independent mod m.

(d_1) $S \cong \mathscr{D}_{2^{\alpha+2}}$, $\alpha \geqslant 1$; $d^2 = 1$, $\beta \equiv -1(2^{\alpha+1})$.

(d_2) $S \cong \mathscr{Q}_{2^{\alpha+2}}$, $\alpha \geqslant 1$; $d^2 = a^{m/2}$, $\beta \equiv -1(2^{\alpha+1})$.

(d_3) $S \cong \mathscr{S}_{2^{\alpha+2}}$, $\alpha \geqslant 2$; $d^2 = 1$, $\beta \equiv -1 + 2^{\alpha}(2^{\alpha+1})$.

(e) $S \cong \mathscr{E}$; $2^{\alpha} \| s$, $\alpha \geqslant 2$, $2 | n$, $\beta = 1 + ns/2$, $d^2 = 1$, $s = (r-1, r'-1, m)$, r and r' are independent mod m.

Class 3: *G is the direct or central product of a pair of groups G_1, G_2 of class* 1, *except for* (f), *where G_1 belongs to class* 2. *In the central product case, the* 2*-part of $Z(G_1)$ is identified with an isomorphic subgroup of $Z(G_2)$. We denote a Sylow* 2*-subgroup of G_i and $O_2(G_i)$ by S_i and C_i. ($|G_1|, |G_2|$) is a power of* 2.

(f) $G \cong G_1 \curlyvee \mathscr{C}$, $S_1 \cong \mathscr{Q}_8$ (or $\mathscr{D}_8$), $|C_1| = 2$; $|G_2| \geqslant 4$.

(g_1) $G \cong \mathscr{Q}_{2^{\alpha+1}m_1} \times \mathscr{D}_{2m_2}$; $\alpha \geqslant 2$, m_1 *and* m_2 *odd*, $m_1 \geqslant 1$, $m_2 > 1$.

(g_2) $G \cong \mathscr{Q}_8 \times G_2$; $S_2 \cong \mathscr{C}_2$, $C_2 = 1$.

(h_1) $G \cong G_1 \times G_2$; $S_1 \cong \mathscr{C}$; $S_2 \cong \mathscr{C}_2$, $C_2 = 1$.

(h_2) $G \cong G_1 \curlyvee G_2$; S_1, $S_2 \cong \mathscr{C}$, $C_1 = C_2$, $|S_2 : C_2| = 2$.

(i) $G = G_1 \curlyvee G_2$; $S_1 \cong \mathscr{D}$, $\mathscr{Q}$, $\mathscr{S}$ *of order* $2^{\alpha+1}$, $\alpha \geqslant 3$; $S_2 \cong \mathscr{C}_4$, $|C_2| = 2$; *either* $|C_1| = 2^{\alpha}$ *or* $G_1 = S_1$.

(j) $G \cong G_1 \curlyvee G_2$; $S_1 \cong \mathscr{E}_{2^{\alpha+1}}$ *or* $\mathscr{Q}_8$, $\alpha \geqslant 2$; $S_2 = \mathscr{C}$, $|C_2| = 2^{\alpha-1}$; *either* $|C_1| = 2^{\alpha}$ *or* $G_1 = S_1 \cong \mathscr{Q}_8$.

(k) $G \cong G_1 \curlyvee \mathscr{C}$; $S_1 \cong \mathscr{C}$; $|G_2 : C_1| = 2$.

Class 4: $G = \langle a, b, c, d \rangle$.

$c^{2^{\alpha}} = 1$, $\alpha \geqslant 3$; $aca^{-1} = c^{-1}$, $bcb^{-1} = cz$, *where* $z = c^{2^{\alpha-1}}$, $a^2 = z$, $b^2 = 1$ *or* z, $ab = ba$, $d^m = 1$ m *odd* > 1, $ada^{-1} = d^{-1}$, $bdb^{-1} = d^r$, $r^2 \equiv 1(m)$, $r \not\equiv 1(m)$. *If* $r \not\equiv -1(m)$ *then* $O_2(G) = \langle c \rangle$, *if* $r \equiv -1(m)$ *then* $O_2(G) = \langle ab, c \rangle \cong \mathscr{S}$. $cd = dc$.

Proof. We have determined the structure of a Sylow 2-subgroup of G in Lemma 2. With our assumption on G when $O_2(G) \cong \mathscr{Q}_8$, the automorphisms induced by G on $O_2(G)$ are of 2-power order. Put $R_1/F(G) = O_{2'}(G/F(G))$. Thus $R_1 = O_2(G) \times R$, where $R = O_{2'}(R_1)$. It is clear that $R \lhd G$ and R is the Hall $2'$-subgroup of G. So G is 2-nilpotent. Now $F(R) = O_{2'}(F(G))$ is cyclic. So by Lemma 6 and the succeeding remark, $R = H_1 \curlywedge \mathscr{D}R$ for some cyclic subgroup H_1 of R and ($|H_1|$, $|\mathscr{D}R|$) $= 1$. By a Frattini argument $G = N_G(H_1)R$. Let $S \in \mathrm{Syl}_2 N_G(H_1)$. Then S is a Sylow 2-subgroup of G and $G = SR = SH_1 \mathscr{D}R$, where S normalises H_1 and $\mathscr{D}R$. We have $H_1 = H \times [S, H_1]$, where $H = C_{H_1}(S)$. Since $\mathrm{Aut}(\mathscr{D}R)$ is abelian, $[S, H_1]$ centralises $\mathscr{D}R$. So finally we get

$G = L \rtimes (H \times S)$, where $L = [S, H_1] \times \mathscr{D} R$ and $[L, H \times S] = L$. Here $(|H|, |L|) = 1$, $|L|$ is odd, and the primes dividing $|H|$ divide $|C_H(L)|$, by Lemma 6(a). Also $O_2(G) = C_S(L)$, $Z(G) = C_H(L) \times (O_2(G) \cap Z(S))$, and $O_{2'}(F(G)) = L \times C_H(L)$.

We proceed from the classification of S given in Lemma 2:

Class 1 *and* 2: Here one can pass from $G = L \rtimes (H \times S)$ to the required presentation. We illustrate the method for one group in each class. First consider the group 2(c):

$$S = \langle g, h \rangle \cong \mathscr{E}_{2^{\beta+1}}, \qquad g^{2^\beta} = 1, {}^h g = g^{1+2^{\beta-1}}, h^2 = 1;$$
$$C = \langle g^{2^{\beta-\alpha}} h \rangle, \alpha \geqslant 2, \beta \geqslant \alpha.$$

Clearly we can assume $\beta \geqslant 3$ for $\beta = 2$ is covered in 2(a). Recalling how C was defined in Section 3.1, it is easy to convince oneself that $O_2(G) = C$. Now, let $\langle a \rangle = \langle L, C_H(L), C \rangle$, $\langle b \rangle = \langle H, g \rangle$. We have $G = \langle a, b \rangle$, $\langle a \rangle \cap \langle b \rangle = Z(G)$. Put $|\langle a \rangle| = m$, $|\langle a \rangle : Z(G)| = t$, $|Z(G)| = s$, and $|\langle b \rangle : Z(G)| = n$. By a suitable choice of a, we have

$$a^m = 1, \; b^n = a^t, \; bab^{-1} = a^r, \; \textit{where} \; (r, m) = 1; \; st = m, \; 2^{\alpha-1} \| s,$$
$$2 \| t, \; 2 | n, \; \textit{and} \; r \equiv 1 + 2^{\alpha-1} (2^\alpha).$$

Now $m | t(r-1)$, for a^t is centralised by b. Hence $s | s'$, where $s' = (r-1, m)$. Conversely $a^{m/s'} \in Z(G)$, therefore $s' | s$. This shows $s = (r-1, m)$. Finally, since $Z(G) = \langle b^n \rangle$, $\langle b \rangle \bmod \langle b^n \rangle$ acts faithfully on $\langle a \rangle$. Therefore $n = \gamma(r, m) =$ order of $r \bmod m$.

Now consider the group 2(e):

$$S = \langle g, d \rangle \cong \mathscr{E}_{2^{\beta+1}}, \qquad g^{2^\beta} = 1, d^2 = 1, {}^d g = gz, \text{ where}$$
$$z = g^{2^{\beta-1}}; \; C = \langle g^{2^{\beta-\alpha}} \rangle, \beta > \alpha.$$

Here $C \leqslant Z(S)$, so by the definition of C, $O_2(G) = C$. Let $\langle a \rangle = \langle L, C_H(L), C \rangle$, $\langle b \rangle = \langle H, g \rangle$, $G_1 = \langle a, b \rangle$. Then $G = \langle a, b, d \rangle$, $|G : G_1| = 2$, and $\langle a \rangle \cap \langle b \rangle = C_H(L) \times C = Z(G)$. Let m, n, r, s, t be defined exactly as above. Note that in general $Z(G_1) > Z(G)$. Let $dad^{-1} = a^{r'}$. Clearly $dbd^{-1} = bz = b^{1+ns/2}$, $r'^2 \equiv 1 (m)$. Since $a^t \in Z(G)$, m divides $t(r-1)$ and $t(r'-1)$. So $s | s'$, where $s' = (r-1, r'-1, m)$. Conversely $a^{m/s'} \in Z(G) = \langle a^t \rangle$, so $s' | s$. Hence $s = (r-1, r'-1, m)$. If $\alpha = 1$, then by the proof of Lemma 3.2, $S \cong \mathscr{D}_8$, which is covered under (d_1). So $\alpha \geqslant 2$. This completes the calculations for the two examples.

Class 3: Here we want to show that G factorises as S does. One essential reason for this phenomenon is the observation in Remark 7. In fact all that is actually required is to prove that the two factors of S, after a rearrangement if needed, act on different Sylow p-subgroups of L. For suppose that for a decomposition $S = S_1 \mathbin{Y} S_2$ of S, we can write $L = L_1 \times L_2$

such that $[L_1, S_2] = [L_2, S_1] = 1$. Then applying Remark 7 to this factorisation of L, we have $H = H_1 \times H_2$ such that $[L_1, H_2] = [L_2, H_1] = 1$. Thus $G = G_1 \curlyvee G_2$, $G_i = L_i \leftthreetimes (H_i \times S_i)$, is the required decomposition. Clearly $l = |L| > 1$, otherwise $O_2(G) = S$ contrary to assumption 2.12(1). Now going through the types in class 3, we establish the above requirement:

(f), (k). Here $C = O_2(G)$ centralises L so there is nothing to show (clearly we can take $L_2 = H_2 = 1$, $G_2 = C$).

(g) $S = \langle b, c \rangle \times \langle a \rangle \cong \mathscr{D}_{2^{\alpha+1}} \times \mathscr{C}_2$, $C = \langle c \rangle$, $\alpha \geqslant 2$.

If $O_2(G) = \langle b, c \rangle$ then $G = \mathscr{D}_{2^{\alpha+1}} \times G_2$, where $G_2 = L \leftthreetimes (H \times \langle a \rangle)$. For $\alpha = 2$ we cannot say any more, so we get (g_2). However, if $\alpha \geqslant 3$, then $\mathbb{Q}\{O_2(G)\} \cong \mathscr{A}_K$, $K = \mathbb{Q}(\zeta_{2^\alpha} + \zeta_{2^\alpha}^{-1})$, has nonzero invariants at the real places of K only. Since the prime divisors of $|H|$ divide $|C_H(L)|$, if $H \neq 1$, then $C_H(L) \neq 1$. Thus $\mathbb{Q}\{L, C_H(L), a\} \cong M_2(E)$, where E is a complex field. Hence EK splits $\mathscr{A}_K$, a contradiction. Thus $H = 1$ and by a similar argument a inverts L. We get $G \cong \mathscr{D}_{2^{\alpha+1}} \times \mathscr{D}_{2l}$, $l > 1$ odd. Next, suppose that $O_2(G) = C$. Thus $\langle b, a \rangle$ mod $\langle z \rangle$ acts faithfully on L $(z = c^{2^{\alpha-1}})$. In $E = \mathbb{Q}(\zeta_{2^s m})$, $m = |L \times C_H(L)|$, let F, F', K be the fixed fields of a, b, $\langle a, b \rangle$. By Lemma 2.3,

$$\mathbb{Q}\{a, b, c, L, C_H(L)\} \cong \langle F'/K, a, 1 \rangle \otimes_K \langle F/K, b, -1 \rangle.$$

The first algebra is isomorphic to $M_2(K)$. The second one is isomorphic to $\mathscr{A}_K$, for $F = K(i)$ and b: $i \to -i$. Now $K_2/\mathbb{Q}_2$ is ramified. For $\langle a, b \rangle \cap I_2(E/\mathbb{Q}) = 1$, so E_2/K_2 is unramified and $e(K_2/\mathbb{Q}_2) = e(E_2/\mathbb{Q}_2) = 2^{\alpha-1}$. Hence in order that $\mathscr{A}_K$ not be split, we want K to be a real field. Thus $C_H(L) = 1$ implying $H = 1$ and $\langle a, b \rangle$ includes complex conjugation of E. So either b inverts L and a inverts part of L or b and a invert complementary parts of L. If the first possibility were true, then replace b by ab to get the second one. Writing $L = \langle g_1 \rangle \times \langle g_2 \rangle$, where $g_1^{m_1} = 1$, $g_2^{m_2} = 1$, $g_1^b = g_1^{-1}$, $g_2^a = g_2^{-1}$, we get $G = \mathscr{D}_{2^{\alpha+1} m_1} \times \mathscr{D}_{2m_2}$, m_1 and $m_2 > 1$ odd.

(h) $S = \langle a \rangle \times \langle b \rangle$, $a^{2^\beta} = 1$, $b^2 = 1$; $C = \langle a^{\beta-\alpha} \rangle$, $\beta \geqslant \alpha \geqslant 1$.

When $\beta = \alpha$, $C = \langle a \rangle$ centralises L, and there is nothing to show. Hence assume that $\beta \geqslant \alpha + 1$. Clearly $O_2(G) = C$. In the present case, we will show that a or ab and b or $ba^{2^{\beta-\alpha-1}}$ act on different parts of L. By our earlier remarks, this leads to the factorisation of G given in (h_1) and (h_2). We consider $\mathbb{Q}\{L, S\}$. Applying Lemmas 2.3 and 2.6, let the fixed fields of $\langle a \rangle$, $\langle b \rangle$, S in $E = \mathbb{Q}\{L, C\} \cong \mathbb{Q}(\zeta_{2^s l})$ be F', F, K. We have $\mathbb{Q}\{L, S\} = \langle F'/K, b, 1 \rangle \otimes_K A$, where $A = \langle F/K, a, \zeta \rangle$, $\zeta = \zeta_{2^\alpha}$. Thus we require A to be a division algebra. As in [1, p. 368], a necessary and sufficient condition for that is that $\zeta^{2^{\beta-\alpha-1}} \notin \mathscr{N}_{F/K}$ (note that the index of A is $2^{\beta-\alpha}$).

Equivalently, $\zeta \notin \mathcal{N}_{Z/K}$, where Z/K is the quadratic subextension of F/K. By Hasse's norm theorem we require $\zeta \notin \mathcal{N}_{Z_p/K_p}$ for some prime p. So suppose that this holds. We remind the reader that in the calculation to follow, it is immaterial which prime divisor of p is to be taken in Z/K. So we only specify the rational prime p in the completions (cf. 1.1). First, suppose that p is the real infinite prime and K and Z are real and complex fields, respectively. Then $\alpha = 1$, $\beta = 2$ for $\zeta \in K$ and a induces the complex conjugation on F. Since K is real, a or ab must induce complex conjugation on E. In other words, one of them must invert L. Then clearly ab or a and b invert complementary parts of L as required.

Now assume that p is a finite prime. Z_p/K_p is ramified of degree 2, for ζ is a unit of K_p. So $p \mid 2^\alpha l$ and we want $I_p(Z/K) = I_p(E/\mathbb{Q}) \cap \langle a, b\rangle \bmod \langle a^2, b\rangle \neq 1$. Thus, putting $I_p = I_p(E/\mathbb{Q})$, $I_p \cap \langle a, b\rangle \not\leq \langle a^2, b\rangle$, i.e., a or ab belongs to I_p. Since $\langle a, b\rangle \bmod C$ acts faithfully on L, $p = 2$ is ruled out. Thus $p \mid l$ and a or ab centralise $O_{p'}(L)$. Clearly then either b or $ba^{2^{\beta-\alpha-1}}$ centralises $O_p(L)$. This concludes the proof of the claim above and the case (h).

(i) $S = \langle b, c\rangle \,Y\, \langle a\rangle \cong \mathcal{D}$, $\mathcal{Q}$, $\mathcal{S} \,Y\, \mathcal{C}_4$, $c^{2^\alpha} = 1$, $b^2 = 1$ or z, where $z = c^{2^{\alpha-1}}$; $a^2 = z$, $C = \langle c\rangle$, $\alpha \geqslant 3$.

If $O_2(G) = \langle b, c\rangle$ then we just take $G_1 = O_2(G)$ and $G_2 = L \rtimes (H \times \langle a\rangle)$. So assume that $O_2(G) = C$. We need to show that b or ba and a act on different parts of L. It suffices to show that it is not possible to have $g, g' \in L$ of prime orders p, q $(p \neq q)$ such that b acts only on g while a inverts both g and g'. Suppose this is possible and let $i \in C$ be of order 4. In $E = \mathbb{Q}(\zeta_{4pq})$, let the fixed fields of a, b, $\langle a, b\rangle$ be F, F', K. We have

$$\mathbb{Q}\{g, g', i, a, b\} = \langle F/K, b, \pm 1\rangle \otimes_K \langle F'/K, a, -1\rangle.$$

The first algebra is split because it is isomorphic to $\mathcal{A}_K$ if $b^2 = -1$ and K is complex with $e(K_2/\mathbb{Q}_2) = 2$. This is proved in a way similar to that of the argument for (g) above. $\langle F'/K, a, -1\rangle = B \otimes_{K'} K$, where $K' = \mathbb{Q}(\zeta_q + \zeta_q^{-1})$ and $B = \langle \mathbb{Q}(\zeta_q)/K', a, -1\rangle$. The algebra B has nonzero invariants at the real places of K' and the divisors of q when $q \equiv 3(4)$. This is proved, for instance, in [24, Sect. 8, Proposition 1]. Let $I_q = I_q(E/\mathbb{Q})$. Clearly $I_q \cap \langle a, b\rangle = 1$ so $e(K_q/\mathbb{Q}_q) = e(E_q/\mathbb{Q}_q) = q - 1$, $e(K'_q/\mathbb{Q}_q) = (q-1)/2$. Thus $e(K_q/K'_q) = 2$. Also K is complex. Therefore $B \otimes_{K'} K$ is split, a contradiction.

(j) $S = \langle b, c\rangle \,Y\, \langle a\rangle$, $c^{2^\alpha} = 1$, $b^2 = 1$, ${}^b c = c^{1+2^{\alpha-1}}$, $\alpha \geqslant 2$; $a^{2^\beta} = c^2$, $\beta \geqslant 1$; $C = \langle c\rangle$.

First suppose that $O_2(G) > C$. Then $\alpha = 2$, $\beta = 1$ (see the final paragraph of part (E) of the proof of Lemma 2 above) and $O_2(G) = \langle b, c\rangle \cong \mathcal{D}_8$ or

$O_2(G) = \langle ba, c\rangle \cong \mathscr{Q}_8$. The first case gives an imprimitive group by Lemma 2.8. So we get $G = \mathscr{Q}_8 \,Y\, G_2$, where $G_2 = L \times (H \times \langle a\rangle)$. Now assume $O_2(G) = C$. The proof here is similar to that for (h). Thus we consider $\mathbb{Q}\{L, S\}$. In $E = \mathbb{Q}(\zeta_{2^{\alpha}l})$, let F, F', Z, and K denote the fixed fields of $\langle b\rangle$, $\langle a\rangle$, $\langle a^2, b\rangle$, and $\langle a, b\rangle$. By Lemma 2.3, $\mathbb{Q}\{L, S\} \cong M_2(K) \otimes_K B$, where $B = \langle F/K, a, \zeta\rangle$, $\zeta = \zeta_{2^{\alpha-1}}$. In order that B be a division algebra, it is necessary and sufficient that $\zeta \notin \mathscr{N}_{Z/K}$. So for a prime p, at least Z_p/K_p must be ramified. Assume first that p is real so that K is real and Z is complex. As $\zeta_{2^{\alpha-1}} \in K$, $\alpha = 2$. Also $\beta = 1$, otherwise K and Z will be both real or complex. Now $Z = F$ is complex iff b does not act on all of L and then K is real iff a and b act on complementary parts of L. Thus there is a factorisation of L corresponding to $S = \mathscr{D}_8 \,Y\, \mathscr{C}_4$. Now suppose that p is a finite prime. In order that Z_p/K_p be ramified, we want $I_p \cap \langle a, b\rangle \not\leqslant \langle a^2, b\rangle$, where $I_p = I_p(E/\mathbb{Q})$. Thus a or ab belongs to I_p. Since $\langle a, b\rangle \bmod C$ acts faithfully on L, $p \neq 2$. Hence $p \mid l$. But then $ab \notin I_p$. So $a \in I_p$, i.e., a centralises $O_{p'}(L)$ and acts with order 2^{β} on $O_p(L)$. Clearly either b or $b' = ba^{2^{\beta-1}} c^{-1+2^{\alpha-2}}$ centralises $O_p(L)$. So $L = O_p(L) \times O_{p'}(L)$ is the required factorisation of L. Note that when $\alpha \geqslant 3$, $\langle c, b'\rangle \cong \mathscr{E}_{2^{\alpha+1}}$ but $\langle c, b'\rangle \cong \mathscr{Q}_8$ if $\alpha = 2$. This concludes case (j).

Class 4: Let $S = \langle a, b, c\rangle$ and a, b, c satisfy the relations in Lemma 2. Put $m = |L \times C_H(L)|$. In $E = \mathbb{Q}(\zeta_{2^{\alpha}m})$, let F, F', and K be the fixed fields of b, a, and $S \pmod C$. We have $\mathbb{Q}\{L, C_H(L), S\} = A \otimes_K B$, where $A = \langle F/K, a, -1\rangle \cong \mathscr{A} \otimes_{\mathbb{Q}} K$ and $B = \langle F'/K, b, \pm 1\rangle \cong \langle \mathbb{Q}(\zeta + \zeta^{-1})/\mathbb{Q}(\zeta^2 + \zeta^{-2}), b, \pm 1\rangle \otimes_{\mathbb{Q}(\zeta^2+\zeta^{-2})} K$, where $\zeta = \zeta_{2^{\alpha}}$. The crossed product algebra on the right of the formula for B was shown to be split in part (A) of the proof of Lemma 2 above. As for A, $2 \mid e(K_2/\mathbb{Q}_2)$ since $S \bmod C \notin I_2(E/\mathbb{Q})$ so $e(E_2/K_2) \leqslant 2$. Therefore we require K to be real so as not to split $\mathscr{A}$. Hence $C_H(L) = 1$, $H = 1$, and a inverts L. Letting $L = \langle d\rangle$, we get

$$^a d = d^{-1},\ ^b d = d^r, \qquad \text{where } r^2 \equiv 1(m) \text{ and } r \not\equiv 1(m)$$

(otherwise $O_2(G) = \langle b, c\rangle \cong \mathscr{E}_{2^{\alpha+1}}$, a contradiction). **q.e.d.**

4. Soluble Groups II

1. In this section we complete the classification of the soluble group G by examining the remaining possibilities for $O_2(G)$ listed in 2.12(2). Recalling the calculation of Aut $O_2(G)$ in 2.13, we observe that except for the group $\mathscr{Q}_8 \,Y\, \mathscr{D}_8$, the $\mathscr{Q}_8$ factor of $O_2(G)$ is characteristic in $O_2(G)$. Denote this factor by $T = \langle i, j\rangle$, $i^4 = 1$, $j^2 = i^2$, $^j i = i^{-1}$. Thus by Lemmas 2.9 and 2.6, $\mathbb{Q}\{T\} = \langle \mathbb{Q}(i), j, -1\rangle = \mathscr{A}$. Incidentally this explains the notation for T. Furthermore Out $T \cong \mathrm{Sym}_3$ has the normal 3-cycle $\langle \sigma\rangle$, where $\sigma: i \to j$,

$j \to ij$. The group G must induce such an automorphism on T. That was an assumption when $O_2(G) = T$. In the cases $O_2(G) \cong \mathscr{Q}_8 \Upsilon \mathscr{C}$ or $\mathscr{Q}_8 \Upsilon \mathscr{D}_{2^{\alpha+1}}$, $\alpha \geqslant 3$, if this were false than G would normalise a 4-cycle in T. That cycle together with the cyclic factor or the cyclic subgroup of index 2 in the dihedral factor of $O_2(G)$, both of which are characteristic, would contradict Lemma 2.9. This is the reason why the present groups require a treatment different from the ones in Section 3. However, by a simple trick, also used in the paper of Amitsur [1, p. 375], we can overcome the problems. The crucial observation here is that the element $\rho = -(1+i+j+ij)/2 \in \mathbb{Q}\{T\}$ satisfies the relations

$$\rho i \rho^{-1} = j, \qquad \rho j \rho^{-1} = ij, \qquad \rho^3 = 1.$$

Moreover if $g \in G$ induces σ on T by conjugation, then this action extends to an automorphism of $\mathbb{Q}\{T\}$ as $g\mathbb{Q}\{T\}g^{-1} = \mathbb{Q}\{gTg^{-1}\} = \mathbb{Q}\{T\}$. Clearly this automorphism of $\mathbb{Q}\{T\}$ is nothing but conjugation by ρ. Hence $g\rho g^{-1} = \rho$. That could also be observed from the definition of ρ. Now the trick roughly is to replace gx for all $x \in C_G(T)$ by $g\rho^{-1}x$ (note $x\rho = \rho x$) to obtain a new group $\bar{G}$ which is free from the problem for G and spans the same enveloping algebra as G. Once $\bar{G}$ is classified, we reverse the procedure to retrieve the group G. Variations on this theme will be used extensively in this and Section 5. In these sections $G_{m,r}$ denotes a group of the type $\langle a, b;\ a^m = 1,\ b^n = a^t,\ bab^{-1} = a^r \rangle$, where $(m, r) = 1$, $(ns, t) = 1$, t odd, $n = \gamma(r, m)$, $st = m$, and $s = (r-1, m)$. See [1]. In that context n, s, and t will always have the above values.

Among the groups obtained here, many are subgroups of other (simpler) ones. For instance 4(e) is a subgroup of 4(c). We leave it to the reader to work out such relations.

2. LEMMA. *$R = M \times N$, where $M \cong \mathscr{Q}_8$, $N \cong \mathscr{C}_3 \times \mathscr{C}_3$, does not embed in $M_2(D)$.*

Proof. Suppose that it does. We have $\mathbb{Q}M \cong \mathscr{A} \oplus \mathbb{Q}^4$, $\mathbb{Q}N \cong \mathbb{Q}(\zeta)^4 \oplus \mathbb{Q}$, where $\zeta = \zeta_3$ and the exponent denotes the number of copies in the sum. Since M and N are represented faithfully in $\mathbb{Q}\{M\}$ and $\mathbb{Q}\{N\}$, we have $\mathbb{Q}\{M\} \cong \mathscr{A}$ or $\mathscr{A} \oplus \mathbb{Q}$ and $\mathbb{Q}\{N\} \cong \mathbb{Q}(\zeta) \oplus \mathbb{Q}(\zeta)$. Note that $\mathbb{Q}(\zeta)$ splits $\mathscr{A}$. Applying cases (c) or (d) of Lemma 2.4, we see that $\mathbb{Q}\{M\} \cong M_2(\mathbb{Q}(\zeta))^2$ or $M_2(\mathbb{Q}(\zeta)) \oplus \mathbb{Q}(\zeta)$. Contradiction.

3. LEMMA. *Suppose that $T \Upsilon_2 R \leqslant M_2(D)$, where $T \cong \mathscr{Q}_8$, R is soluble, $\mathbb{Q}\{TR\}$ is simple, $O_{2'}(F(R))$ is cyclic, and $O_2(R)$ is among the list in* 2.11. *Then R is one of the following groups*:

(a) $G_{m,r}$; $2 \mid s$.

(b) $\langle z \rangle \times G_{m,r}$; $\langle z \rangle = Z(T)$, *m is odd, and* $2 \parallel n$.

(c) $\mathscr{D}_8 \times G_{m,r}$; *mn is odd.*

(d) $\mathscr{D}_{2^{\alpha+1}m}$; $\alpha \geqslant 2$, $m > 1$ *is odd.*

(e) $\mathscr{D}_{2^{\alpha+1}}$; $\alpha \geqslant 3$.

Proof. It follows from Lemma 2.4 that $\mathbb{Q}\{T\}$ and $\mathbb{Q}\{R\}$ are simple. Since $T \curlyvee O_2(R) \leqslant M_2(D)$, one deduces in a manner similar to the proof of Lemma 2.11 that $O_2(R)$ does not have a $\mathscr{Q}$ or $\mathscr{S}$ factor. Hence $O_2(R)$ is cyclic or dihedral. Clearly the classification of Lemma 3.2 is applicable to a Sylow 2-subgroup of R. In addition Theorem 3.8 is relevant to R. Now going through the list in Lemma 3.2, one concludes by Lemma 2.4 that in the presence of T, the Sylow 2-subgroup of R is one of the following:

1. Cyclic. Then $R = G_{m,r}$. This is (a).

2. $\mathscr{D}_{2^{\alpha+1}}$ in class 1, $\alpha \geqslant 2$ (the class 2 groups are ruled out because their enveloping algebra is $M_2(D_1)$ with $2 \mid \text{index } D_1$. So D_1 is split partially by $\mathscr{A} = \mathbb{Q}\{T\}$). Let $S = \langle c, d \rangle$; $c^{2^\alpha} = 1$, $d^2 = 1$, $dcd^{-1} = c^{-1}$ be a Sylow 2-subgroup of R. If $O_2(R) = S$, then $R = O_2(R) \times R_1$, $R_1 \cong G_{m,r}$ has odd order. For $\alpha = 2$ this is (c). For $\alpha \geqslant 3$, the algebra $A = \mathbb{Q}\{T \curlyvee O_2(R)\} \cong M_2(\mathscr{A} \otimes_{\mathbb{Q}} \mathbb{Q}(\zeta + \zeta^{-1}))$, $\zeta = \zeta_{2^\alpha}$, has a nonzero invariant at the real places of the centre only. So it is split by a complex field. Hence $R_1 = 1$ and we get (e). Thus now assume that $O_2(R) = \langle c \rangle$. Write $R = L \rtimes (H \times S)$ as in the proof of Theorem 3.8 and put $m = |L \times C_H(L)|$. We have $\mathbb{Q}\{T \curlyvee (LC_H(L)S)\} \cong \mathscr{A} \otimes_K M_2(K)$, where K is the fixed field of d in $E = \mathbb{Q}(\zeta_{2^\alpha m})$. Now $e(E_2/K_2) = |I_2(E/\mathbb{Q}) \cap \langle d \rangle| = 1$ for d acts non-trivially on L. So $e(K_2/\mathbb{Q}_2) = 2^{\alpha-1}$. Since the nonzero invariants of $\mathscr{A}$ are at ∞ and 2, we require K to be real. Therefore $C_H(L) = 1$, $H = 1$, d inverts L, and we get (d).

3. $\langle z \rangle \times \mathscr{C}_2$, where $\langle z \rangle = Z(T)$. Then clearly $R = \langle d \rangle \times R_1$, where $R_1 \cong G_{m,r}$ with a Sylow 2-subgroup of order 2 and $O_2(R_1) = 1$. This is (b).

4. THEOREM. *Let G be soluble and induce an automorphism of order 3 on $O_2(G) = \langle i, j \rangle \cong \mathscr{Q}_8$. Then G is classified in the five classes below: In* (a_1), (a_2), (b_1), (b_2) *we have* $G_1 = G_{m,r}$. *In* (b_1), (b_2), *and* (c) *we have the relations*:

$$h^8 = 1,\ jhj^{-1} = h^{-1} \text{ or } h^3,\ i = h^2 \text{ or } h^{-2},\ \rho = -(1 + i + j + ij)/2.$$

So $h\rho h^{-1} = \rho^{-1} i$, $\rho i \rho^{-1} = j$, $\rho j \rho^{-1} = ij$.

(a_1) $T_\alpha^* \times G_1$; *m odd,* $4 \nmid n$. *If* $2 \mid n$ *then* $\alpha = 1$.

(a_2) $T_\alpha^* \curlyvee_2 G_1$; $2 \| s$, $2 \| n$, $\alpha \geqslant 1$.

(b_1) $\langle j, h, \rho \rangle \in G_1$; *m odd,* $G_1 \cong \mathscr{D}_{2m}$, $jhj^{-1} = h^{-1}$; *or mn odd.*

(b_2) $\langle j, h, \rho \rangle \curlyvee_2 G_1$; $2 \| s$, $2 \| n$.

(c) $\langle j, h, \rho \rangle \wr \langle a, b \rangle$;

$a^m = 1$, $b^n = a^t$, $bab^{-1} = a^r$; $\langle i, j, \rho \rangle$ *commutes with* $\langle a, b \rangle$, $hb = bh$, $hah^{-1} = a^{r'}$; $2 = \gamma(r', m)$, $n = \gamma(r, m)$, $s = (r-1, r'-1, m)$, *mn odd*, $st = m$, $(ns, t) = 1$.

(d_1) $\langle i, j \rangle \rtimes \langle a, g \rangle$; *m odd*, $4 \nmid n$.

(d_2) $\langle i, j \rangle \rtimes_2 \langle a, g \rangle$; $2 \| s$, $2 \| n$.

For these two groups $\langle a, g \rangle = G_{m,r}$, $a^m = 1$, *etc.*; $3 \mid n$; $g: i \to j, j \to ij$; $\langle i, j \rangle$ *commutes with a.*

(e) $G = \langle j, h \rangle \langle g, b \rangle$;

$h^8 = 1$, $jhj^{-1} = h^{-1}$; $i = h^2$, $j^2 = h^4$; $gig^{-1} = j$, $gjg^{-1} = ij$; $g^m = 1$, $b^n = g^t$, $bgb^{-1} = g^r$; $\langle j, h \rangle$ *commutes with b*, $hgh^{-1} = g^r i$; $r'^2 \equiv 1(m)$, $r' \equiv -1(3)$, $3 \mid t$, $st = m$, $(ns, t) = 1$, $s = (r-1), r'-1, m)$, *mn odd.*

Proof. Put $T = O_2(G)$, $R = C_G(T)$, and $\tilde{G} = G/TR$. We have $\mathbb{Q}\{T\} \cong \mathscr{A}$ and $\tilde{G} \subsetneq \mathrm{Sym}_3$. In view of the assumption on G, we have two possibilities:

(1) $\tilde{G} \cong \mathscr{C}_3$. Let $g \in G$ be such that $g: i \to j, j \to ij$.

The element g is well defined modulo R, $g^3 \in R$, and $G = \langle T, R, g \rangle$. Put $\rho = -(1+i+j+ij)/2$. Then ρ and $\langle R, g \rangle$ commute, $\rho^3 = 1$, $\rho i \rho^{-1} = j$, $\rho j \rho^{-1} = ij$. Hence $\bar{g} = g\rho^{-1}$ centralizes T and $\bar{g}^3 = g^3$. Put $R_1 = \langle R, \bar{g} \rangle$, $\bar{G} = \langle T, R, \bar{g} \rangle = T \curlyvee R_1$. We have $\mathbb{Q}\{\bar{G}\} = \mathbb{Q}\{G\}$, $O_{\pi'}(F(R_1)) = O_{\pi'}(F(G))$, where $\pi = \{2, 3\}$, $O_2(R_1) = Z(T)$, and $O_3(R_1)$ is cyclic by Lemma 2. Hence we deduce from Lemma 3 that R_1 is ($Z(T)$ or 1) $\times$ metacyclic with a Sylow 2-subgroup of order at most 4. To get back to G, one has to consider two cases. First, $\bar{g} \in R$. Then we can take $g = \rho$, giving the groups (a_1) or (a_2) with $\alpha = 1$. Second, $\bar{g} \notin R$. Then R_1 has the normal subgroup R of index 3. Therefore if $O_3(R_1)$ is the Sylow 3-subgroup of R_1 then we have $R_1 = (Z(T)$ or $1) \times \langle c \rangle \times G_1$, where $c^{3^\alpha} = 1$, $\alpha \geqslant 1$, and $G_1 = G_{m,r}$ has order coprime to 3. Obviously we can take $\bar{g} = c$ so $g = c\rho$ and we get (a_1) or (a_2). Note that $\mathbb{Q}\{T, g\} = \mathscr{A} \otimes_{\mathbb{Q}} \mathbb{Q}(\zeta) = M_2(\mathbb{Q}(\zeta))$, where $\zeta = \zeta_{3^\alpha}$. So in (a_1), G_1 must be of odd order. Finally, suppose $O_3(R_1)$ is smaller than a Sylow 3-subgroup of R_1 and write $R_1 = (Z(T)$ or $1) \times \langle a, b \rangle$, where $a^m = 1$, $b^n = a^t$, $bab^{-1} = a^r$, $st = m$, $s = (r-1, m)$, and $3 \mid n$. Clearly $R = (Z(T)$ or $1) \times \langle a, b^3 \rangle$, so we can take $\bar{g} = b$, $g = b\rho$. Then $G = \langle T, a, b^3, g \rangle = T \rtimes \langle a, g \rangle$ or $T \rtimes_2 \langle a, g \rangle$ with $gag^{-1} = a^r$ and $g^n = a^t$. These are the groups (d_1) and (d_2).

(2) $\tilde{G} \cong \mathrm{Sym}_3$. Pick $g, h \in G$ such that

$$g: i \to j, j \to ij; \qquad h: i \to i, j \to ij.$$

Then $g^3 = *$, $h^2 = *i$, $hgh^{-1} = *g^{-1}i$, where $*$ denotes an element of R and $G = \langle T, R, g, h \rangle$. Let ρ and $\bar{g}$ be as in (1). $\bar{G} = \langle T, R, \bar{g}, h \rangle$ is a finite

group for $h\rho h^{-1} = \rho^{-1} i$, $h\bar{g}h^{-1} = *\bar{g}^{-1}$. Like before $\mathbb{Q}\{\bar{G}\} = \mathbb{Q}\{G\}$ and we have two cases to consider. First, suppose that $\bar{g} \in R$. Then we can take $g = \rho$. $G = \langle T, R, h \rangle$, the 2'-part of the Fitting subgroup of G, R, or $\bar{G}$ is the same and $|O_2(\bar{G}) : T| \leqslant 2$. So $O_2(\bar{G}) = T$ of Q_{16} or $\mathscr{S}_{16}$. Clearly Theorem 3.8 is applicable to $\bar{G}$. Thus if $O_2(\bar{G}) = T$, then the relevant case is 3.8(d). Since we are free to change h by elements of R, we can take $h^2 \in T$, so we get the group (c). Next, if $O_2(\bar{G}) > T$ then 3.8(b), (g) or (i) applies to $\bar{G}$, getting the (b) groups. Finally, assume that $\bar{g} \notin R$. Then $F(\bar{G}) = F(G)$. Again Theorem 3.8 is applicable to $\bar{G}$. In fact $\bar{G}$ is of the type 3.8(d). So we can express $\bar{G} = \langle j, h, a, b \rangle$, where $\langle j, h \rangle \cong \mathscr{Q}_{16}$ or $\mathscr{S}_{16}$ is a Sylow 2-subgroup of $\bar{G}$ and $a^m = 1$, $b^n = a^t$, $bab^{-1} = a^r$, mn odd; $\langle j, h \rangle$ commutes with b, $ja = aj$, $hah^{-1} = a^{r'}$; $st = m$, $(ns, t) = 1$, and $s = (r-1, r'-1, m)$. Since $\bar{G}/TR \cong \mathrm{Sym}_3$, we must have $r' \equiv -1(3)$ and $3 \mid t$. If $\langle j, h \rangle \cong \mathscr{S}_{16}$, then let $c \in \langle a \rangle$ be of order 3. So $hch^{-1} = c^{-1}$. In the algebra $A = \mathbb{Q}\{j, h, c\}$, j and $h' = h(1-i)$ commute (where $i = h^{-2}$) and $h'^2 = -2$. By Lemma 2.3, $A = \langle \mathbb{Q}(i), g, -1 \rangle \otimes_{\mathbb{Q}} \langle \mathbb{Q}(\zeta_3), h', -2 \rangle$. Now both algebras have invariant $\frac{1}{2}$ at 2 and ∞. So $A = M_4(\mathbb{Q})$, a contradiction. Thus $\langle j, h \rangle \cong \mathscr{Q}_{16}$, $i = h^2$. We can take $\bar{g} = a$, $g = a\rho$. Then $R = \langle a^3, b \rangle$ and $G = \langle j, h, g, b \rangle$. We have $bgb^{-1} = a^r \rho = (a\rho)^r = g^r$ for $r \equiv 1(3)$ as $n = \gamma(r, m)$ is odd. $b^n = a^t = (a\rho)^t = g^t$, $g^m = (a\rho)^m = 1$, and $hgh^{-1} = a^{r'} \rho^{-1} i = (a\rho)^{r'} i = g^{r'} i$. This shows that G is the group (e) and the proof is completed.

5. THEOREM. *Let G be soluble and $O_2(G) = T \curlyvee \langle c \rangle \cong \mathscr{Q}_8 \curlyvee \mathscr{C}_{2^\alpha}$, $\alpha \geqslant 2$. Put $T = \langle i, j \rangle$, $\rho = -(1+i+j+ij)/2$, $\eta = c^{2^{\alpha-2}}$. There are 12 classes for G, listed below. In them, the elements g, h normalize T; $hih^{-1} = i$, $hjh^{-1} = ij$ $(h\rho h^{-1} = \rho^{-1} i)$; $gig^{-1} = j$, $gjg^{-1} = ij$.*

(a) $T_\beta^* \curlyvee_2 G_{m,r}$;

$T_\beta^* = \langle i, j, g \rangle$; $g^{3^\beta} = 1$; $2^\alpha \| s$. Either $g = \rho$, $\beta = 1$ or $g \neq \rho$, $\beta \geqslant 1$ and $3 \nmid mn$.

(b) $T^* \curlyvee_2 \mathscr{D}_{2^{\alpha+1}m}$; *$T^* = \langle i, j, \rho \rangle$, $m > 1$ odd.*

(c) $\langle i, j \rangle \wr_2 \langle a, g \rangle$;

$\langle a, g \rangle = G_{m,r}$; $2^\alpha \| s$, $3 \mid n$; $\langle i, j \rangle$ commutes with a.

(d) $(T^* \curlyvee_2 G_{m,r})\langle h \rangle$;

$T^* = \langle i, j, \rho \rangle$; $2^\alpha \| s$, $h = (1+i)(1+\eta)/2$. So $h^2 = i\eta$ and h centralises $G_{m,r}$.

(e) $(T^* \curlyvee_2 \mathscr{D}_{2^{\alpha+1}m})\langle h \rangle$;

$T^* = \langle i, j, \rho \rangle$; $\mathscr{D}_{2^{\alpha+1}m} = \langle x, d \rangle\, x^{2^\alpha m} = 1$, $d^2 = 1$, $dxd^{-1} = x^{-1}$, $m > 1$ odd, $\langle c \rangle < \langle x \rangle$; $h : x \to x$, $d \to \eta d$, and $h^2 = i\eta$.

(f) $(T^* \curlyvee_2 \langle a, b_1 \rangle)\langle h \rangle$;

$T^* = \langle i, j, \rho \rangle$; $a^m = 1$, $b^{n/2} = a^t$, $bab^{-1} = a^{r^2}$, $st = m$, $2^\alpha \| s$, t odd, $2 \mid n$, $(ns, t) = 1$; $h : a \to a^r$, $b_1 \to b_1$; $h^2 = b_1 i\eta$; $s = (r-1, m)$.

(g) $(T^* \curlyvee_2 \langle c\rangle)\langle h\rangle \times G_{m,r}$;

$T^* = \langle i, j, \rho\rangle$; $hc = ch$; $h^2 = ic\eta$; *mn odd.*

(h) $\mathcal{O}^* \upharpoonright_2 \langle x\rangle$;

$\mathcal{O}^* = \langle i, j, \rho, h\rangle$, $h^2 = i$; $x^{2^\alpha m} = 1$, $m \geqslant 1$ *odd*; $\langle i, j, \rho\rangle$ *commutes with* $\langle x\rangle$, $h: x \to x^{-1}$.

(i_1) $\mathcal{O}^* \curlyvee_2 \mathcal{D}_{8m}$; $\alpha = 2$, $m > 1$ *odd.*

(i_2) $(T^* \curlyvee_2 \mathcal{D}_{2^{\alpha+1}m})\langle h\rangle$;

$T^* = \langle i, j, \rho\rangle$; $\mathcal{D}_{2^{\alpha+1}m} = \langle x, d\rangle$, $x^{2^\alpha m} = 1$, $\alpha \geqslant 3$, $m > 1$ *odd*; $h^2 = ix$, $h: x \to x$, $d \to xd$.

(j) $(\mathcal{O}^* \upharpoonright_2 \langle c\rangle) \times G_{m,r}$;

$\mathcal{O}^* = \langle i, j, \rho, h\rangle$, $h^2 = i$; $\alpha = 2$, $h: c \to c^{-1}$; $mn > 1$ *odd.*

(k) $\langle i, j, g, b_1, h\rangle$;

$g^m = 1$, $b_1^{n/2} = g^t$, $b_1 g b_1^{-1} = g^{r^2}$; $hgh^{-1} = g^r i$, $hb_1 = b_1 h$, $h^2 = ib_1\eta$; $c \in \langle g\rangle$; T *and* b_1 *commute*; $n = \gamma(r, m)$, $r \equiv -1(3)$, $2 \mid n$, $2^\alpha \| s$, $3 \mid t$, $ts = m$, $(t, ns) = 1$, t *odd*, $s = (r-1, m)$.

(l) $\langle i, j, g, h\rangle$;

$h^2 = i$, $g^{2^\alpha m} = 1$, $hgh^{-1} = g^{-1}i$; m *odd*, $3 \mid m$.

Proof. We proved in 2.13 that T (and $\langle c\rangle = Z(O_2(G))$) is characteristic in G. So $\mathbb{Q}\{T\} \cong \mathscr{A}$ and $\mathbb{Q}\{c\} \cong \mathbb{Q}(\zeta_{2^\alpha})$. Put $R = C_G(T)$. Then $O_2(R) = \langle c\rangle$ and $\tilde{G} = G/TR \subsetneq \mathrm{Sym}_3$. As proved in 1, $3 \mid |\tilde{G}|$. We pick g and h (if $\tilde{G} \cong \mathrm{Sym}_3$) in G to induce the automorphisms

$$g: i \to j,\ i \to ij; \qquad h: i \to i,\ j \to ij$$

on T. So g and h are well determined modulo R and satisfy the relations

$$g^3 = *, \qquad h^2 = *i, \qquad hgh^{-1} = *g^{-1}i, \qquad \text{where} \quad * \in R.$$

Now pick $\eta \in \langle c\rangle$ of order 4 and put

$$\rho = -(1 + i + j + ij)/2, \qquad \bar{g} = g\rho^{-1}, \qquad \bar{h} = h(1-i)(1-\eta)/2.$$

$\bar{g}$ and $\bar{h}$ centralise T and act as automorphisms on R. The last assertion in clear for $\bar{g}$. As to $\bar{h}$, we observe first that $O_{2'}(F(R))$ is normal in G, hence cyclic, and R is classified under Lemma 3. The relevant cases are (a) and (d). For (a), $\eta \in Z(R)$ so h and $\bar{h}$ have the same action on R. In (d), putting $R = \langle x, d\rangle$, $x^{2^\alpha m} = 1$, $d^2 = 1$ we have $(1-\eta)\, x (1-\eta)^{-1} = x$, $(1-\eta)\, d (1-\eta)^{-1} = \eta^{-1} d$. So $\bar{h}$ induces an automorphism on R in this case as well. As before $\bar{g}^3 = g^3$ and we distinguish two cases according to $\tilde{G}$:

(1) $\bar{G} \cong \mathscr{C}_3$. The treatment of this case is similar to the one in Theorem 4. First suppose that $\bar{g} \in R$. Then we can take $g = \rho$ so $G = T^* \Upsilon_2 R$, where $R \cong G_{m,r}$ or $\mathscr{D}_{2^{\alpha+1}m}$, $m > 1$ odd, as we saw above. This gives (a) and (b). Next suppose that $\bar{g} \notin R$. Put $\bar{R} = \langle R, \bar{g} \rangle$. We have modified G to get the groups $\bar{G} = T \Upsilon \bar{R}$ with the same enveloping algebra. A Sylow 3-subgroup of $\bar{R}$ is cyclic by Lemma 2, $O_2(\bar{R}) = \langle c \rangle$, and $O_{\pi'}(\bar{R}) = O_{\pi'}(G)$, where $\pi = \{2, 3\}$. So we can apply Lemma 3 to $\bar{R}$. Since $\bar{R}$ has the normal subgroups R of index 3, only the case (a) is applicable to $\bar{R}$. Now if $O_3(\bar{R})$ is the Sylow 3-subgroup then we can write $\bar{R} = \langle d \rangle \times G_{m,r}$, where $d^{3^\beta} = 1$, $\beta \geqslant 1$, and $3 \nmid mn$. So $R = \langle d^3 \rangle \times G_{m,r}$, $g = d\rho$, and $G = T_\beta^* \Upsilon G_{m,r}$ as in (a). Finally, if $O_3(\bar{R})$ is smaller than a Sylow 3-subgroup, then we have $\bar{R} = \langle a, b \rangle = G_{m,r}$, where $3 \mid n$ and $R = \langle a, b^3 \rangle$. We can take $\bar{g} = b$, $g = b\rho$. So $G = T \rtimes \langle a, g \rangle$ as in (c). This concludes (1).

(2) $\bar{G} \cong \mathrm{Sym}_3$. Here the relations for $\bar{g}$ and $\bar{h}$ are

$$\bar{g}^3 = *, \qquad \bar{h}^2 = *, \qquad \bar{h}\bar{g}\bar{h}^{-1} = *\bar{g}^{-1}, \qquad \text{where } * \in R.$$

For the last relation, note that g centralises $O_2(R)$ and η. Put $\bar{R} = \langle R, \bar{g}, \bar{h} \rangle$, a finite group. If $\bar{h} \in R$ then $g \equiv \bar{g}^{-1} \bmod R$, so that $\bar{g} \in R$. Hence $|\bar{R} : R| = 1, 2$, or 6. We consider these cases separately:

(2.1) $\bar{R} = R$. We have $g = x\rho$, $h = y(1 + i)(1 + \eta)/2$; $x, y \in R$. Replacing g, h by $x^{-1}g$, $y^{-1}h$, we can assume $g = \rho$ and $h = (1 + i)(1 + \eta)/2$. As we have seen $R \cong G_{m,r}$ or $\mathscr{D}_{2^{\alpha+1}m}$, $m > 1$ odd. So we have $G = (\langle i, j, h \rangle \Upsilon_2 R)\langle h \rangle$ as in (d) or (e).

(2.2) $|\bar{R} : R| = 2$. Like above, take $g = \rho$. Now $\bar{R} = \langle R, \bar{h} \rangle$ and $O_2(\bar{R})$ has $\langle c \rangle$ as a subgroup of index 1 or 2. Since $T \Upsilon O_2(\bar{R}) \leqslant M_2(D)$, we must have $O_2(\bar{R}) \cong \mathscr{C}$ or $\mathscr{D}$. Furthermore $O_{2'}(F(R)) = O_{2'}(F(G))$. Hence we can apply Lemma 3 to $\bar{R}$. All the cases there except (b) are relevant:

First, suppose that $\bar{R}$ has type 2(a). If $O_2(\bar{R})$ is smaller than a Sylow 2-subgroup, then write $\bar{R} = \langle a, b \rangle = G_{m,r}$; $2 \mid n$, $2^\alpha \| s$. Now $R = \langle a, b^2 \rangle$, $\bar{h} = b$, so $h = b(1 + i)(1 + \eta)/2$. Put $b_1 = b^2$. We get $G = \langle T, \rho, a, b_1, h \rangle$ as in (f). However, if $O_2(\bar{R})$ is the Sylow 2-subgroup, then we can write $\bar{R} = \langle d \rangle \times G_{m,r}$, $d^{2^{\alpha+1}} = 1$, $d^2 = c$, and mn is odd. We have $R = \langle c \rangle \times G_{m,r}$, $\bar{h} = d$, $h = d(1 + i)(1 + \eta)/2$, and $G = \langle T, \rho, c, h \rangle \times G_{m,r}$ as in (g).

Second, let $\bar{R} = \langle x, d \rangle$, $d^2 = 1$ be of type 2(d) or 2(e). There are two types of subgroups of index 2 in $\bar{R}$. If R is cyclic, then $R = \langle x \rangle$, $x^{2^\alpha m} = 1$, $m \geqslant 1$ odd. So $\bar{h} = d$, $h = d(1 + i)^2(1 + \eta)/2$, $h^2 = (1 + i)^2(1 - \eta^2)/4 = i$ and $G = \langle T, \rho, h \rangle \rtimes_2 \langle x \rangle$, $h : x \to x^{-1}$, and $\langle T, \rho, h \rangle \cong \mathscr{O}^*$. This is (h). However, if R is dihedral, then without loss of generality we can take $R = \langle x^2, d \rangle$, $x^{2^{\alpha+1}m} = 1$, $m > 1$. We put $\bar{h} = x$, $h = x(1 + i)(1 + \eta)/2$, $x_1 = x^2$. So $G = \{\langle i, j, \rho \rangle \Upsilon_2 \langle x_1, d \rangle\}\langle h \rangle$; $h^2 = ix_1\eta$, $h : x_1 \to x_1$, $d \to x_1\eta d$. If $\alpha = 2$, then we can choose $\gamma \in \langle x_1 \rangle$ of odd order and η such that $\gamma^2 \eta x_1 = 1$.

Then $(\gamma h)^2 = i$, $\gamma h: x_1 \to x_1$, $d \to d$. We get (i_1). If $\alpha \geqslant 3$, then choose $\gamma \in \langle x_1 \rangle$ such that $\gamma^2\eta = 1$ and put $h_1 = \gamma h$. We have $h_1^2 = ix_1$, $h_1: x_1 \to x_1$, $d \to x_1 d$. This is the group (i_2), where we have written x, h instead of x_1, h_1.

Finally, let $\bar{R} = \langle c, d \rangle \times G_{m,r}$, where $\langle c, d \rangle = \mathscr{D}_8$, $\alpha = 2$, and $mn > 1$ is odd. Here $R = \langle c \rangle \times G_{m,r}$ and like the second case above, we get $G = (\mathscr{O}^* \wr_2 \langle c \rangle) \times G_{m,r}$. This is (j).

(2.3) $|\bar{R} : R| = 6$. Here a Sylow 3-subgroup of $\bar{R}$ is cyclic by Lemma 2, $O_2(\bar{R}) = \langle c \rangle$, and $O_{\pi'}(F(\bar{R})) = O_{\pi'}(F(G))$, where $\pi = \{2, 3\}$. So $\bar{R}$ is classified in Lemma 3, cases (a) and (d). First suppose 3(a) holds. So $R = \langle a, b \rangle = G_{m,r}$, $a^m = 1$, etc. Since $\bar{R}/R \cong \mathrm{Sym}_3$, we must have $3 \mid t$, $2 \mid n$, $r \equiv -1(3)$, and $R = \langle a^3, b^2 \rangle$. Since a, b, r can be replaced by a^{-1}, b^{-1}, r^{-1} (mod m) and then b by any of its conjugates, we can put $\bar{g} = a$, $\bar{h} = b$ so $g = a\rho$, $h = b(1+i)(1+\eta)/2$. Hence $G = \langle T, a^3, b^2, g, h \rangle = \langle T, g, b_1, h \rangle$; $b_1 = b^2$, $hgh^{-1} = a^r\rho^{-1}i = g^r i$, $b_1 g b_1^{-1} = g^{r^2}$, $g^m = 1$, $b_1^{n/2} = g^t$, $h^2 = ib_1\eta$. This is the group (k). Finally, suppose that 3(d) holds:

$$\bar{R} = \langle a, b \rangle \cong \mathscr{D}_{2^{\alpha+1}m}, \qquad a^{2^\alpha m} = 1,\ b^2 = 1,\ bab^{-1} = a^{-1},\ m > 1 \text{ odd}.$$

Here, we must have $3 \mid m$, $R = \langle a^3 \rangle$. Put $\bar{g} = a$, $\bar{h} = b$ so $g = a\rho$, $h = b(1+i)(1+\eta)/2$. We have $g^3 = a^3$, $h^2 = i$, $hgh^{-1} = a^{-1}\rho^{-1}i = g^{-1}i$, and $G = \langle T, g, h \rangle$ as in (1).

The proof of Theorem 5 is complete.

6. THEOREM. *Let G be a soluble primitive, finite subgroups of $M_2(D)$ and $O_2(G) = T \Upsilon_2 S$, where $T = \langle i, j \rangle \cong \mathscr{Q}_8$ and $S = \langle a, b \rangle \cong \mathscr{D}_{2^{\alpha+1}}$, $\alpha \geqslant 3$; $a^{2^\alpha} = 1$, $b^2 = 1$, ${}^b a = a^{-1}$. In $\mathbb{Q}\{T\}$, put $\rho = -(1+i+j+ij)/2$. Then G is one of the following three groups*:

(a) $T^* \Upsilon_2 S$; $\quad T^* = \langle i, j, \rho \rangle$.

(b) $\mathscr{O}^* \Upsilon_2 S$; $\quad \mathscr{O}^* = \langle i, j, \rho, h \rangle$; $h^2 = i$, $h: i \to i$, $j \to ij$, $\rho \to \rho^{-1}i$. ($h = (1+i)/(\zeta + \zeta^{-1})$, *where* $\zeta = a^{2^{\alpha-3}}$.)

(c) $(T^* \Upsilon_2 S)\langle h \rangle$; $\quad T^* = \langle i, j, \rho \rangle$; $h^2 = ia$, $h: i \to i$, $j \to ij$, $\rho \to \rho^{-1}i$, $a \to a$, $b \to ab$.

Proof. The proof could be incorporated in the calculations of Theorem 5. However, in the interests of clarity, we give an alternative proof. We proved in 2.13 that T, S, and $\langle a \rangle$ are characteristic in $O_2(G)$. Therefore $\mathbb{Q}\{T\} = \mathscr{A}$, $\mathbb{Q}\{S\} = M_2(K)$, where $K = \mathbb{Q}(\zeta_{2^\alpha} + \zeta_{2^\alpha}^{-1})$ and $\mathbb{Q}\{O_2(G)\} = M_2(\mathscr{A}_K)$. The algebra $\mathscr{A}_K$ has nonzero invariant at the real places of K only. So $O_{2'}(F(G)) = 1$. Putting $R = C_G(T)$, we have $O_2(R) = S$, $O_{2'}(R) = 1$ so $F(R) = S$. By Fitting's lemma, $R/S \subsetneq \mathrm{Out}\, S$, which is a 2-group. Hence $R = S$ and $\tilde{G} = G/O_2(G) \subsetneq \mathrm{Out}\, T \cong \mathrm{Sym}_3$. We saw in 1 that

$3 \mid |\tilde{G}|$. Hence there exists $g \in G$ of order 3 exactly such that $g: i \to j, j \to ij$. Clearly $[g, S] = 1$. Put $\rho = -(1+i+j+ij)/2$, $\bar{g} = g\rho^{-1}$. Then $\bar{g}$ centralizes $O_2(G)$ and $\bar{g}^3 = 1$. Since $\mathbb{Q}(\zeta_3)$ splits $\mathscr{A}$, we get a contradiction by Lemma 2.4 if $\bar{g} \neq 1$. Hence $g = \rho$. When $\tilde{G} = \mathscr{C}_3$, we have $G = \langle O_2(G), \rho \rangle = \langle i, j, \rho \rangle \curlyvee S$, which is (a). Hence suppose that $\tilde{G} \cong \mathrm{Sym}_3$. Let $h \in G$ be of order 2 mod $O_2(G)$ such that $h: i \to i, j \to ij$. So h is well determined modulo S and $h^2 = *i$ with $* \in S$. Let $\zeta \in \langle a \rangle$ be of order 8 and put $\eta = \zeta + \zeta^{-1} \in Z(\mathbb{Q}\{S\})$, $\bar{h} = h(1-i)/\eta$. Then $\bar{h}$ centralises T, h and $\bar{h}$ have the same action on S, $\eta^2 = 2$ and $\bar{h}^2 \in S$. If $\bar{h} \in S$, then we replace h by $\bar{h}^{-1}h = (1+i)/\eta$; getting the group (b). If $\bar{h} \notin S$, then by Lemma 3, $\langle S, \bar{h} \rangle = \mathscr{D}_{2^{a+2}}$. Hence by changing h with a suitable element of S, we can take $\bar{h}^2 = a$, $\bar{h}: a \to a$, $b \to ab$. Therefore $h^2 = ia$ and $h: a \to a$, $b \to ab$ as in (c). The theorem is proved.

In the final classification theorem of this section, we need to know about the groups $\mathscr{B}$ and $\mathscr{B}^*$ and their embeddings in $M_2(\mathscr{A})$ and $M_2(\mathscr{A}) \otimes_{\mathbb{Q}} \mathbb{Q}(\sqrt{2})$. This is dealt with in Theorem 6 and Lemma 7 of the next section.

7. THEOREM. *Let G be a finite primitive soluble subgroup of $M_2(D)$ and $T = O_2(G) \cong \mathscr{Q}_8 \curlyvee \mathscr{D}_8$. Then $G = R \times G_{m,r}$, where R is a soluble subgroup of $\mathscr{B}^*$ containing $O_2(\mathscr{B}^*)$ and $(mn, 30) = 1$. If $R \not\leq \mathscr{B}$ then $mn = 1$. In fact only four types of subgroups of* Sym_5 *are allowed for $R/O_2(R)$, namely* Sym_3, $\mathscr{C}_5$, $\mathscr{D}_{10}$, *and $\mathscr{C}_5 \rceil \mathscr{C}_4$, where only in the last case $R \not\leq \mathscr{B}$.*

Proof. Observe that if $S \cong \mathscr{Q}_8 \curlyvee \mathscr{D}_8$, then $\mathbb{Q}S \cong M_2(\mathscr{A}) \oplus \mathbb{Q}^{16}$. For there are 16 one-dimensional representations of S in $\mathbb{Q}$ and there is one in $M_2(\mathscr{A})$ spanning it over $\mathbb{Q}$. Hence if ϕ, $\phi': S \to A \cong M_2(\mathscr{A})$ are two embedding of S in A, then the map $\phi(s) \to \phi'(s)$ for all $s \in S$ extends linearly to an automorphism of A. So by the Noether–Skolem theorem $\phi'(s) = x\phi(s)x^{-1}$ for some $x \in A$. Thus any two faithful representation of S in $M_2(\mathscr{A})$ are conjugate.

Now consider G. We have $\mathbb{Q}\{T\} \cong M_2(\mathscr{A})$. A Sylow 2-subgroup S of $C_G(T)$ is $Z(T)$, otherwise $\mathrm{rank}(ST/Z(T)) > 4$ contrary to Lemma 2.10(c) Since $O_{2'}(F(C_G(T))) = O_{2'}(F(G))$ is cyclic, we have $C_G(T) = Z(T) \times G_1$, where $G_1 = G_{m,r}$ has odd order. $\mathbb{Q}(\zeta_3)$ or $\mathbb{Q}(\zeta_5)$ splits $\mathscr{A}$. Therefore $(mn, 30) = 1$. Now $G/TG_1 \to \mathrm{Out}\, T = \mathrm{Sym}_5$. Therefore $(|G/TG_1|, |G_1|) = 1$ and by the Schur–Zassenhaus theorem, there exists a subgroup R of G such that $G = RG_1$, $R \cap G_1 = 1$, $T \leqslant R$, and $\bar{R} = R/T \to \mathrm{Out}\, T = \mathrm{Sym}_5$. Let R_1 be the inverse image of Alt_5 in R. By the first paragraph above and Theorem 5.5 on the embedding of $\mathscr{B}$. We can construct a group $H \cong \mathscr{B}$ in $\mathbb{Q}\{T\}$ such that $T = O_2(H)$. We prove that $R_1 \leqslant H$. For instance, suppose that $2 \mid |R_1/T|$ and take $g \in R_1$ of order 2 modulo T. There exists $\gamma \in H$ with the same action on T as g. Hence g and γ have the same action on $\mathbb{Q}\{T\}$.

Thus $g\gamma = \gamma g$. Now $g\gamma^{-1}$ centralises T and has 2-power order. Since $\mathbb{Q}(i)$ splits $\mathscr{A}$, we must have $g\gamma^{-1} = \pm 1$ so that $g = \pm\gamma \in H$. We can proceed similarly for elements of R_1 of order 3 or 5, proving the claim. Since $\mathbb{Q}\{T\}$ commutes with G_1, it follows that $[R_1, G_1] = 1$. Now consider the case $|R : R_1| = 2$. Put $T = \langle a, b\rangle \curlyvee \langle c, d\rangle \cong \mathscr{Q}_8 \curlyvee \mathscr{Q}_8$ and pick $h \in R \backslash R_1$. From the construction of the group $\mathscr{B}^*$, it follows that for some $x \in H$, $\eta = x(a+b)c$ induces the same automorphism on T as h. Therefore $\eta^2 = \pm 2h^2$. So $\eta \in \mathbb{Q}\{T\}$ and h commute, $\eta^{-1}h$ centralizes T, R_1, and $(\eta^{-1}h)^2 = \pm 1/2$. Since $\mathbb{Q}(\sqrt{-2})$ splits $\mathscr{A}$, we must have $\eta^2 = 2h^2$ and $h = \pm\eta/\sqrt{2}$. Thus $\mathbb{Q}\{R\} \cong M_2(\mathscr{A}) \otimes_{\mathbb{Q}} \mathbb{Q}(\sqrt{2})$. Let $F(G_1) = \langle g\rangle$ have order m. Suppose that $m \neq 1$. If h acts nontrivially on $\langle g\rangle$ then $\mathbb{Q}\{R, g\} = M_2(\mathscr{A}) \otimes_{\mathbb{Q}} \langle \mathbb{Q}(\zeta_m), \eta^{-1}h, \frac{1}{2}\rangle$, which has exponent $\leqslant 2$, a contradiction. If h centralizes $\langle g\rangle$, then $\mathbb{Q}\{R, g\} = M_2(\mathscr{A}) \otimes_{\mathbb{Q}} \mathbb{Q}(\sqrt{2}, \zeta_m)$, which is split, a contradiction. Hence $m = 1$, $G_1 = 1$, and $G = R \leqslant \mathscr{B}^*$ in this case. Now we come to the choices for $\bar{R}$ in Sym_5. Obviously conjugate subgroups of Sym_5 produce isomorphic groups R, so we need to consider conjugacy classes of subgroups. Note that $O_2(\bar{R}) = 1$. If $5 \nmid |\bar{R}|$, then it is easily shown that $\bar{R} \cong \mathrm{Sym}_3$ of which there are two conjugacy classes. It can be verified that in this case the group R is $\mathscr{O}^* \curlyvee \mathscr{Q}_8$ or $(T^* \curlyvee \mathscr{Q}_8)\langle h\rangle$, where $h: a \to a$, $b \to ab$, $c \to c$, $d \to cd$, $h^2 = ac$. The first group is imprimitive and ruled out. The second group is primitive and $R < \mathscr{B}$. In fact $h = (1+a)(1+c)/2$ (cf. Theorem 6(b), (c)). If $5 \mid |\bar{R}|$ then $\bar{R}$ has a normal subgroup of order 5 so $\bar{R}$ is in the normaliser of a Sylow 5-subgroup which is $\mathscr{C}_5 \rfloor \mathscr{C}_4$. Thus there are three choices for $\bar{R}$ each of one conjugacy class. Finally, one can see that only the normaliser itself is not contained in Alt_5. The theorem is now completely proved.

8. It can be shown that all the groups obtained in this section are primitively represented in $A = \mathbb{Q}\{G\}$. For this purpose, we assume that A has the structure described during the proofs of Theorems 4, 5, and 6. Namely $A = \mathbb{Q}\{\bar{G}\}$ is either a crossed product algebra or the tensor product of $\mathscr{A}$ with one. By Lemma 2.2, it is sufficient to show that for any subgroup H of G of index 2, $\mathbb{Q}\{H\}$ is a simple algebra. In particular, this would be the case if H has a subgroup H_1 with $\mathbb{Q}\{H_1\} \cong M_2(*)$. This remark takes care of the groups in Theorem 5 when $\alpha \geqslant 3$, 6, and 7. For one can easily prove that $H_1 = T \curlyvee \langle c^2\rangle$, $T \curlyvee \langle a^2\rangle$, or $\langle a, b\rangle \curlyvee \langle c\rangle$, respectively, lies in H. As to the remaining groups, we illustrate the method for two examples. Note that $T \leqslant H$. First consider $4(\mathrm{b}_2)$: $G = \langle j, h, \rho\rangle \curlyvee \langle a, b\rangle$ with $h^2 = i$. We have $h = (1+i)/\sqrt{2}$, $\sqrt{2} \in Z(A)$, and $\mathbb{Q}\{\sqrt{2}, a\}$ a field (as $2 \| m$). Thus the cases $H = \langle i, j, \rho\rangle \curlyvee \langle a, b\rangle$ and $H = \langle j, h, \rho\rangle \curlyvee \langle a, b^2\rangle$ follow from Lemma 2.4(a). For $H = (\langle i, j, \rho\rangle \curlyvee \langle a, b^2\rangle)\langle hb\rangle$ we have $hb = (1+i)b/\sqrt{2}$ and $\mathbb{Q}\{H\} = \mathscr{A} \otimes_{\mathbb{Q}} \mathbb{Q}\{a, b\sqrt{2}\}$, which is simple. Finally, consider 5(h), for example. If $m > 1$ or $\langle x\rangle \leqslant H$,

then $H_1 = \langle i, j \rangle \curlyvee \langle x \rangle$ or $\langle x^2, h \rangle$ or $\langle x^2, xh \rangle$ lies in H. So let $m = 1$, $\langle x \rangle \trianglelefteq H$, $\alpha = 2$. We have $\bar{G} = \langle i, j \rangle \rtimes \langle x, d \rangle$; $h = (1+i)(1+x)d/2$, $dxd^{-1} = x^{-1}$. There remain two possibilities for H. If $H = \langle j, h, \rho \rangle$ then $\mathbb{Q}\{H\} = \mathscr{A} \otimes_{\mathbb{Q}} \mathbb{Q}\{(1+x)d\} \cong \mathscr{A} \otimes_{\mathbb{Q}} \mathbb{Q}(\sqrt{2})$. Next $H = \langle i, j, \rho, xh \rangle$. Here again $\mathbb{Q}\{H\} = \mathscr{A} \otimes_{\mathbb{Q}} \mathbb{Q}\{x(1+x)d\} \cong \mathscr{A} \otimes_{\mathbb{Q}} \mathbb{Q}(\sqrt{2})$. Thus $\mathbb{Q}\{H\}$ is always simple.

5. Insoluble Groups

1. We bring our group theoretic classification to a close by investigating an insoluble subgroup G of $M_2(D)$. We are unable to determine the nonabelian composition factors of G from the matrix representation. Instead, we have recourse to a heavy group theoretic result which classifies simple groups whose Sylow 2-subgroups have a structure which includes the types in 2.10(c). Actually we use the version published in [11], which classifies the quasi-simple subgroups of $M_2(D)$. Recall that a group R is called quasi-simple if R is perfect and $R/Z(R)$ is simple. The use of this group theoretic machinery should be compared to the use of the classification of fixed point free matrix groups by Zassenhaus [29] in [1]. However, in the case when D is p-adic, an alternative module theoretic method for the determination of perfect subgroups is possible. It uses the properties of the maximal order of D. Incidentally, the three perfect groups of the global case are obtainable here as well.

We begin by classifying the perfect subgroups of $M_2(D)$ and then move on to the insoluble ones.

2. We assume, until further notice, that G is perfect and $\mathbb{Q}\{G\} = M_2(D)$. The latter assumption implies by Lemma 2.2 that G is primitive. We require the following result of [11]:

THEOREM. *A quasi-simple group R is emdabble in $M_2(D)$ if and only if $R \cong SL(2, 5)$ or $SL(2, 9)$.*

We need to know $\mathbb{Q}\{R\}$. This is determined by the simple components of $\mathbb{Q}R$ which are specified by $\mathbb{Q}$-conjugacy classes of the characters of R and their local Schur indices. In [21], Janusz works out this information for all groups of the type $SL(2, q)$. The relevant data for us are:

(a) $R = SL(2, 5)$. Then $\mathbb{Q}R \cong A \oplus M_2(B) \oplus M_3(D_1) \oplus \mathbb{Q} \oplus M_3(\mathbb{Q}(\sqrt{5})) \oplus M_4(\mathbb{Q}) \oplus M_5(\mathbb{Q})$, where $A = \mathscr{A} \otimes_{\mathbb{Q}} \mathbb{Q}(\sqrt{5})$; $B = \langle \mathbb{Q}(\zeta_3), \tau, -1 \rangle$, $\tau : \zeta_3 \to \zeta_3^{-1}$. The corresponding Galois conjugacy classes of characters, in the notation of [8], are

$$(\eta_1, \eta_2); \theta_1; \chi_1; 1; (\xi_1, \xi_2); \theta_2, \psi.$$

The components on which R is represented faithfully are the first three. Hence $\mathbb{Q}\{R\} \cong A$ or $A \oplus \mathbb{Q}$ or $M_2(B)$.

(b) $R = SL(2, 9)$. There are two faithful components of $\mathbb{Q}R$ both of which are isomorphic to $M_2(B)$, B as in (a). Hence $\mathbb{Q}\{R\} \cong M_2(B)$.

3. LEMMA. *There are no (nonabelian) simple subgroups of* $M_2(D)^\times$.

Proof. Let $t \in M_2(D)$ be an involution and V be D-columns of size 2. For each $v \in V$, $v = \frac{1}{2}(1-t)v + \frac{1}{2}(1+t)v$. So $V = (1-t)V \oplus (1+t)V$. The sum is direct as the summands are t-eigenspaces with eigenvalues -1 and $+1$. So on a basis of V adapted to this decomposition, t is represented by $\left(\begin{smallmatrix} \pm 1 & 0 \\ 0 & \pm 1 \end{smallmatrix}\right)$. Now suppose $R \leqslant M_2(D)$ is nonabelian simple. By [8, p. 97] it contains a $\mathscr{C}_2 \times \mathscr{C}_2$ subgroup S. By a similarity operation, we bring one of the involutions $t \in S$ into the form $\left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$. Then $C_{M_2(D)}(t) = \left(\begin{smallmatrix} x & 0 \\ 0 & y \end{smallmatrix}\right)$; $x, y \in D$. So $S = \left\{\left(\begin{smallmatrix} \pm 1 & 0 \\ 0 & \pm 1 \end{smallmatrix}\right)\right\}$, which contains a central involution, a contradiction.

4. THEOREM. *Let* $G \leqslant M_2(D)$ *be a perfect group with* $\mathbb{Q}\{G\} = M_2(D)$. *Then* G *is one of the following three groups*:

(a) $SL(2, 5)$, $D = \langle \mathbb{Q}(\zeta_3), \tau, -1 \rangle$, $\tau : \zeta_3 \to \zeta_3^{-1}$.

(b) $SL(2, 9)$, D *as in* (a).

(c) $\mathscr{B} = E \wr_2 L$, *where* $L \cong SL(2, 5)$, $E \cong \mathscr{Q}_8 \circ \mathscr{D}_8$, $L \cap E = Z(E)$, *and* $L/Z(L)$ *acts faithfully on* E *as a group of outer automorphisms. Furthermore* $D \cong \mathscr{A}$.

Proof. Let p be an odd prime. By Lemmas 2.9 and 2.10, $O_p(G)$ is cyclic. So $O_p(G) \leqslant Z(G)$. Let P be a Sylow p-subgroup of G and $\phi : G \to P$ be the transfer map [16, Chap. IV, 1.4]. For $g \in O_p(G)$, $\phi(g) = g^{|G:P|}$. Since G is perfect, $\phi = 1$. Hence $g = 1$ and $O_p(G) = 1$. A minimal normal subgroups of G is by Lemmas 3 and 2.9 of order 2. So $E = O_2(G) \neq 1$ and is one of the 2-groups listed in Lemma 2.11. Put $C = C_G(E)$. We have $G/EC \subsetneq \operatorname{Out} E$. We see from 2.13 that, except for $E \cong \mathscr{Q}_8 \circ \mathscr{D}_8$, the group Out E is soluble. Therefore $G = EC$. This group is not perfect unless $E \leqslant C$. We conclude that $E \cong \mathscr{C}$ or $\mathscr{Q}_8 \circ \mathscr{D}_8$, which we consider separately:

(4.1) $E \cong \mathscr{C}$. It follows from above that $E = Z(G)$. Now let L/E be a minimal normal subgroup of G/E. If L/E is an elementary abelian p-group, then p is odd and $L = P \times E$, where P is the Sylow p-subgroup of L, contrary to $O_p(G) = 1$. So L/E is the direct product of isomorphic simple groups. If L/E were not simple, then it would have exactly two factors by Lemma 2.10(a). Moreover conjugation by G must permute these two factors nontrivially, a contradiction to G perfect. So L/E is simple. Let $L_1 = \mathscr{D}L$. Then $L = L_1 \circ E$ and L_1 is quasi-simple and normal in G. By the classification of these groups $L_1 \cong SL(2, 5)$ or $SL(2, 9)$. Let $H = C_G(L_1)$.

Then $G/L_1H \subsetneq \operatorname{Out} L_1 \cong \mathscr{C}_2$ or $\mathscr{C}_2 \times \mathscr{C}_2$; see 2.13(h). Hence $G = L_1H$, $O_2(H) = E$, and $L_1 \cap H = Z(L_1)$. Suppose that $H > Z(L_1)$. Then $H = Z(L_1)G_1$, where $G_1 = \mathscr{D}H > 1$ is perfect. We have $G = L_1 \circ G_1$ and $\mathbb{Q}\{G_1\} \cong D_1$ or $M_2(D_1)$ by Lemma 2.9. In the first case $G_1 = SL(2, 5)$ and put $L_2 = G_1$. For the second case, all the above argument applies to G_1 so $G_1 = L_1 \circ G_2$, where $L_2 \cong SL(2, 5)$ or $SL(2, 9)$ and $L_2 \lhd G$. Now $\mathbb{Q}\{L_1\}$ and $\mathbb{Q}\{L_2\}$ are simple and by 2.4, $\mathbb{Q}\{L_1L_2\} \cong \mathbb{Q}\{L_1\} \otimes \mathbb{Q}\{L_2\} = M_\alpha(*)$, where $\alpha = 4, 8$, or 16 depending on L_1 and L_2. Contradiction. Hence $H = Z(L_1)$ and $G = L_1$ which is (a) or (b).

(4.2) $E \cong \mathscr{Q}_8 \circ \mathscr{D}_8$. Let $C = C_G(E)$ and S be a Sylow 2-subgroup of C. If $Z(E) < S$, then $\operatorname{rank}(ES/Z(E)) > 4$, contrary to Lemma 2.10(c). So $Z(E) = S$ and $C = Z(E) \times C_1$, where C_1 is of odd order and normal in G. Since C_1 is soluble and $F(C_1) = 1$, we have $C_1 = 1$. Therefore $G/E \subsetneq \operatorname{Out} E = \operatorname{Sym}_5$. Since G/E is perfect, $G/E \cong \operatorname{Alt}_5$ and it acts faithfully on $E/Z(E)$. This is because any automorphism of E which centralises $E/Z(E)$ is inner. In fact $E/Z(E)$ is isomorphic to the 4-dimensional summand of the $\mathbb{F}_2$-permutation module for Alt_5. So it is a projective G/E module. Hence $G/Z(E)$ is split over $E/Z(E)$. Let $L/Z(E)$ be a complement. Then $L \cong SL(2, 5)$ $\operatorname{Alt}_5 \times \mathscr{C}_2$. The latter is ruled out by Lemma 3. So $L \cong SL(2, 5)$ and $G = E \rfloor_2 L \cong \mathscr{B}$ as in (c).

The assertion about D was shown in 2 for the groups (a) and (b). As to (c) we give a complete treatment of the embedding question in the theorem below.

5. THEOREM. *The group $G = E \rfloor_2 L \cong \mathscr{B}$ with the notation of Theorem* 4(c) *embeds in $M_2(D)$ if and only if $M_2(D)$ has a subalgebra (with the same identity) isomorphic to $M_2(\mathscr{A})$. When $G \leqslant M_2(D)$, we have $\mathbb{Q}\{G\} \cong M_2(\mathscr{A})$. Moreover any two faithful representations of G in $M_2(D)$ are conjugate.*

Proof. Let G be a subgroup of $M_2(D)$. One has $\mathbb{Q}E \cong M_2(\mathscr{A}) \oplus \mathbb{Q}^{16}$ as remarked in the proof of Theorem 4.7. So $\mathbb{Q}\{E\} \cong M_2(\mathscr{A})$. To prove the converse, it is sufficient to show that G embeds in $M_2(\mathscr{A})$. We show that $G/Z(G)$ is a subgroup of $SO_5(\mathbb{R})$ whose inverse image in Spin(5), the double cover of $SO_5(\mathbb{R})$, is isomorphic to G. The pull-back of this group in the isomorphism between $SU_2(\mathbb{H})$ and Spin(5) ends up in $M_2(\mathscr{A})$, thus affording the required embedding. Here $\mathbb{H}$ denotes the real quaternions. The reference for this part of the proof is [6, Chap. 10]. For the convenience of the reader, we summarise the required results below.

The basic sequences of homomorphisms are

$$M_2(\mathbb{H}) \xrightarrow[\cong]{\psi} C_4 \xrightarrow{\phi} C_5; \qquad \operatorname{Pin}(5) \xrightarrow{\rho} O(V_5),$$

where

$$\mathbb{H} = \text{Quaternions over } \mathbb{R}.$$

C_n = Clifford algebra of dimension 2^n over $\mathbb{R}$. It is generated by $e_1, ..., e_n$ with the relations $e_i^2 = -1$ and $e_i e_j = -e_j e_i$, $i \neq j$.

V_n = The $\mathbb{R}$-subspace of C_n with the basis $e_1, ..., e_n$ and the inner product $(\sum_1^n a_i e_i, \sum_1^n b_i e_i) = \sum_1^n a_i b_i$, $a_i, b_i \in \mathbb{R}$.

$\mathrm{Pin}(n)$ = The subgroup of $C_n^\times$ generated by unit length vectors of V_n.

$$\psi: \begin{pmatrix} i & 0 \\ 0 & i \end{pmatrix} \to e_1; \quad \begin{pmatrix} j & 0 \\ 0 & j \end{pmatrix} \to e_2; \quad \begin{pmatrix} k & 0 \\ 0 & -k \end{pmatrix} \to e_3; \quad \begin{pmatrix} 0 & k \\ k & 0 \end{pmatrix} \to e_4.$$

$$\phi: e_i \to e_i e_5, \qquad 1 \leqslant i \leqslant 4.$$

In the obvious grading of C_5, the map ϕ embeds C_4 onto the even graded part of C_5. Let $\alpha: C_5 \to C_5$ be the automorphism of C_5 defined by $\alpha(e_i) = -e_i$. The group $\mathrm{Pin}(5)$ acts as linear orthogonal transformations on V_5 via the map ρ defined by $\rho(x)v = \alpha(x)\, vx^{-1}$ $x \in \mathrm{Pin}(5)$, $v \in V_5$. We have $\ker \rho = \pm 1$ and $\mathrm{Im}\, \rho = O(V_5)$. In fact for a unit length vector x in V_5, $\rho(x) = R_x$, where R_x denotes the reflection of V_5 in the hyperplane orthogonal to x. Furthermore, $\rho^{-1}(SO(V_5))$ is the even graded part of $\mathrm{Pin}(5)$ which is called $\mathrm{Spin}(5)$. The combined map $\rho \circ \phi \circ \psi$ gives an epimorphism of $SU_2(\mathbb{H})$ on $SO(V_5)$ with the kernal ± 1. This completes our brief summary.

We come to the embedding of G. Let H be the symmetric group on 5 letters and X be the permutation module for H over $\mathbb{F}_2$. We regard $X \rtimes H$ as a reflection subgroup of $O(V_5)$ in the following way [3]. Put $V = V_5$. For $\sigma \in \mathrm{Sym}_5$, define $h_\sigma \in O(V)$ by $h_\sigma(e_i) = e_{\sigma(i)}$. Next for any subset I of $T = \{1, 2, ..., 5\}$, define $x_I \in O(V)$ by $x_I: e_i \to -e_i$ if $i \in I$, $e_i \to e_i$ otherwise. Then we have the relations

$$h_\sigma h_\tau = h_{\sigma\tau}, \qquad x_I x_J = x_{I \nabla J}, \qquad h_\sigma x_I h_\sigma^{-1} = x_{\sigma(I)},$$

$$\det h_\sigma = (-1)^{\mathrm{sign}(\sigma)}, \qquad \det x_I = (-1)^{|I|},$$

where σ, $\tau \in \mathrm{Sym}_5$, $I, J \subseteq T$, and $I \nabla J = I \cup J \backslash I \cap J$. Hence $H = \{h_\sigma;\ \sigma \in \mathrm{Sym}_5\} \cong \mathrm{Sym}_5$ and $X = \{x_I; I \subseteq T\}$ is the permutation module for H over $\mathbb{F}_2$. The group $X \rtimes H$ is generated by reflections since $h_{(ij)} = R_{(e_i - e_j)/\sqrt{2}}$ and $x_{\{i\}} = R_{e_i}$, where $i, j \in T$. The groups $H_1 = \{h_\sigma; \sigma \in \mathrm{Alt}_5\}$ and $X_1 = \{x_I;\ I \subseteq T,\ |I| \text{ even }\}$ are subgroups of $SO(V)$ and X_1 is isomorphic to the nontrivial summand of the permutation module for H_1. These groups pull back under ρ to the following subgroups of $\mathrm{Spin}(5)$:

$$\langle (e_1 - e_2)(e_4 - e_5)/2,\ (e_2 - e_3)(e_4 - e_5)/2,\ (e_1 - e_2)(e_3 - e_4)/2 \rangle$$

and

$$\langle e_1e_5, e_2e_5, e_3e_5, e_4e_5\rangle,$$

which pull back under ϕ to

$$L_1 = \langle (e_1-e_2)(e_4-1)/2,\ (e_2-e_3)(e_4-1)/2,\ (e_1-e_2)(e_3-e_4)/2,\ -1\rangle$$

and

$$E_1 = \langle e_1, e_2, e_3, e_4\rangle$$

in $C_4^\times$. One can verify that $E_1 \cong \mathscr{Q}_8 \,Y\, \mathscr{D}_8$ and $L_1 \cong SL(2,5)$. The latter also follows from Lemma 3 which rules out Alt_5 subgroups in $M_2(\mathbb{H})^\times$ or $C_4^\times$. Clearly the pull-back EL of E_1L_1 under ψ is in $M_2(A)$, where $A<\mathbb{H}$ are the quaternions over $\mathbb{Q}$ and $EL \cong \mathscr{B}$.

Now let $\theta, \theta' : G \to M_2(D)$ be two faithful representations of G in $M_2(D)$. Put $A = \mathbb{Q}\{\theta(E)\}$, $A' = \mathbb{Q}\{\theta'(E)\}$, and $K = Z(D)$. $A \cong A' \cong M_2(\mathscr{A})$. Hence by above there exists a faithful representation $\xi : G \to A'$. Since $\dim_{\mathbb{Q}} \mathbb{Q}\{\xi(E)\} = 16$, we have $\mathbb{Q}\{\xi(G)\} = \mathbb{Q}\{\xi(E)\} = A'$. We prove that θ and ξ are conjugate. Since in a completely analogous way we can prove that θ' and ξ are conjugate, the conjugacy of θ and θ' is established and incidentally it shows that $\mathbb{Q}\{\theta(G)\} = A$. Since $\mathbb{Q}E$ has only one faithful component and that is isomorphic to $M_2(\mathscr{A})$, the map $\eta : \theta(g) \to \xi(g)$, $g \in E$, extends to an isomorphism between A and A'. Hence $\eta \otimes 1 : A \otimes_{\mathbb{Q}} K \to A' \otimes_{\mathbb{Q}} K$ is an isomorphism over K of those simple subalgebras of $M_2(D)$. By the Noether–Skolem theorem, it is induced by conjugation with some $x \in M_2(D)$. Thus $\xi(g) = x\theta(g)\,x^{-1}$ for all $g \in E$. Now L is generated by two elements a, b of orders 3 and 5. So it is enough to show that the above equality holds for a and b. For instance consider a. The elements $\xi(a)$ and $x\theta(a)\,x^{-1}$ of $M_2(D)$ have order 3 and induce automorphisms on $\theta'(E)$ and so on A'. Since $\xi(a) \in A'$, they commute, Hence $\alpha = x\theta(a)\,x^{-1}\xi(a)^{-1}$ centralises A' and has order 1 or 3. As $\mathbb{Q}(\zeta_3)$ splits $\mathscr{A}$, we must have $\alpha = 1$. Thus $\xi(a) = x\theta(a)\,x^{-1}$. Similarly for b. The theorem is now proved.

6. There is an extension group $\mathscr{B}^*$ of $\mathscr{B}$ with index 2 formed as follows. Put $L \cong SL(2,5)$, $E = \langle a, b\rangle \,Y\, \langle c, d\rangle = \mathscr{Q}_8 \,Y\, \mathscr{D}_8$ as before. Let $L^* = L\langle h\rangle$, where h indices the automorphism ψ of conjugation by $\left(\begin{smallmatrix}0 & 1\\ 2 & 0\end{smallmatrix}\right)$ on $L \leqslant GL(2,5)$ and $h^2 = \left(\begin{smallmatrix}1 & 0\\ 0 & 1\end{smallmatrix}\right)$, that is, an outer automorphism of L and $L/Z(L)$. Hence $L^*/Z(L^*) \cong \mathrm{Sym}_5$, where this isomorphism can be so chosen that h is mapped onto (12). Consider Sym_5 as a group of automorphisms of E in the way decribed in 2.13(c) and put $\mathscr{B}^* = E \downarrow_2 L^*$. Thus $h : a \to b,\ b \to a,\ c \to c,\ d \to c^2d$. Note that the different choices for the isomorphisms $L/Z(L) \cong \mathrm{Alt}_5$ and $L^*/Z(L^*) = \mathrm{Sym}_5$ give rise to isomorphic groups, for any automorphism of Alt_5 or Sym_5 lifts to one of L or L^*.

7. LEMMA. *The group $G^* = E\downarrow_2 L^* \cong \mathscr{B}^*$ as above embeds in an algebra $B \cong M_2(D)$, with $K = Z(B)$ a number field, if and only if $B \cong M_2(\mathscr{A}) \otimes_{\mathbb{Q}} D'$ and $\sqrt{2} \in K$. Thus D' is a division algebra over K of odd index. The enveloping algebra of the image of G^* is $M_2(\mathscr{A}) \otimes_{\mathbb{Q}} \mathbb{Q}(\sqrt{2})$ and there are exactly two nonconjugate embeddings of G^* in B.*

Proof. Suppose first that $G^* \leqslant B$. As we have seen $\mathbb{Q}\{a, b\} \cong \mathscr{A}$, $A = \mathbb{Q}\{E\} \cong M_2(\mathscr{A})$. Put $\mu = (a+b)c$. Then $h\mu = \mu h$, $\mu^2 = 2$, $\bar{h} = h\mu^{-1}$ centralises E and $\bar{h}^2 = \frac{1}{2}$. By 1.3, $B = A \otimes_{\mathbb{Q}} D'$, where $D' = C_B(A)$. Since $\bar{h} \in D'$ is central over K of odd index by the Lemma in 1.3, $\bar{h}$ belongs to K. Conversely, we prove that G^* embeds in $M_2(\mathscr{A}) \otimes_{\mathbb{Q}} \mathbb{Q}(\sqrt{2})$. Construct $G = EL \cong \mathscr{B}$ in $M_2(\mathscr{A})$ and put $\eta = \pm(a+b)c/\sqrt{2}$. Then $\eta^2 = 1$; ${}^\eta a = b$, ${}^\eta b = a$, ${}^\eta c = c$, ${}^\eta d = c^2 d$. We show that η induces the automorphism ψ on L as above. We know that L is generated by two elements x, y of orders 3, 5. It follows from the construction of the abstract group $\mathscr{B}^*$ that $\psi(x)$ and $x_1 = \eta x \eta^{-1}$ induce identical automorphisms on E and $\mathbb{Q}\{E\}$. Since $\psi(x) \in \mathbb{Q}\{E\}$, they commute. Thus $\psi(x)\, x_1^{-1}$ centralises $\mathbb{Q}\{E\}$ and has order 1 or 3. This forces $x_1 = \psi(x)$. Similarly for y. Thus $\langle G, \eta \rangle \cong \mathscr{B}^*$. Finally, consider two embeddings $\sigma_1, \sigma_2 : G^* \to B$. By Theorem 5, we can take $\sigma_1(g) = \sigma_2(g)$ for all $g \in EL$. We know now that $\sigma_i(h) = \pm(\sigma_i(a) + \sigma_i(b))\sigma_i(c)/\sqrt{2}$. If $\sigma_2(g) = x\sigma_1(g)\, x^{-1}$ for all $g \in G^*$, then $x \in D'$ and so $\sigma_2(h) = \sigma_1(h)$. Thus σ_1 and σ_2 are conjugate according as $\sigma_1(h)$ is $\sigma_2(h)$ or $-\sigma_2(h)$.

8. THEOREM. *Let G be a finite primitive insoluble subgroup of $M_2(D)$. Then G belongs to one of the following nine classes in which $a = \left(\begin{smallmatrix} 2 & 0 \\ 0 & -2 \end{smallmatrix}\right) \in SL(2, 5)$ and d induces conjugation by $\left(\begin{smallmatrix} 1 & 0 \\ 0 & -2 \end{smallmatrix}\right)$ on $SL(2, 5) < GL(2, 5)$.*

(a) $SL(2, 5)\, \mathrm{Y}_2\, \mathscr{D}_{2^{\alpha+1}m}$; *$m = 1$, $\alpha \geqslant 3$ or $m > 1$ odd, $\alpha \geqslant 1$.*

(b) $SL(2, 5)\, \mathrm{Y}_2\, G_{m,r}$; *$2 \mid s$.*

(c) $SL(2, 5)\langle d \rangle \times G_{m,r}$; *$mn$ odd, $5 \nmid m$; $d^2 = \pm a$.*

(d) $(SL(2, 5)\, \mathrm{Y}_2\, \langle d_1 \rangle)\langle d \rangle \times G_{m,r}$;

$d_1^{2^\alpha} = 1$, $\alpha \geqslant 2$, $d^2 = a d_1^{1+2^{\alpha-2}}$, $dd_1 = d_1 d$; mn odd, $5 \nmid m$.

(e) $(SL(2, 5)\, \mathrm{Y}_2\, \langle g, h_1 \rangle)\langle d \rangle$;

$g^m = 1$, $h_1^{n/2} = g^t$, $h_1 g h_1^{-1} = g^{r^2}$; $d : g \to g^r$, $h_1 \to h_1$; $st = m$, $s = (r-1, m)$, $n = \gamma(r, m)$, t odd, $(ns, t) = 1$, $4 \mid s$, $5 \mid t$, $r \equiv \pm 2(5)$ so $4 \mid n$; $d^2 = a h_1^{1+ns/8}$.

(f) $SL(2, 9) \times G_{m,r}$; *mn odd.*

(g) $SL(2, 9)\langle h \rangle$; *$h$ induces the field automorphism on $SL(2, 9)$ and $h^2 = \pm 1$.*

(h) $\mathscr{B} \times G_{m,r}$; *$mn$ odd.*

(i) $\mathscr{B}^*$.

Proof. Let $L = \bigcap_n \mathscr{D}^n G$ be the perfect radical of G. By Lemma 2.9, $\mathbb{Q}\{L\} \cong D_1$ or $M_2(D_1)$. So by [1] or Theorem 4, $L \cong SL(2, 5)$, $SL(2, 9)$, or $\mathscr{B}$. Put $R = C_G(L)$. So $G/LR \to \operatorname{Out} L$. We consider the above cases separately.

(A) $L \cong SL(2, 5)$.

The outer automorphism group of L is of order 2, generated by χ which is conjugation with $\left(\begin{smallmatrix} 1 & 0 \\ 0 & -2 \end{smallmatrix}\right)$ in the embedding of $SL(2, 5)$ in $GL(2, 5)$. Since the faithful components of $\mathbb{Q}L$ are nonisomorphic, χ fixes them. So χ acts on $\mathbb{Q}\{L\}$. We have two choices for $\mathbb{Q}\{L\}$:

Case 1. $\mathbb{Q}\{L\} \cong \langle \mathbb{Q}(i), j, -1 \rangle \otimes_{\mathbb{Q}} \mathbb{Q}(\sqrt{5}) = A \cong \langle \mathbb{Q}(\zeta_5), \tau, -1 \rangle$. Note that A is split by a complex field. The representation of L in A given in [1, p. 377] contains a misprint. A correct one is

$$a = \begin{pmatrix} 2 & 0 \\ 0 & -2 \end{pmatrix} \to [(\alpha+1)i + \alpha j + ij]/2$$

$$b = \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix} \to (-1 + i + j + ij)/2$$

$$c = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \to [\alpha + i - (\alpha+1)\, ij]/2 \qquad (= \zeta_5),$$

where $\alpha = (-1+\sqrt{5})/2$, $\alpha^2 + \alpha - 1 = 0$. Lemma 2.11 applies to $O_2(R)$ and $O_{2'}(F(R))$ since they are both normal in G. The group R is classified under Lemma 4.3 as the essential fact there is that $\mathbb{Q}\{T\} \cong \mathscr{A}$ whose role is taken by A here. Since A is split by a complex field, in the case 4.3(b) we must have $R = Z(L) \times \mathscr{D}_{2m}$ which is $\mathscr{D}_{4m}$ and the case 4.3(d) is ruled out. Summarising, R is either a $G_{m,r}$ group or $\mathscr{D}_{2^{\alpha+1}m}$ with $\alpha \geqslant 1$, $m \geqslant 1$ (excluding $\mathscr{D}_4 = \mathscr{C}_2 \times \mathscr{C}_2$). Now we turn to G. Either $G = L \curlyvee R$, giving (a) or (b) ($L \curlyvee \mathscr{D}_8$ is not allowed because it is imprimitive) or $|G : LR| = 2$, which we now consider. Let $d \in G \backslash LR$ have the same action on L as $\left(\begin{smallmatrix} 1 & 0 \\ 0 & -2 \end{smallmatrix}\right)$ so that $d^2 = ay$, $y \in R$. We are free to change d by elements of R. The centre of A is generated by $c + c^{-1}$ and $dcd^{-1} = c^{-2}$. So d induces a nontrivial automorphism on $Z(A)$. Let $\tau: A \to A$ centralise $\langle \mathbb{Q}(i), j, -1 \rangle$ and act on $\mathbb{Q}(\sqrt{5})$, $\tau: \sqrt{5} \to -\sqrt{5}$. Then $\tau \circ (S_d)$ centralises $Z(A)$, where S_d denotes conjugation by d on A. By the Noether–Skolem theorem $\tau(dxd^{-1}) = \sigma x \sigma^{-1}$, $x \in A$ for some $\sigma \in A$. A calculation shows $\sigma = [1 - i + j - (2\alpha+3)\, ij]/2$. So $dxd^{-1} = \tau(\sigma)\, \tau(x)\, \tau(\sigma)^{-1}$. Let $\bar{d} = \tau(\sigma)^{-1} d$. Then

$$\bar{d} x \bar{d}^{-1} = \tau(x), \qquad d\tau(\sigma)\, d^{-1} = \tau(\sigma)\, \sigma \tau(\sigma)^{-1},$$

$$\bar{d}^2 = \tau(\sigma)^{-1} (d\tau(\sigma)\, d^{-1})\, d^2 = (\tau(\sigma)\sigma)^{-1} d^2.$$

Now $\tau(\sigma)\sigma = -2a$. So $\bar{d}^2 = -y/2$. Next we show that R is of $G_{m,r}$ type. For suppose not, then $R = \langle g, h\rangle \cong \mathscr{D}_{2^{\alpha+1}m}$ $\alpha \geqslant 1$, $g^{2^\alpha m} = 1$, $h^2 = 1$, $hgh^{-1} = g^{-1}$. We have by Lemmas 2.4(a) and 2.6 that

$$\mathbb{Q}\{G\} = \mathbb{Q}\{L, g, h, \bar{d}\} = \mathscr{A} \otimes_{\mathbb{Q}} B,$$

where $B = \mathbb{Q}\{g, \sqrt{5}, h, \bar{d}\}$, $\mathbb{Q}\{g, \sqrt{5}\} = \mathbb{Q}(\zeta_{2^\alpha m}, \sqrt{5})$, $h: \sqrt{5} \to \sqrt{5}$, $\bar{d}: \sqrt{5} \to -\sqrt{5}$. If $y \in \langle g\rangle$ then by Lemma 2.3, B factorises and has exponent $\leqslant 2$. If $y \notin \langle g\rangle$, then $\bar{d}^4 = \frac{1}{4}$ and $B = \langle \mathbb{Q}(\zeta_{2^\alpha m}, \sqrt{5}), \bar{d}, \frac{1}{4}\rangle$, which clearly has exponent $\leqslant 2$. Hence so does $\mathbb{Q}\{G\}$ in either case, a contradiction. This proves the claim above. Now we distinguishes two cases

(i) $|O_2(R)| = 2$. Then a Sylow 2-subgroup of R has order at most 4, otherwise $\mathbb{Q}\{R\} = M_2(D_1)$ with $2 \mid \text{index } D_1$, which makes $D_1 \otimes \mathscr{A}$ split partially, a contradiction. In fact $2 \| |R|$. Suppose not and take d in a Sylow 2-subgroup S of G containing $\langle a\rangle$. Put $R \cap S = \langle c\rangle$ which is of order 4. Clearly $y \in \langle c\rangle$. Put $O_{2'}(F(R)) = \langle g\rangle$ of order $m > 1$. If $y = 1$ or c^2, then $\bar{d}^2 = -\frac{1}{2}$ or $\frac{1}{2}$. Therefore $B = \mathbb{Q}\{L, g, c, d\} = \mathscr{A} \otimes_{\mathbb{Q}} \mathbb{Q}\{g, \sqrt{5}, c, \bar{d}\}$. The latter algebra is a crossed product of $\mathbb{Q}(\zeta_m, \sqrt{5})$ with a $\mathscr{C}_2 \times \mathscr{C}_2$ group to which Lemma 2.3 applies. So the exponent of B is $\leqslant 2$, a contradiction. Next if $y = c$ or c^{-1}, then $\bar{d}^2 = -c/2$ or $-c^{-1}/2$ and $\bar{d}^4 = -\frac{1}{4}$. Therefore $B = \mathscr{A} \otimes_{\mathbb{Q}} \langle \mathbb{Q}(\zeta_m, \sqrt{5}), \bar{d}, -\frac{1}{4}\rangle$ again has exponent $\leqslant 2$. Contradiction. Hence $2 \| |R|$ and $R = Z(L) \times R_1$, where R_1 is of odd order and has cyclic Sylow subgroups. Proceeding as in the proof of Theorem 3.8, let $R_1 = \mathscr{D}R_1 \rtimes H$, $(|H|, |\mathscr{D}R_1|) = 1$. Since $G = N_G(H)\, R_1$, we can choose d to lie in a Sylow 2-subgroup of $N_G(H)$. Then $d^2 = \pm a$. Also $H = H_1 \times H_2$, where $H_1 = [d, H]$, $H_2 = C_H(d)$. Since $\mathrm{Aut}(\mathscr{D}R_1)$ is abelian, H_1 centralises $\mathscr{D}R_1$. We can choose g, $h \in R_1$ such that $\langle g\rangle = \mathscr{D}R_1 \times H_1 \times C_{H_2}(\mathscr{D}R_1)$, $\langle h\rangle = H_2$. Then $R_1 = \langle g, h\rangle$ and $g^m = 1$, $h^n = g^t$, $hgh^{-1} = g^r$; $st = m$, mn odd; $d: g \to g^{r'}$, $h \to h$; $r'^2 \equiv 1(m)$, $s = (r-1, r'-1, m)$. If $5 \mid m$, then $\sqrt{5} \in Z(\mathbb{Q}\{R_1\})$ is centralised by $\bar{d}$ so that $Z(\mathbb{Q}\{R_1\})\, Z(\mathbb{Q}\{L\})$ is not a field, a contradiction to the remark after Lemma 2.9. Hence $5 \nmid m$. We show that $r' \equiv 1(m)$. Suppose not, i.e., $m \neq 1$, $r \not\equiv 1(m)$. Then

$$\mathbb{Q}\{L, g, d\} = \mathbb{Q}\{L, g, \bar{d}\} = (\mathscr{A} \otimes_{\mathbb{Q}} K) \otimes_K B,$$

where $F = \mathbb{Q}(\zeta_m, \sqrt{5})$, K is the fixed field of $\bar{d}$ in F, and $B = \langle F/K, \bar{d}, \pm\frac{1}{2}\rangle$. Since $F = K(\sqrt{5})$, we have $B = K \otimes_{\mathbb{Q}} B'$ where $B' = \langle \mathbb{Q}(\sqrt{5}), \bar{d}, \pm\frac{1}{2}\rangle$. So $A = K \otimes_{\mathbb{Q}} (\mathscr{A} \times_{\mathbb{Q}} B')$. Now B' has invariant of $\frac{1}{2}$ exactly at 2 and 5. Hence $\mathscr{A} \otimes_{\mathbb{Q}} B'$ has invariant of $\frac{1}{2}$ at ∞ and 5. Since $s \neq 1$ and $\zeta_s \in K$, K is a complex field. Since $r' \not\equiv 1(m)$, we have $I_5(F/\mathbb{Q}) \cap \langle \bar{d}\rangle = 1$, so $e(F_5/K_5) = 1$, $e(K_5/\mathbb{Q}_5) = 2$. Therefore K splits $\mathscr{A} \otimes_{\mathbb{Q}} B'$, a contradiction. This shows that $G = L\langle d\rangle \times R_1$ as in (c).

(ii) $O_2(R) = \mathscr{C}_{2^\alpha}$, $\alpha \geqslant 2$. Let $\eta \in O_2(R)$ be of order 4 and this time take

$\bar{d}=\tau(\sigma)^{-1}d(1-\eta)$. Then $\bar{d}^2=-\frac{1}{2}y\times(-2\eta$ or $2)$ according as $d:\eta\to\eta$ or $\eta\to\eta^{-1}$. So $\bar{d}^2=y\eta$ or $-y$. $\bar{d}\notin R$ since $\bar{d}$ acts on $Z(\mathbb{Q}\{L\})$. Put $\bar{R}=\langle R,\bar{d}\rangle$, which is a finite group. $O_2(\bar{R})$ contains $O_2(R)$ as a subgroup of index 1 or 2 and $O_{2'}(F(\bar{R}))=O_{2'}(F(R))$. Hence we can apply Lemma 4.3 to $\bar{R}$ as $\bar{R}$ commutes with $\mathbb{Q}\{i,j\}$. In cases 4.3(d) or 4.3(e) write $\bar{R}=\langle g,h\rangle$, $g^{2^\alpha m}=1$, $d^2=1$, $\alpha\geqslant 2$. Then $R=\langle g\rangle$ and as d, $\bar{d}$ can be modified by elements of R, we can put $\bar{d}=h$. So $h:\sqrt{5}\to-\sqrt{5}$ and $\mathbb{Q}\{G\}=\mathscr{A}\otimes_K\mathbb{Q}\{g,\sqrt{5},h\}=M_2(\mathscr{A}\otimes_{\mathbb{Q}}K)$, where K is the fixed field of h in $\mathbb{Q}(\zeta_{2^\alpha m},\sqrt{5})$ ($5\nmid m$ for $\mathbb{Q}\{g\}\,Z(\mathbb{Q}\{L\})$ must be simple). But $\sqrt{-5}\in K$ splits $\mathscr{A}$, a contradiction. For 4.3(c), we get a similar contradiction. Hence 4.3(a) holds and $\bar{R}$ has cyclic Sylow subgroups. To begin with, suppose that $O_2(\bar{R})$ is the Sylow 2-subgroup of $\bar{R}$. Then we can write $\bar{G}=\langle\bar{d}\rangle\times G_{m,r}$, where mn is odd and $\bar{d}^{2^{\alpha+1}}=1$. We have $R=\langle d_1\rangle\times G_{m,r}$, where $d_1=\bar{d}^2$ and $y=d_1\eta^{-1}=d_1^{1+2^{\alpha-2}}$ (where $\eta=d_1^{-2^{\alpha-2}}$). $5\nmid m$ otherwise $5\mid s$ and $Z(\mathbb{Q}\{L\})\,Z(\mathbb{Q}\{G_{m,r}\})$ would not be a field. This gives (d). Clearly

$$\mathbb{Q}\{G\}=\mathscr{A}\otimes_{\mathbb{Q}}\langle\mathbb{Q}(\zeta_{2^\alpha},\sqrt{5}),\bar{d},\zeta_{2^\alpha}\rangle\otimes_{\mathbb{Q}}\mathbb{Q}\{G_{m,r}\}.$$

Finally, suppose that $O_2(\bar{R})$ is smaller than the Sylow 2-subgroup of $\bar{R}$. Write $\bar{R}=\langle g,h\rangle\cong G_{m,r}$, $2\mid n$. Then $R=\langle g,h_1\rangle$, $h_1=h^2$, $\bar{d}=h$, $y=h_1\eta^{-1}$, $2^\alpha\| s$. We have $5\nmid s$ and if $5\mid t$ then $r\equiv\pm 2(5)$, so as to make $Z(\mathbb{Q}\{L\})$ $Z(\mathbb{Q}\{R\})$ a field. Suppose that $5\nmid t$. We will get a contradiction. We have

$$\mathbb{Q}\{G\}=\mathbb{Q}\{L,g,h\}=(\mathscr{A}\otimes_{\mathbb{Q}}K')\otimes_{K'}A',$$

where $A'=\langle\mathbb{Q}(\zeta_m,\sqrt{5}),h,\zeta_s\rangle$, $K'=Z(A')$, and $h:\zeta_m\to\zeta_m^r$, $\sqrt{5}\to-\sqrt{5}$. Since $2^\alpha\in K'$, the algebra $\mathscr{A}$ is split by K'. So in order that $\mathbb{Q}\{G\}$ be of size 2, it is required that A' be a division algebra. Let K be the fixed field of h in $\mathbb{Q}(\zeta_m)$ and $K(\sqrt{\xi})$, $\xi\in K$, be the unique quadratic subextension of it. It is easy to show that $K'=K(\sqrt{5\xi})$ and $A'=A\otimes_K K'$, where

$$A=\langle\mathbb{Q}(\zeta_m),h,\zeta_s\rangle\cong A_{m,r}\qquad\text{in the notation of [1].}$$

Hence we require that A be a division algebra and not be split by K'. The necessary and sufficient conditions for A to be a division algebra are obtained in [1]. As $s>2$, K is complex. One of the conditions in [1] is that for a uniquely determined $p\mid t$, $K_p(\sqrt{\xi})/K_p$ is ramified (and ζ_s does not belong to the norm group of this extension). In fact this ensures that the 2-part of the local exponent of A at p is 2^β, where $2^\beta\| n$. At other primes that is less than 2^β. Now if $\sqrt{5}\notin K_p(\sqrt{\xi})$, then $|K_p':K_p|=2$. Otherwise $\sqrt{5}\in K_p$ since $\mathbb{Q}_p(\sqrt{5})/\mathbb{Q}_p$ is unramified. Then $K_p'=K_p(\sqrt{\xi})$. Hence $|K_p':K_p|=2$ always, so that the 2-part of the exponent of A' is less than

$2^{\beta-1}$, a contradiction. We have shows $5 \mid t$ and we have the group (d) on putting $\eta = h_1^{-ns/8}$. One sees fairly easily that

$$\mathbb{Q}\{G\} = \mathbb{Q}\{L, g, h\} \cong (\mathscr{A} \otimes_{\mathbb{Q}} K) \otimes_K A_{m,r},$$

where $K = Z(A_{m,r})$.

Case 2. $\mathbb{Q}\{L\} = M_2(B)$, $B = \langle \mathbb{Q}(\zeta), \tau, -1 \rangle$, $\zeta = \zeta_3$, $\tau: \zeta \to \zeta^{-1}$. The representation of L in $M_2(B)$ is uniquely determined, up to similarity. Specifically,

$$\begin{aligned} a &= \begin{pmatrix} 2 & 0 \\ 0 & -2 \end{pmatrix} \to 1/3[1 + 2\zeta + (1 + 2\zeta)\tau] \begin{pmatrix} -1 & \frac{1}{2} \\ 1 & 1 \end{pmatrix} \\ b &= \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix} \to \begin{pmatrix} 1 & 0 \\ 0 & \zeta \end{pmatrix} \qquad (*) \\ c_1 &= \begin{pmatrix} 0 & 2 \\ 2 & 0 \end{pmatrix} \to \begin{pmatrix} \tau & 0 \\ 0 & \tau \end{pmatrix} \end{aligned}$$

is one representation. This is worked out in the following way. The complex character corresponding to this representation is θ_1 as in 2(a). We have $\theta_1(b) = 1$, $\theta_1(c_1) = 0$. In fact θ_1 is the reduced trace of our sought representation. We denote the reduced trace of both B and $M_2(B)$ by tr. So $\mathrm{tr}(\zeta) = -1$, $\mathrm{tr}(\tau) = 0$. Now $b^3 = 1$, $c_1^2 = -1$, and $c_1 b c_1^{-1} = b^{-1}$ so $\langle b, c_1 \rangle \cong \mathscr{D}_{12}$ (normaliser of a Sylow 3-subgroup). If $\mathbb{Q}\{b\}$ were a field, $\mathbb{Q}\{b\} \cong \mathbb{Q}(\zeta)$, then by the Noether–Skolem theorem we can take the matrix for b to be $\left(\begin{smallmatrix} \zeta & 0 \\ 0 & \zeta \end{smallmatrix}\right)$, but then $\theta_1(b) = 2\,\mathrm{tr}(\zeta) = -2$, a contradiction. So $\mathbb{Q}\{b\} \cong \mathbb{Q} \oplus \mathbb{Q}(\zeta)$. So, as proved in Lemma 2.7, we can represent b by $\left(\begin{smallmatrix} 1 & 0 \\ 0 & \zeta \end{smallmatrix}\right)$. This forces $c \to \left(\begin{smallmatrix} \alpha & 0 \\ 0 & \beta \end{smallmatrix}\right)$ and $\alpha^2 = \beta^2 = -1$ as $-1 \in L$ is represented by $\left(\begin{smallmatrix} -1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$. Since $\mathbb{Q}(\alpha) \cong \mathbb{Q}(\tau)$ and $\mathbb{Q}(\zeta, \beta) \cong \mathbb{Q}(\zeta, \tau)$, by the Noether–Skolem theorem there exist $x, y \in B$ such that $x\alpha x^{-1} = \tau$ and $y\zeta y^{-1} = \zeta$, $y\beta y^1 = \tau$. Thus conjugating by $\left(\begin{smallmatrix} x & 0 \\ 0 & y \end{smallmatrix}\right)$, we get the form in $(*)$ for b and c_1. It remains to determine the matrix for a. We put undetermined coefficients for this matrix and use the value of reduced trace on elements of L, represented as words on a, b, and c_1, to get the maximum number of equations on them. Finally, a judicial use of relations between a, b, and c_1 determines these coefficients. We remark that the choice of matrices for b and c_1 does not fix that for a as $C_{M_2(B)}(\mathbb{Q}\{b, c_1\}) = \left(\begin{smallmatrix} \mathbb{Q}(\tau) & 0 \\ 0 & \mathbb{Q} \end{smallmatrix}\right)$, we have merely given one particularly simple one which we adopt for what follows.

To determine R, we note that $\mathbb{Q}(i)$ splits B. Hence $2 \| |R|$ and $R = Z(L) \times R_1$, where $R_1 = G_{m,r}$ is of odd order. We have either $G = LR$ as in (f) or there exists $d \in G \backslash LR$ inducing the automorphism of conjugation by $\left(\begin{smallmatrix} 1 & 0 \\ 0 & -2 \end{smallmatrix}\right)$ on L. We consider the latter case. We have an action of d on

$\mathbb{Q}\{L\}$. So by the Noether–Skolem theorem $dxd^{-1} = \sigma x \sigma^{-1}$ for some $\sigma \in M_2(B)$ and all $x \in M_2(B)$. After some arduous calculations one gets

$$\sigma = \begin{pmatrix} [-1+(1+2\zeta)\tau]/2 & [-\zeta+(\zeta-1)\tau]/2 \\ -\zeta+(2+\zeta)\tau & 1+\zeta \end{pmatrix},$$

which is determined up to a $\mathbb{Q}$-multiple. Furthermore

$$\sigma^2 = 3a, \qquad d\sigma = \sigma d.$$

Choose d in a Sylow 2-subgroup of G containing a. Then $d^2 = \pm a$. Now $\bar{d} = \sigma^{-1}d$ centralises L and $\bar{d}^2 = (1/3a)(\pm a) = \pm\frac{1}{3}$. Since $\mathbb{Q}(\sqrt{-3})$ splits B, we must have $d^2 = a$ and $\mathbb{Q}\{L, d\} = M_2(B \otimes_{\mathbb{Q}} \mathbb{Q}(\sqrt{3}))$, which has nonzero invariants only at the real places of $\mathbb{Q}(\sqrt{3})$. Now suppose $F(R_1) = \langle g \rangle$ has order $m \neq 1$. If d acts nontriviality on g, then $\mathbb{Q}\{L, g, d\} = M_2(B) \otimes_{\mathbb{Q}} \langle \mathbb{Q}(\zeta_m), \bar{d}, \frac{1}{3} \rangle$ which has exponent $\leqslant 2$, a contradiction. However, if d centralises $\langle g \rangle$ then $\mathbb{Q}\{g\} \cong \mathbb{Q}(\zeta_m)$ is a complex field which splits $B \otimes_{\mathbb{Q}} \mathbb{Q}(\sqrt{3})$, a contradiction again. Hence $F(R_1) = 1$, $R_1 = 1$, and G belongs to the (c) type.

(B) $L \cong SL(2, 9)$.

The outer automorphism group of L is $\mathscr{C}_2 \times \mathscr{C}_2$ generated by $\chi =$ Extension of the field automorphism of $\mathbb{F}_9$ to L, $\xi =$ conjugation by $\left(\begin{smallmatrix} 1 & 0 \\ 0 & v \end{smallmatrix}\right)$; we take v to be a generator of $\mathbb{F}_9^{\times}$ satisfying $v^2 = 2v + 1$. We have

$$\chi^2 = 1, \qquad \xi^2 = S_{\left(\begin{smallmatrix} v^{-1} & 0 \\ 0 & v \end{smallmatrix}\right)}, \qquad \chi\xi\chi^{-1} = S_{\left(\begin{smallmatrix} v^{-1} & 0 \\ 0 & v \end{smallmatrix}\right)} \circ \xi,$$

where S_g denotes conjugation of L by g. Recalling the structure of $\mathbb{Q}L$ in 5.2(b), there are only two faithful components of $\mathbb{Q}L$ of size 2 with the complex η_1, η_2. These characters are obtainable as the reduced trace of the 2×2 representations. Choose representatives for the conjugacy classes of L as in [8, Sect. 38]:

$$1,\ z = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix},\ c = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix},\ d = \begin{pmatrix} 1 & 0 \\ v & 1 \end{pmatrix},\ zc, zd, a = \begin{pmatrix} v & 0 \\ 0 & v^{-1} \end{pmatrix},$$

$$a^2, a^3, b \text{ of order } 10, b^2, b^3, b^4.$$

The relevant portion of the character table of L for us is

order	1	2	3	3	6	6	8	4	8	10	5	10	5
g	1	z	c	d	zc	zd	a	a^2	a^3	b	b^2	b^3	b^4
η_1	4	−4	1	−2	−1	2	0	0	0	1	−1	1	−1
η_2	4	−4	−2	1	2	−1	0	0	0	1	−1	1	−1

Let $e_1, e_2 \in \mathbb{Q}L$ be the central primitive idempotents which give rise to η_1, η_2:

$$e_i = \frac{\eta_i(1)}{|L|} \sum_{g \in L} \overline{\eta_i(g)}\, g \qquad (*)$$

χ and ξ act on $\mathbb{Q}L$ and permute its central idempotents. It follows from $(*)$ and the character table that $\chi(e_i) = e_i$; $\xi(e_1) = e_2$, $\xi(e_2) = e_1$. Now

$$\mathbb{Q}\{L\} \cong M_2(B); \qquad B = \langle \mathbb{Q}(\zeta), \tau, -1 \rangle, \qquad \zeta = \zeta_3,\ \tau : \zeta \to \zeta^{-1}.$$

This is valid for both the embeddings of L. Since $\mathbb{Q}(i)$ splits B, $2 \| |R|$ and $R = Z(L) \times R_1$, where $R_1 \cong G_{m,r}$ has odd order. Either $G = LR = L \times R_1$ as in (f) or $G > LR_1$. So suppose the latter holds and pick any $h \in G \backslash LR_1$. Suppose that under the map $\mathbb{Q}L \to \mathbb{Q}\{L\}$, e_1 goes to 1 and e_2 to 0. If conjugation by h permutes e_1 and e_2 in $\mathbb{Q}L$, then working in $\mathbb{Q}\{G\}$, $1 = h^{-1}e_1 h = e_2 = 0$, a contradiction. So h fixes e_1 and e_2. Therefore h induces the automorphism χ on L. The same holds when $e_1 \to 0$ and $e_2 \to 1$. Therefore $|G : LR_1| = 2$. The action of h on L extends to an action on $\mathbb{Q}\{L\}$. By the Noether–Skolem theorem, $hxh^{-1} = \sigma x \sigma^{-1}$ for all $x \in \mathbb{Q}\{L\}$ and some $\sigma \in \mathbb{Q}\{L\}$. To determine σ, we have to find a representation of L. Now $\langle c, d \rangle$ is a Sylow 3-subgroup of L and $M = N_L(\langle c, d \rangle) = \langle c, d, a \rangle \cong (\mathscr{C}_3 \times \mathscr{C}_3) \rtimes C_8$. By Lemma 2.9, M is represented imprimitively. We work out this representation of M from Lemma 2.2. So let H, N be as in that lemma. Clearly $H = \langle c, d, a^2 \rangle$. We have

$$a^{-1}ca = cd^2,\ a^{-1}da = c^2d^2;\ a^2 : c \to c^2,\ d \to d^2;\ a^4 = z.$$

It is easily established that $N \leqslant \langle c, d \rangle$ and $|N| = 3$. There are four choices for N, but the resulting representations of M are equivalent in pairs (i.e., conjugate in $M_2(*)$). This can be seen from their reduced traces. We get

$$(1)\quad N = \langle c \rangle;\quad c \to \begin{pmatrix} 1 & 0 \\ 0 & \zeta^2 \end{pmatrix},\quad d \to \begin{pmatrix} \zeta & 0 \\ 0 & \zeta^2 \end{pmatrix},\quad a \to \begin{pmatrix} 0 & \tau \\ 1 & 0 \end{pmatrix},$$

$$(2)\quad N = \langle d \rangle;\quad c \to \begin{pmatrix} \zeta & 0 \\ 0 & \zeta \end{pmatrix},\quad d \to \begin{pmatrix} 1 & 0 \\ 0 & \zeta^2 \end{pmatrix},\quad a \to \begin{pmatrix} 0 & \tau \\ 1 & 0 \end{pmatrix}.$$

One has the convenient fact that $\mathbb{Q}\{M\} = \mathbb{Q}\{L\}$, the reduced traces are $\mathrm{tr}(\zeta) = \mathrm{tr}(\zeta^2) = -1$, $\mathrm{tr}(\tau) = 0$.

(1) $\mathrm{tr}(c) = 1$, $\mathrm{tr}(d) = -2$, $\mathrm{tr}(a) = 0$. So the character is η_1, $e_1 = 1$, and $e_2 = 0$.

(2) $\mathrm{tr}(c) = -2$, $\mathrm{tr}(d) = 1$, $\mathrm{tr}(a) = 0$. So the character is η_2, $e_1 = 0$, and $e_2 = 1$.

These two representations of M extend to the whole of L. The action of h is $h: c \to c$, $d \to c^2 d^2$, $a \to a^3$. Thus we can now calculate σ. The result is

$$(1) \quad \sigma = \begin{pmatrix} (1+2\zeta)\tau & 0 \\ 0 & 1+2\zeta \end{pmatrix} \quad \sigma^2 = -3,$$

$$(2) \quad \sigma = \begin{pmatrix} 0 & -(1+2\zeta) \\ 1+2\zeta & 0 \end{pmatrix} \quad \sigma^2 = 3.$$

Of course $h\sigma = \sigma h$. Choose h in a Sylow 2-subgroup of G. Then $h^2 = 1$ or z. So $\bar{h} = \sigma^{-1}h$ centralises L and $\bar{h}^2 = \pm 1/3$. Since $\mathbb{Q}(\sqrt{-3})$ splits B, we must have $\bar{h}^2 = \frac{1}{3}$, i.e., in (1), $h^2 = z$ and in (2), $h^2 = 1$. Here $\mathbb{Q}\{L, h\} = M_2(B \otimes_{\mathbb{Q}} \mathbb{Q}(\sqrt{3}))$, which has a nonzero invariant at the real places of $\mathbb{Q}(\sqrt{3})$ only. Now it is shown exactly as in Case 2 above that $R_1 = 1$. Thus $G = \langle L, h \rangle$, $h^2 = z$ or 1 according as 1 or 2 is valid. We have got the type (g).

(C) $L = EM \cong \mathscr{B}$; $E \cong \mathscr{Q}_8 \curlyvee \mathscr{D}_8$, $M \cong SL(2, 5)$.

First we prove that Out $(\mathscr{B})$ is of order 2. Clearly in the embedding $\mathscr{B} < \mathscr{B}^*$, conjugation by h on $\mathscr{B}$ (cf. Section 6) induces an outer automorphism χ on $\mathscr{B}$. Now suppose that $\sigma \in \mathrm{Aut}(L)$. Then σ induces an automorphism on $E = O_2(L)$. So $\sigma' = (\sigma \text{ or } \chi^{-1}\sigma)$ will induce an automorphism on E which in $\mathrm{Out}(E) = \mathrm{Sym}_5$ belongs to Alt_5. Since M induces Alt_5 group of outer automorphisms on E, there exists $g \in L$ such that $\sigma' = S_g$ on E. Here S_g denotes conjugation of L by g. Then $[S_g^{-1}\sigma', L] \leqslant C_L(E) = Z(L)$. Now one can show that $[S_g^{-1}\sigma', *]: L \to Z(L)$ is a homomorphism. Thus $\sigma' = S_g$ is inner. This proves $|\mathrm{Out}(\mathscr{B})| = 2$. Since $\mathbb{Q}(i)$ splits $\mathscr{A}$, $2 \| |R|$ and $R = Z(L) \times R_1$, where $R_1 \cong G_{m,r}$ has odd order. $G/LR_1 \subsetneq \mathrm{Out}(L)$. So either $G = LR_1$ giving (h) or $|G : LR_1| = 2$. In the latter case, note that $(mn, 30) = 1$ as $\mathbb{Q}(\zeta_3)$ or $\mathbb{Q}(\zeta_5)$ splits $\mathscr{A}$. So by the Schur–Zassenhaus theorem $G = L^* R_1$ for some subgroup L^* containing L. Pick $h' \in L^* \backslash L$ to induce the automorphism χ on L. We can proceed exactly as in the proof of Theorem 4.7 to show that $h' = \pm(a+b)c/\sqrt{2}$, where $E = \langle a, b \rangle \curlyvee \langle c, d \rangle = \mathscr{Q}_8 \curlyvee \mathscr{D}_8$, $h'^2 = 1$, and $R_1 = 1$. Thus $G = L^* \cong \mathscr{B}^*$, which is the final group (i).

9. We observe that any of the groups obtained in this theorem is primitively represented in the algebra $A = \mathbb{Q}\{G\}$ given that A with the structure as prescribed during the proof has size 2. The demonstration of this fact is entirely analogous to 4.8 and is therefore omitted.

6. Arithmetic Restrictions on the Parameters

1. In the previous three sections, we started by assuming that G is a finite primitive subgroup of $M_2(D)$ spanning it over $\mathbb{Q}$ and then obtained the group theoretic structure of G. In the meanwhile, we were able to express $A = \mathbb{Q}\{G\}$ for each type of G as a (tensor product of) crossed product algebra(s). Clearly the parameters of G have to satisfy certain conditions to ensure that A has size 2. The aim of this section is to find the precise such conditions. Now conversely if we start with an algebra A of above types and size 2, then it can easily be seen to contain a spanning subgroup of the corresponding types. In this regard, Lemma 2.4 applies to factorisable groups. As observed in 2.8, 4.8, and 5.9, the representation of this group in A will be primitive.

We illustrate the required calculations for a sample of three groups. It is hoped that the reader will have no difficulty in carrying out similar calculations for any of the remaining groups. We leave out the various groups obtained in Section 4, for there G can be modified to $\bar{G}$ in such a way that $\mathbb{Q}\{G\} = \mathbb{Q}\{\bar{G}\}$ and $\bar{G}$ is (the central product of $\mathcal{Q}_8$ with) a group of Section 3. Thus the calculations reduce to the ones necessary for Section 3. The same remark applies to insoluble groups of Theorem 5.8, except that there is a slight complication when the perfect radical of G is $SL(2, 5)$. To illustrate the technique there, we examine the case (d) of that theorem. Finally, regarding the groups in Theorem 3.8, we remark that those in class 1 are dealt with in a manner analogous to that in [1]. Moreover the conditions given for class 4 groups are complete. Hence we treat one group from the classes 2 and 3 only. Namely we examine (d_1) and (j).

2. The lemma below shows that when G is of the types in Theorem 3.8, its expression as a 2-nilpotent group is most suitable for working with $\mathbb{Q}\{G\}$. Thus starting with $G = L \rfloor (H \times S)$, put $G_1 = L \rfloor H$, $\langle a \rangle = L \times C_H(L)$, $\langle b \rangle = H$. We have the relations $a^m = 1$, $b^n = a^{t'}$, $bab^{-1} = a^r$, $s't' = m$, $s' \mid (r-1, m)$, $n = \gamma(r, m)$, $(s', t') = 1$, and mn is odd. Clearly $G_1 \cong G_{m,r}$ in the notation of [1]. S is a Sylow 2-subgroup of G and $[S, b] = 1$. Recall that $C \leqslant S$ has order 2^α and $|O_2(G) : C| \leqslant 2$. Moreover $\bar{S} = S/C$ acts faithfully on $\langle a \rangle \times C$.

3. Lemma. *With the above notation, $\mathbb{Q}\{G\}$ has size 2 if and only if both of the following hold:*

(a) $\mathbb{Q}\{G_1\} \cong A_{m,r}$ *is a division algebra.*

(b) $\mathbb{Q}\{a, S\} \cong \langle \mathbb{Q}(\zeta_{2^\alpha m}), \bar{S}, * \rangle$ *has size* 2.

Proof. Using Lemma 2.3, we have $\mathbb{Q}\{G\} = A \otimes_K B$, where F, F', K are the fixed fields of S, b, $S \times \langle b \rangle$ in $E = \mathbb{Q}(\zeta_{2^\alpha m})$ and $A = \langle F'/K, S, * \rangle$,

$B = \langle F/K, b, * \rangle$. Furthermore $\mathbb{Q}\{a, S\} = A \otimes_K F$ and $B \otimes_K F' = \mathbb{Q}\{G_1\} \otimes_Z F'$, where $Z = Z(\mathbb{Q}\{G_1\})$. Now A, B have 2-power, odd index, respectively, and $|F:K|$ is odd while $|F':K|$, $|F':Z|$ are even ($F' = Z(\zeta_{2^s})$). Therefore by 1.3,

> $\mathbb{Q}\{G\}$ has size $2 \Leftrightarrow A$ has size 2 and B is a division algebra $\Leftrightarrow$ $\mathbb{Q}\{a, S\}$ has size 2 and $\mathbb{Q}\{G_1\}$ is a division algebra.

By Theorem 5 of [1], 3(a) is satisfied if and only if the following holds:

> For every prime $q \mid n$, there exists a prime $p \mid m$ since that $q \nmid \gamma(r, mp^{-l_p})$ and $\beta(q, s) \geqslant \beta(q, m-1) + \max_{i=1}^{k} \beta(q, \gamma_i)$, $p^{l_p} \| m$; $s = (r-1, m)$; $\gamma_i = \gamma(p, p_i)$ and the p_i, $1 \leqslant i \leqslant k$, are the prime divisors of m different from p or q.

Thus for the groups of Theorem 3.8 we may restrict our attention to the treatment of condition 3(b).

4. We consider here the type 3.8(d_1). Put $S = \langle c, d \rangle$; $c^{2^{\alpha+2}} = 1$, $d^2 = 1$, $dcd^{-1} = c^{-1}$, $\alpha \geqslant 1$; $C = \langle c^2 \rangle$; $cac^{-1} = a^{r_1}$, $dad^{-1} = a^{r_2}$. Clearly if $\alpha = 1$ then $O_2(G)$ must be C, i.e., r_1 and r_2 must be independent modulo m. When $\alpha \geqslant 2$, we have $O_2(G) = C$ or $\langle c^2, d \rangle$ or $\langle c^2, cd \rangle$. That is, we may have r_2 or $r_1 r_2 = 1(m)$. We summarise our result:

> $A = \mathbb{Q}\{a, S\}$ has size 2 with Hasse invariant of $\frac{1}{2}$ at the prime divisors of p if and only if one of the conditions below holds:

(a) $p = \infty$; $\alpha = 1$; $r_1 \equiv -1(m)$; $r_2 \not\equiv 1, -1(m)$.

For the remaining conditions $p^l \| m$, $l \geqslant 1$. Put $m' = mp^{-l}$, $f = \gamma(p, m')$.

(b) $\alpha \geqslant 2$; $r_1 \equiv -1(p^l)$, $r_1 \equiv 1(m')$, $p \equiv -1 + 2^{\alpha}(2^{\alpha+1})$; either $2 \| f$, $p^{f/2} \equiv r_2(m')$ or f odd, $r_2 \equiv 1(m')$ so that $O_2(G) = \langle c^2, d \rangle$ or $\langle c^2, cd \rangle$.

(c) $\alpha \geqslant 2$; $r_1 \equiv -1(p^l)$, $r_1 \equiv 1(m')$; either $2^i \| p-1$, $2 \leqslant i \leqslant \alpha$, $2^{\alpha-i+1} \nmid f$ or $p \equiv 1 + 2 + \cdots + 2^i(2^{i+2})$, $1 \leqslant i \leqslant \alpha - 2$, $2^{\alpha-i} \nmid f$.

(d) $\alpha = 1$; r_2 or $r_1 r_2 \equiv -1(p^l)$ and $\equiv 1(m')$; f is even and $p^{f/2} \equiv r_1(m')$.

(e) $\alpha = 1$; $r_1 \equiv -1(p^l)$, $r_1 \equiv 1(m')$. Either f is odd, $p \equiv 3(4)$, $r_2 \not\equiv 1(m')$ or f is even, $p^{f/2} \equiv r_2(m')$, $p \equiv 1(4)$ or $4 \mid f$.

Proof. The two cases $\alpha = 1$ and $\alpha \geqslant 2$ require different calculations. To begin with, let $\alpha \geqslant 2$. The algebra A can be factorised according to Lemma 2.3. Put $\zeta = c^2$, $c' = c(1 + \zeta^{-1})$. Since $\alpha \geqslant 2$ c' is nonzero, c' and d commute and $\eta = c'^2 = (1+\zeta)(1+\zeta^{-1}) = \zeta + \zeta^{-1} + 2$. In the field $E = \mathbb{Q}(\zeta_{2^s m})$, let F, F', K be the fixed fields of $\langle d \rangle$, $\langle c \rangle$, $\langle c, d \rangle$. We have $A = B \otimes_K \langle F'/K, d, 1 \rangle$, where $B = \langle F/K, c', \eta \rangle$. So we require B to be a

division algebra. So at some prime p, the invariant of B is $\frac{1}{2}$. Equivalently $\eta \notin \mathcal{N}_{F_p/K_p}$. Put $Z=\mathbb{Q}(\zeta)$, $Z'=\mathbb{Q}(\zeta+\zeta^{-1}) \leqslant K$. $N_{Z'/\mathbb{Q}}(\eta)=N_{Z/\mathbb{Q}}(1+\zeta)=2$. So η is a unit of $K_q=K\mathbb{Q}_q$ for any odd prime q. η is totally positive as $\zeta+\zeta^{-1}>-2$. At $q=2$, η is a norm, for $N_{K_2/\mathbb{Q}_2}(\eta)=N_{Z_2'/\mathbb{Q}_2}(\eta)^h=2^h$, where $h=|K_2:Z_2'|$. So $(\eta, F_2/K_2)=(N_{K_2/\mathbb{Q}_2}(\eta), F_2/\mathbb{Q}_2)=(2^h, E_2/\mathbb{Q}_2)|_{F_2}=1$. At a prime $q \nmid m$, $q \neq 2$, the extension F_q/K_q is unramified so that η is a norm. Hence $p \mid m$. Put $p^l \| m$, $m'=mp^{-l}$, $f=\gamma(p, m')$, $D_p=D_p(E/\mathbb{Q})$, $I_p=I_p(E/\mathbb{Q})$. For F_p/K_p to be ramified, we require $I_p \cap \langle c, d\rangle \not\leqslant \langle d\rangle$. Hence $c \in I_p$ as cd inverts ζ. So $r_1 \equiv -1(p^l)$, $r_1 \equiv 1(m')$. We have two possibilities for D_p.

Case 1. $d \in D_p$. So a 2-power of p is congruent to $-1 \bmod 2^\alpha$. Since -1 does not have a square root mod 2^α, $p \equiv -1(2^\alpha)$. If f is even, then $|D_p/I_p|=f$ and d induces the $f/2$-power of the Frobenius on $\mathbb{Q}_p(\zeta_{2^\alpha m'})/\mathbb{Q}_p$. Thus $f=2f'$, f' odd, and $r_2 \equiv p^{f'}(m')$. If f is odd, then $|D_p/I_p|=2f$ and d is the f-power of the Frobenius on $\mathbb{Q}_p(\zeta_{2^\alpha m'})/\mathbb{Q}_p$. So $f=f'$ is odd and $r_2=p^{f'} \equiv 1(m')$ (so $O_2(G)=\langle c^2, d\rangle$ or $\langle c^2, cd\rangle$). Now $h=|K_p:\mathbb{Q}_p|=p^{l-1}(p-1)\,2f'/4$ and $\eta \in \mathbb{Q}_p$. So $(\eta, F_p/K_p)=\sigma|_{F_p}$, where $\sigma=(\eta^h, E_p/\mathbb{Q}_p)$. Since σ is trivial on $\mathbb{Q}_p(\zeta_{2^\alpha m'})$ and the norm group of $\mathbb{Q}_p(\zeta_{p^l})/\mathbb{Q}_p$ consists of $\langle$Units of $\mathbb{Z}_p$ congruent to 1 mod $p^l\rangle \times \langle p\rangle$, we see that $\eta \notin \mathcal{N}_{F_p/K_p} \Leftrightarrow \sigma|_{F_p} \neq 1 \Leftrightarrow \sigma \neq 1 \Leftrightarrow \eta \notin (\mathbb{Z}_p^\times)^2$. Now in an algebraic closure of $\mathbb{Q}_p$, put $\zeta=\xi^2$. Then $\eta=(\xi+\xi^{-1})^2$. So we want $\xi+\xi^{-1} \notin \mathbb{Q}_p$. Since $p \equiv -1(2^\alpha)$, $|\mathbb{Q}_p(\xi):\mathbb{Q}_p|=2$ and its automorphism is $\chi: \xi \to \xi^p$. Clearly we want $p \equiv -1+2^\alpha(2^{\alpha+1})$ as then $\chi(\xi+\xi^{-1})=-(\xi+\xi^{-1})$. Thus we get conditions (b).

Case 2. $d \notin D_p$. We have $F_p=E_p$, $Z_p \leqslant K_p$. Put $f'=\gamma(p, 2^\alpha)$, $h=|K_p:Z_p|=p^{l-1}(p-1)\,\mathrm{lcm}(f, f')/2f'$, and $\sigma=(\eta, E_p/K_p)=(N_{Z_p/\mathbb{Q}_p}(\eta)^h, E_p/\mathbb{Q}_p)$. Now σ is trivial on $\mathbb{Q}_p(\zeta_{2^\alpha m'})/\mathbb{Q}_p$ and $p^{l-1}(p-1)/2 \mid h$. Hence in order that $\sigma \neq 1$ or equivalently $\eta \notin \mathcal{N}_{E_p/K_p}$, we want $N_{Z_p/\mathbb{Q}_p}(\eta)=N_{Z_p/\mathbb{Q}_p}(1+\zeta^{-1})^2 \times \zeta^{(p^{f'}-1)/(p-1)}$ to be a nonsquare in $\mathbb{Q}_p$ and $\gcd(f, f')/f'$ to be odd. An easy calculation shows that this is equivalent to condition (c) of our statement. Notice that $d \notin D_p$ follows from (c) as no power of p is congruent to $-1 \bmod 2^\alpha$.

Now we consider $\alpha=1$. Pick a prime divisor q of m such that d inverts $O_q(\langle a\rangle)$. Let $q^\delta \| m$, $\zeta=\zeta_{q^\delta}$, and $c_q=(\zeta-\zeta^{-1})c$. Then c_q and d commute and $\eta_q=c_q^2=\mp(\zeta-\zeta^{-1})^2$ according as $c\zeta c^{-1}=\zeta^{\pm 1}$. By Lemma 2.3, $A=B_q \otimes_K \langle F'/K, d, 1\rangle$, where $B_q=\langle F/K, c_q, \eta_q\rangle$ and F, F', K are the fixed fields of d, c, $\langle c, d\rangle$ in $E=\mathbb{Q}(\zeta_m)$. First suppose that p is an infinite prime. So F is complex, K is real, and $\eta_q<0$. So $c\zeta c^{-1}=\zeta^{-1}$. It follows that c inverts $\langle a\rangle$ while d acts on some part of $\langle a\rangle$. We get the condition (a). Next assume that p is a finite prime. We will see that $p \mid m$. Put $p^l \| m$, $l \geqslant 0$; $m'=mp^{-l}$, $D_p=D_p(E/\mathbb{Q})$, $I_p=I_p(E/\mathbb{Q})$, $f=\gamma(p, m')$, $Z=\mathbb{Q}(\zeta)$, and $Z'=\mathbb{Q}(\zeta+\zeta^{-1})$. We distinguish two cases:

Case 1. d or cd centralises $O_{p'}(\langle a\rangle)$. Thus $p\mid m$. If cd centralises $O_{p'}(\langle a\rangle)$. Thus $p\mid m$. If cd centralises $O_{p'}(\langle a\rangle)$, then replace d by cd (and r_2 by r_1r_2) and start again. So we may assume that d centralises $O_{p'}(\langle a\rangle)$. Therefore $q=p$ and $r_2\equiv -1(p^l)$, $r_2\equiv 1(m')$. Since B_p has invariant of $\frac{1}{2}$ at p, we have $|F_p:K_p|=2$ and $\eta_p\notin\mathcal{N}_{F_p/K_p}$. So $c\in D_p$ as $d\in I_p$. So f is even and $r_1\equiv p^{f/2}(m')$. We have $|K_p:Z_p'|=f/2$, $N_{Z_p'/\mathbb{Q}_p}(\eta_p)=\pm N_{Z_p/\mathbb{Q}_p}(\zeta-\zeta^{-1})=\pm p$, $N_{K_p/\mathbb{Q}_p}(\eta_p)=(\pm p)^{f/2}$. Therefore $(\eta_p, F_p/K_p)=(\pm p^{f/2}, E_p/\mathbb{Q}_p)|_{F_p}\neq 1$ because $(\pm p^{f/2}, E_p/\mathbb{Q}_p)\colon \zeta_{m'}\to\zeta_{m'}^{p^{f/2}}$ is not 1 or d. So in fact $\eta_p\notin\mathcal{N}_{F_p/K_p}$. We have got (d).

Case 2. Neither d nor cd centralises $O_{p'}(\langle a\rangle)$. Clearly we can take $q\neq p$. Writing η for η_q, we have $N_{Z'/\mathbb{Q}}(\eta)=\pm q$. So η is a unit of K_p. Therefore in order that $\eta\notin\mathcal{N}_{F_p/K_p}$, we require F_p/K_p to be ramified of degree 2. In view of the assumption above, it follows that $p\mid m$ and $c\in I_p$. Thus $r_1\equiv -1(p^l)$, $r_1\equiv 1(m')$, and $\eta=-(\zeta-\zeta^{-1})^2$. Let $q^\delta\parallel m'$, $\delta\geqslant 1$, and $f'=\gamma(p,q^\delta)$. First, suppose that $d\notin D_p$. We have $F_p=E_p$, $h=|K_p:Z_p'|=p^{l-1}(p-1)f/\varepsilon f'$, where $\varepsilon=1$ or 2 according as f' is even or odd. Now $\sigma=(\eta, E_p/K_p)=(N_{Z_p'/\mathbb{Q}_p}(\eta)^h, E_p/\mathbb{Q}_p)=1$ if f' or f/f' is even as then $p^{l-1}(p-1)\mid h$. Thus f is odd (which ensures $d\notin D_p$) and $Z_p'=Z_p$. Now $N_{Z_p/\mathbb{Q}_p}(\eta)=-N_{Z_p/\mathbb{Q}_p}(\zeta-\zeta^{-1})^2$. Therefore

$$\eta\notin\mathcal{N}_{E_p/K_p}\Leftrightarrow\sigma\neq 1\Leftrightarrow -1\notin\mathbb{Z}_p^{\times 2}\Leftrightarrow p\equiv 3(4).$$

This is the first part of condition (e). Finally, let $d\in D_p$. So f is even, $r_2\equiv p^{f/2}(m')$ so that f' is also even. This time we have $h=|K_p:Z_p'|=p^{l-1}(p-1)f/2f'$. Put $\xi=N_{Z_p'/\mathbb{Q}_p}(\eta)$. Now $(\eta, F_p/K_p)=(\xi^h, E_p/\mathbb{Q}_p)|_{F_p}$ is nontrivial if and only if $\xi\notin\mathbb{Z}_p^{\times 2}$ and f/f' is odd. We have $\xi=(-1)^{f'/2}\omega^2$, where $\omega^2\in\mathbb{Q}_p$, $\omega=(\zeta-\zeta^{-1})(\zeta^p-\zeta^{-p})\cdots(\zeta^{p^{f'/2-1}}-\zeta^{-p^{f'/2-1}})$. Letting χ be the Frobenius automorphism of $\mathbb{Q}_p(\zeta)/\mathbb{Q}_p$, we have $\chi(\omega)=-\omega$ so $\omega\notin\mathbb{Q}_p$. Hence

$$\xi\notin\mathbb{Z}_p^{\times 2}\Leftrightarrow(-1)^{f'/2}\in\mathbb{Z}_p^{\times 2}\Leftrightarrow 4\mid f' \text{ or } p\equiv 1(4).$$

Clearly the second alternative of condition (e) follows from above. Conversely if that holds, then since q was so chosen that d inverts $O_q(\langle a\rangle)$ we have that f/f' is odd and the above requirement will follow. This concludes the calculations for this group.

5. In this section we shall deal with the type 3.8(j). Put $S=\langle d_1, c\rangle \mathrm{Y}\langle d_2\rangle$, $c^{2^\alpha}=1$, $d_1^2=1$, $d_1cd_1^{-1}=c^{1+2^{\alpha-1}}$; $d_2^{2^\beta}=c^2$; $\alpha\geqslant 2$, $\beta\geqslant 1$; $C=\langle c\rangle$, $d_1\colon a\to a^{r_1}$, $d_2\colon a\to a^{r_2}$. We showed in the proof of Theorem 3.8 that on replacing d_1 by $d_1d_2^{2^{\beta-1}}c^{-1+2^{\alpha-2}}$ (and r_1 by $r_1r_2^{2^{\beta-1}}$), if needed, we can assume that d_1 and d_2 operate on different parts of $\langle a\rangle$, i.e., there exists a factorisation $m=m_1m_2$, $(m_1,m_2)=1$ such that r_1 (or $r_1r_2^{2^{\beta-1}}$) $\equiv 1$ (m_2) and $r_2\equiv 1$ (m_1). Moreover in the case when $\alpha=2$, we have $\beta=1$, $\langle d_1d_2, c\rangle\cong\mathcal{Q}_8$, and possibly $O_2(G)=\langle d_1d_2, c\rangle$ in which case we take

$m=1$. In other cases $O_2(G)=C$ and we choose m_2 so that $(r_2-1, m_2)=1$. Now we summarise our results.

The algebra $A=\mathbb{Q}\{a, S\}$ with $\langle a, S\rangle$ as above has size 2 with a Hasse invariant of denominator 2^β at (the prime divisors of) p if and only if one of the following holds:

(a) $p=2$, $\alpha=2$, $\beta=1$; $r_1r_2\equiv 1(m)$. Putting $f=\gamma(2, m)$, either f is odd or $2\|f$, $2^{f/2}\equiv r_2(m)$.

(b) $p\mid m$, $\alpha=2$, $\beta=1$; $r_1r_2\equiv 1(m)$. Let $p^l\|m$, $m'=mp^{-l}$, $f=\gamma(p, m')$. Then $r_2\equiv -1(p^l)$, $r_2\equiv 1(m')$; f odd, $p\equiv 3(4)$.

In the remaining conditions, there exists a nontrivial decomposition $m=m_1m_2$, $(m_1, m_2)=1$, $r_2\equiv 1(m_1)$:

(c) $p=\infty$, $\alpha=2$, $\beta=1$, $r_1\equiv -1(m_1)$, $r_1\equiv 1(m_2)$, $r_2\equiv -1(m_2)$.

(d) $m_2=p^l$, $l\geqslant 1$; either $2^i\|p-1$, $2\leqslant i\leqslant \alpha-1$ or $p\equiv 1+2+\cdots+2^{i-1}(2^{i+1})$ $i\geqslant 2$, $\alpha\geqslant i+2$, $\beta=1$. Put $f=\gamma(p, m_1)$. We have $2^{\alpha-i}\|f$, r_1 or $r_1r_2^{2^{\beta-1}}\equiv p^{f/2}(m_1)$ and $\equiv 1(m_2)$.

(e) $m_2=p^l$, $l\geqslant 1$, $p\equiv 3(4)$, $\alpha=2$, $\beta=1$. Put $f=\gamma(p, m_1)$. We have $2\|f$, r_1 or $r_1r_2\equiv p^{f/2}(m_1)$ and $\equiv 1(m_2)$.

Proof. Let us deal with $O_2(G)\cong\mathscr{Q}_8$ first. Thus $r_1\equiv r_2(m)$ and $A=\mathscr{A}_Z\otimes_Z B$, where $B=\langle E/Z, d_2, -1\rangle$, $E=\mathbb{Q}(\zeta_m)$, and Z is the fixed field of d_2 in E. Now $\mathscr{A}_Z$ has nonzero invariant at ∞ if Z is real and at 2 if $|Z_2:\mathbb{Q}_2|$ is odd. When Z is real, B also has nonzero invariant at ∞. Therefore A has size 2 with invariant $\frac{1}{2}$ at (prime divisor of) p if and only if one of the following two holds:

(i) $p=2$ and $|Z_2:\mathbb{Q}_2|$ is odd. Putting $f=\gamma(2, m)$, we require f to be odd or $2\|f$ and $2^{f/2}\equiv r_2(m)$. This is (a).

(ii) $p\mid m$ and $(-1, E_p/Z_p)\neq 1$. So $d\in I_p(E/\mathbb{Q})$, i.e., $r_2\equiv -1(p^l)$, $r_2\equiv 1(m')$, where $p^l\|m$ and $m'=mp^{-l}$. Putting $f=\gamma(p, m')$, we have $(-1, E_p/Z_p)=((-1)^{p^{l-1}(p-1)f/2}, E_p/\mathbb{Q}_p)$. So we want f to be odd and $p\equiv 3(4)$. We get (b).

We can now assume that $O_2(G)=C$. Let $a=a_1a_2=a_2a_1$ with $a_1^{m_1}=a_2^{m_2}=1$. After a possible replacement of d_1 and r_1 we have $S=\mathscr{E}_{2^{\alpha+1}}\curlyvee\mathscr{C}_{2^{\beta+\alpha-1}}$ (*) or $\mathscr{Q}_8\curlyvee\mathscr{C}_4$ (**). Now $\langle a, S\rangle=\langle a_1, c, d_1\rangle\curlyvee\langle a_2, d_2\rangle$ and

$$A=(X\otimes_{\mathbb{Q}} Z)\otimes_Z(B\otimes_{Z_2} Z),$$

where Z_1 and Z_2 are the fixed fields of d_1 and d_2 in $E=\mathbb{Q}(\zeta_{2^\alpha m_1})$ and $\mathbb{Q}(\zeta_{2^{\alpha-1}m_2})$, $Z=Z_1Z_2$, $B=\langle\mathbb{Q}(\zeta_{2^{\alpha-1}m}), d, \zeta_{2^{\alpha-1}}\rangle$, and $X=M_2(\mathbb{Q})$ or $\mathscr{A}$ according as (*) or (**) holds. Now $d_1\notin D_2(E/\mathbb{Q})$ so $\mathscr{A}\otimes_{\mathbb{Q}} Z$ is plit except

when Z is real which is the case iff $r_1 \equiv -1(m_1)$, $r_2 \equiv -1(m_2)$. But then the invariant of B is $\frac{1}{2}$ at ∞. So A has size 2 with a Hasse invariant of denominator 2^β at some prime p if and only if either $p=\infty$, $(*)$ holds and Z is real, so that $\alpha=2$, $\beta=1$, $r_1 \equiv -1(m_1)$, $r_2 \equiv -1(m_2)$ giving (c) or p is finite, B has a similar Hasse invariant at p, and $|Z\mathbb{Q}_p : Z_2\mathbb{Q}_p|$ is odd. We concentrate our attention on the latter case. Now $B \cong A_{2^{\alpha-1}m_2,r}$, where $r \equiv 1(2^{\alpha-1})$, $r \equiv r_2(m_2)$, and $s=(r-1, 2^{\alpha-1}m_2)=2^{\alpha-1}$. Thus the first requirement is answered by Theorem 5 of [1]:

(i) $m_2 = p^l$, $l \geqslant 1$, $2^i \| p-1$, $2 \leqslant i \leqslant \alpha-1$.

(ii) $m_2 = p^l$, $l \geqslant 1$; $\beta=1$; $p \equiv 1+2+\cdots+2^{i-1}(2^{i+1})$ $i \geqslant 2$; $r_2 \equiv -1(m_2)$. Either $\alpha \geqslant i+2$ or $\alpha=2$.

Now we treat the second requirement for the above possibilities:

(i) Since $Z_2\mathbb{Q}_p \cap Z_1\mathbb{Q}_p = \mathbb{Q}_p(\zeta_{2^{\alpha-1}})$, we want $h=|Z\mathbb{Q}_p : Z_2\mathbb{Q}_p| = |Z_1\mathbb{Q}_p : \mathbb{Q}_p(\zeta_{2^{\alpha-1}})|$ to be odd. We have $|\mathbb{Q}_p(\zeta_{2^{\alpha-1}}) : \mathbb{Q}_p| = 2^{\alpha-i-1}$, $|\mathbb{Q}_p(\zeta_{2^\alpha}) : \mathbb{Q}_p| = 2^{\alpha-i}$. Thus we want $Z_1\mathbb{Q}_p < \mathbb{Q}_p(\zeta_{2^\alpha m_1})$, that is, $d_1 \in D_p = D_p(\mathbb{Q}(\zeta)/\mathbb{Q})$, where $\zeta = \zeta_{2^\alpha m_1}$. Now D_p is cyclic, generated by $\zeta \to \zeta^p$ of order $f' = \operatorname{lcm}(2^{\alpha-i}, f)$, where $f = \gamma(p, m_1)$. So we must have $p^{f'/2} \equiv r_1 \not\equiv 1(m_1)$ and $p^{f'/2} \equiv 1 + 2^{\alpha-1}(2^\alpha)$. This forces $f'=f$ and $2^{\alpha-i} \| f$. Now $h = f/2^{\alpha-i}$ is in fact odd. We get (d).

(ii) When $\alpha \geqslant i+2$, all the above argument goes through, giving the other half of (d). So let $\alpha=2$. We have $Z_2\mathbb{Q}_p \cap Z_1\mathbb{Q}_p = \mathbb{Q}_p$ so want $|Z_1\mathbb{Q}_p : \mathbb{Q}_p|$ to be odd. Put $f = \gamma(p, m_1)$. If f is odd, then $Z_1\mathbb{Q}_p = \mathbb{Q}_p(\zeta_{4m_1})$, which has degree $2f$ over $\mathbb{Q}_p$. So f is even and we want $2 \| f$, $p^{f/2} \equiv r_1(m_1)$, which ensures $|Z_1\mathbb{Q}_p : \mathbb{Q}_p| = f/2$ is odd. We get (e). The proof is complete.

6. In this final section, we consider the group 5.8(d). Let G be that group. The structure of the algebra $\mathbb{Q}\{G\}$ is described in Case 1(ii) of the proof of Theorem 5.8. Putting $F=\mathbb{Q}(\zeta_{2^\alpha})$, $A_{m,r} = \mathbb{Q}\{G_{m,r}\}$, $K = Z(A_{m,r})$, $A = \langle F(\sqrt{5})/F, \bar{d}, \zeta_{2^\alpha}\rangle$, where $\bar{d}: \sqrt{5} \to -\sqrt{5}$, we have

$$\mathbb{Q}\{G\} = (M_2(A) \otimes_F KF) \otimes_{KF} (KF \otimes_K A_{m,r}),$$

as the $\mathscr{A}$ factor is split by F. Now $|KF : K| = 2^{\alpha-1}$ and $A_{m,r}$ has odd index. So $\mathbb{Q}\{G\}$ has size 2 if and only if $A_{m,r}$ is a division algebra and A is a division algebra not split by KF. The conditions for the first requirement are given preceding 6.4. As to the second, we prove first that A is necessarily a division algebra. Since F is complex and ζ_{2^α} is a unit of F, the algebra A is split at all (prime divisors of) rational primes except for those which ramify in $F(\sqrt{5})/F$. That is, $p=5$. We have $|F_5 : \mathbb{Q}_5| = 2^{\alpha-2}$, $\xi = N_{F_5/\mathbb{Q}_5}(\zeta_{2^\alpha})$ is a primitive 4th root of 1 in $\mathbb{Q}_5$. So $\xi \equiv \pm 2(5)$ and $(\zeta_{2^\alpha}, F_5(\sqrt{5})/F_5) = (\xi, F_5(\zeta_5)/\mathbb{Q}_5)|_{F_5(\sqrt{5})} \neq 1$ as $(\xi, F_5(\zeta_5)/\mathbb{Q}_5)$: $\zeta_5 \to \zeta_5^{\mp 2}$.

Thus A is a division algebra with invariant of $\frac{1}{2}$ at 5 only. Now $|\mathbb{Q}(\zeta_m) : K|$ is odd. Therefore we want $F(\zeta_m)$ not to split A, i.e., $|F_5(\zeta_m) : F_5|$ to be odd. Putting $f = \gamma(5, m)$, we have $|F_5(\zeta_m) : \mathbb{Q}_5| = \text{lcm}(2^{\alpha-2}, f)$. Thus we want $2^{\alpha-1} \nmid f$. Summarising:

> The algebra $\mathbb{Q}\{G\}$ has size 2 if and only if m, r (and $n = \gamma(r, m)$, $s = (r-1, m)$) satisfy the condition cited above and $2^{\alpha-1} \nmid \gamma(5, m)$.

ACKNOWLEDGMENTS

There remains for me the pleasant task of expressing my deep gratitude to Professor B. Hartley, whose guidance has been invaluable in the completion of this task. I also thank the University of Manchester for providing financial support during the preparation of this work.

REFERENCES

1. S. A. AMITSUR, Finite subgroups of division rings, *Trans. Amer. Math. Soc.* **80** (1955), 361–386.
2. E. ARTIN, "Algebraic Numbers and Algebraic Functions," Gordon & Breach, New York, 1967.
3. C. T. BENSON AND L. C. GROVE, "Finite Reflection Groups," Bogden & Quigley, New York, 1971.
4. R. W. CARTER, "Simple Groups of Lie Type," Wiley–Interscience, New York, 1972.
5. C. CURTIS AND I. REINER, "Representation Theory of Finite Groups and Associative Algebras," Wiley–Interscience, New York, 1962.
6. M. L. CURTIS, "Matrix Groups," Springer-Verlag, New York, 1979.
7. L. E. DICKSON, "Linear Groups," Dover, New York, 1958.
8. L. DORNHOFF, "Group Representation Theory, Part A," Dekker, New York, 1971.
9. B. FEIN AND M. SCHACHER, Embedding finite groups in rational division algebras I, *J. Algebra* **17** (1971), 412–428.
10. D. GORENSTEIN, "Finite Groups," Harper & Row, New York, 1968.
11. B. HARTLEY AND M. A. SHAHABI SHOJAEI, Finite quasi-simple groups of 2×2 matrices over a division ring, to appear.
12. B. HARTLEY AND M. A. SHAHABI SHOJAEI, Finite group of matrices over division rings, *Math. Proc. Cambridge Philos. Soc.* **92** (1982), 55–64.
13. M. HIKARI, On finite multiplicative subgroups of simple algebras of degree 2, *J. Math. Soc. Japan*, **28** (1976), 737–748.
14. M. HIKARI, On simple groups which are homomorphic images of multiplicative subgroups of simple algebras of degree 2, *C. R. Math. Rep. Acad. Sci. Canada*, **4** (1982), 93–96 (Zentralblatt No. 496.16009).
15. M. HIKARI, Nonsolvable multiplicative subgroups of $M_2(D)$, *in* "Proceedings, 15th Symposium on Ring Theory, Takarazuka, Japan, 1982," pp. 31–35 (Zentralblatt No. 498.16018).
16. B. HUPPERT, "Endliche Gruppen I," Springer-Verlag, Berlin, 1982.
17. B. HUPPERT AND N. BLACKBURN, "Finite Groups II," Springer-Verlag, Berlin, 1982.
18. S. IYANAGA (Ed.), "The Theory of Numbers," North-Holland, Amsterdam, 1975.

19. N. JACOBSON, The fundamental theorem of the Galois theory for quasi-fields, *Ann. of Math.*, **41** (1940), 1–7.
20. G. J. JANUSZ, "Algebraic Number Fields," Academic Press, New York, 1973.
21. G. J. JANUSZ, Simple components of $\mathbb{Q}[SL(2, q)]$, *Comm. Algebra* **1** (1974), 1–22.
22. J. NEUKIRCH, "Klassenkörpertheorie," Bibliographisches Institut, Mannheim, 1969.
23. D. PASSMAN, "Permutation Groups," Mathematics Lecture Notes, Benjamin, New York, 1968.
24. I. REINER, "Maximal Order," Academic Press, New York/London, 1975.
25. P. ROQUETTE, Realisierung von Darstellungen endlicher nilpotenter Gruppen, *Arch. Math.* **9** (1958), 241–250.
26. M. SHIRVANI AND B. WEHRFRITZ, "Skew Linear Groups," Lecture Note Series, Vol. 118, London Math. Soc. London, 1986.
27. J. TITS, Quaternions over $\mathbb{Q}(\sqrt{5})$, Leech's lattice and the sporadic simple group of Hall–Janko, *J. Algebra* **63** (1980), 56–75.
28. T. YAMADA, "The Schur Subgroup of the Brauer Group," Lecture Notes in Mathematics, Vol. 397, Springer-Verlag, New York/Berlin, 1974.
29. H. ZASSENHAUS, Über endliche Fastkörper, *Hamb. Abh.* **11** (1936), 187–220.