ON EXCEPTIONAL GROUPS OF ORDER p^5

JOHN R. BRITNELL, NEIL SAUNDERS, AND TONY SKYNER

Abstract. A finite group G is *exceptional* if it has a quotient Q whose minimal faithful permutation degree is greater than that of G. We say that Q is a *distinguished* quotient.

The smallest examples of exceptional p-groups have order p^5. For an odd prime p, we classify all pairs (G, Q) where G has order p^5 and Q is a distinguished quotient. (The case $p = 2$ has already been treated by Easdown and Praeger.) We establish the striking asymptotic result that as p increases, the proportion of groups of order p^5 with at least one exceptional quotient tends to $1/2$.

1. Introduction

Let G be a finite group. The minimal degree $\mu(G)$ of G is the least non-negative integer n such that G embeds into the symmetric group S_n. The question of representing finite groups by permutations is one of the oldest in group theory, and the minimal degree $\mu(G)$ is a natural invariant of the group G. However it is well known that the function μ is badly behaved with regard to quotients: it is possible for a group G to have a quotient Q such that $\mu(G) < \mu(Q)$. Such cases are pitfalls in the design and implementation of permutation group algorithms (see [14]).

The following terminology is derived from Easdown and Praeger [3]. If G has a normal subgroup N such that $\mu(G) < \mu(G/N)$, then we say that N is a *distinguished subgroup* of G, and that G/N a *distinguished quotient*. The group G is *exceptional* if it has at least one distinguished quotient Q; and we say also that G is an *exceptional extension* of Q.

In this paper we give a complete classification of the exceptional groups of order p^5, together with their distinguished subgroups, for any prime p. These are the smallest exceptional p-groups for each p. In the case $p = 2$ these groups are known from [3], in which it is shown there are two exceptional groups of order 32. In the case of an odd prime p, the only previously known construction of an exceptional group of order p^5 is given by Lemieux [13]. Our main result is as follows.

Theorem 1. *Let G be a group of order p^5, and let Q be a quotient of G such that $\mu(Q) > \mu(G)$. Then $|Q| = p^4$, and the pair (G, Q) is one of those listed in Table 1.*

Date: December 12, 2016.

2010 *Mathematics Subject Classification.* 20B35, (secondary) 20D15.

Key words and phrases. permutation representation, minimal degree.

Table 1 gives an explicit presentation for each exceptional G and distinguished quotient Q. For the sake of completeness, we include the results of Easdown and Praeger in the case $p = 2$ where there is only one such Q, namely the quaternion 2-group of order 16.

The number of exceptional groups of order p^5 is surprisingly large. It is perhaps worth noting that Easdown and Praeger [3] expressed doubt as to whether such groups existed at all for $p > 2$, although they found exceptional groups of order p^6 for all primes p.

Theorem 2. *The total number of exceptional groups of order p^5 is*

$$\begin{cases} 2 & \text{if } p = 2, \\ 10 & \text{if } p = 3, \\ p + 6 & \text{otherwise.} \end{cases}$$

The number of groups of order p^5 is at most $2p + 71$. Theorem 2 implies that the number of exceptional groups of order p^5 is $p + 6$ for $p > 3$. Hence the proportion of groups of order p^5 which are exceptional is asymptotically $1/2$. This suggests that the established term *exceptional* for these groups (introduced in [3]) may be less appropriate than it has previously seemed. It would be interesting to understand the asymptotics for exceptional groups of order p^6 and larger, but we have nothing to add on this question at present.

1.1. **Notation for the exceptional groups.** The exceptional groups G are listed in Table 1. For each possible distinguished quotient Q we first give a presentation of Q itself; we then give presentations of the exceptional extensions of Q. Our presentations use the following convention: the generators of G are taken to be preimages of those of Q (and denoted by the same letters), together with a generator n of N. The generator n is always central, and we shall write "n central" in our presentations as a convenient shorthand for the commutator relations.

The names given to the extensions in the table are purely for ease of reference, and are not used in the text of the paper. The names given here to the various quotients, however, are introduced and used during the course of our argument.

In the case that $p = 2$ there are only two exceptional groups, G_1 and G_2 in the table; the classification in this case appears in [3] and will not be treated here. For each odd prime p, we take $\alpha = \alpha_p$ to be a fixed quadratic non-residue modulo p. We shall require the Legendre symbol,

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{if } p \text{ divides } a, \\ 1 & \text{if } a \text{ is a quadratic residue modulo } p, \\ \text{-1} & \text{if } a \text{ is a quadratic non-residue modulo } p. \end{cases}$$

TABLE 1. Exceptional groups of order p^5 arranged by distinguished quotients.

Group	Presentation	Notes
Q_{16}	$\langle x,y \mid x^8=1,\ y^2=x^4,\ [x,y]=x^{-2}\rangle$	$p=2$
G_1	$\langle x,y,n \mid x^8=n^2=1,\ y^2=x^4n,\ n \text{ central},\ [x,y]=x^{-2}\rangle$	
G_2	$\langle x,y,n \mid x^8=n^2=1,\ y^2=x^4,\ n \text{ central},\ [x,y]=x^{-2}n\rangle$	
Q_{81}	$\langle x,y,z \mid x^9=y^3=z^3=1,\ [x,y]=1,\ [x,z]=y,\ [y,z]=x^{-3}\rangle$	$p=3$
G_3	$\langle x,y,z,n \mid x^9=y^3=z^3=n^3=1,\ n \text{ central}, [x,y]=n,\ [x,z]=y,\ [y,z]=x^{-3}n\rangle$	
G_4	$\langle x,y,z,n \mid x^9=y^3=z^3=n^3=1,\ n \text{ central},\ [x,y]=1,\ [x,z]=y,\ [y,z]=x^{-3}n\rangle$	
$Q_1(3)$	$\langle x,y,z \mid x^9=y^3=1,\ z^3=x^3,\ [x,y]=1,\ [x,z]=y,\ [y,z]=x^3\rangle$	$p=3$
G_4	$\langle x,y,z,n \mid x^9=y^3=n^3=1,\ n \text{ central},\ z^3=x^3n,\ [x,y]=n,\ [x,z]=y,\ [y,z]=x^3n\rangle$	
G_5	$\langle x,y,z,n \mid x^9=y^3=n^3=1,\ n \text{ central},\ z^3=x^3n,\ [x,y],\ [x,z]=y,\ [y,z]=x^3n^2\rangle$	
G_6	$\langle x,y,z,n \mid x^9=y^3=n^3=1,\ n \text{ central},\ z^3=x^3,\ [x,y]=1,\ [x,z]=y,\ [y,z]=x^3n\rangle$	
$Q_\alpha(3)$	$\langle x,y,z \mid x^9=y^3=1,\ z^3=x^6,\ [x,y]=1,\ [x,z]=y,\ [y,z]=x^6\rangle$	$p=3$, $(\alpha=2)$
G_6	$\langle x,y,z,n \mid x^9=y^3=n^3=1,\ n \text{ central},\ z^3=x^6n,\ [x,y]=1,\ [x,z]=y,\ [y,z]=x^6\rangle$	
G_7	$\langle x,y,z,n \mid x^9=y^3=n^3=1,\ n \text{ central},\ z^3=x^6,\ [x,y]=1,\ [x,z]=y,\ [y,z]=x^6n\rangle$	
$Q(p)$	$\langle x,y,z \mid x^{p^2}=y^p=z^p=[x,y]=[x,z]=1,\ [y,z]=x^p\rangle$	p odd
E_1	$\langle x,y,z,n \mid x^{p^2}=y^p=z^p=1,\ n \text{ central},\ [x,y]=[x,z]=1,\ [y,z]=x^pn\rangle$	
E_2	$\langle x,y,z,n \mid x^{p^2}=z^p=1,\ y^p=n,\ n \text{ central},\ [x,y]=[x,z]=1,\ [y,z]=x^pn\rangle$	
E_3	$\langle x,y,z,n \mid x^{p^2}=y^p=z^p=1,\ n \text{ central},\ [x,y]=1,\ [x,z]=n,\ [y,z]=x^pn\rangle$	
E_4	$\langle x,y,z,n \mid x^{p^2}=y^p=1,\ z^p=n,\ n \text{ central},\ [x,y]=1,\ [x,z]=n,\ [y,z]=x^pn\rangle$	
E_5	$\langle x,y,z,n \mid x^{p^2}=z^p=1,\ y^p=n,\ n \text{ central},\ [x,y]=1,\ [x,z]=n,\ [y,z]=x^p\rangle$	
$E_6(\lambda)$	$\langle x,y,z,n \mid x^{p^2}=z^p=1,\ y^p=n,\ n \text{ central},\ [x,y]=1,\ [x,z]=n^\lambda,\ [y,z]=x^pn\rangle$	$\lambda\neq 0,\ \left(\frac{1+4\lambda}{p}\right)=1$
$Q_1(p)$	$\langle x,y,z \mid x^{p^2}=y^p=1,\ z^p=x^p,\ [x,y]=1,\ [x,z]=y,\ [y,z]=x^p\rangle$	$p>3$
$F_1^{(1)}$	$\langle x,y,z,n \mid x^{p^2}=y^p=1,\ z^p=x^p,\ n \text{ central},\ [x,y]=1,\ [x,z]=y,\ [y,z]=x^pn\rangle$	
$F_2^{(1)}$	$\langle x,y,z,n \mid x^{p^2}=y^p=1,\ z^p=x^p,\ n \text{ central},\ [x,y]=n^{-1},\ [x,z]=y,\ [y,z]=x^pn^2\rangle$	
$F_3^{(1)}$	$\langle x,y,z,n \mid x^{p^2}=y^p=1,\ z^p=x^pn,\ n \text{ central},\ [x,y]=1,\ [x,z]=y,\ [y,z]=x^pn\rangle$	
$F_4^{(1)}(\lambda)$	$\langle x,y,z,n \mid x^{p^2}=y^p=1,\ z^p=x^pn,\ n \text{ central},\ [x,y]=n^{-1},\ [x,z]=y,\ [y,z]=x^pn^{1+\lambda}\rangle$	$\lambda\geq 0,\ \left(\frac{\lambda^2+4}{p}\right)=1$
$F_5^{(1)}(\lambda)$	$\langle x,y,z,n \mid x^{p^2}=y^p=1,\ z^p=x^pn,\ n \text{ central},\ [x,y]=n^{-\alpha},\ [x,z]=y,\ [y,z]=x^pn^{\alpha+\lambda}\rangle$	$\lambda\geq 0,\ \left(\frac{\lambda^2+4\alpha}{p}\right)=1$
$Q_\alpha(p)$	$\langle x,y,z \mid x^{p^2}=y^p=1,\ z^p=x^{\alpha p},\ [x,y]=1,\ [x,z]=y,\ [y,z]=x^{\alpha p}\rangle$	$p>3$
$F_1^{(\alpha)}$	$\langle x,y,z,n \mid x^{p^2}=y^p=1,\ z^p=x^{\alpha p},\ n \text{ central},\ [x,y]=1,\ [x,z]=y,\ [y,z]=x^{\alpha p}n\rangle$	
$F_2^{(\alpha)}$	$\langle x,y,z,n \mid x^{p^2}=y^p=1,\ z^p=x^{\alpha p},\ n \text{ central},\ [x,y]=n^{-1},\ [x,z]=y,\ [y,z]=x^{\alpha p}n^{(\alpha+1)}\rangle$	
$F_3^{(\alpha)}$	$\langle x,y,z,n \mid x^{p^2}=y^p=1,\ z^p=x^{\alpha p}n,\ n \text{ central},\ [x,y]=1,\ [x,z]=y,\ [y,z]=x^{\alpha p}n\rangle$	
$F_4^{(\alpha)}(\lambda)$	$\langle x,y,z,n \mid x^{p^2}=y^p=1,\ z^p=x^{\alpha p}n,\ n \text{ central},\ [x,y]=n^{-1},\ [x,z]=y,\ [y,z]=x^{\alpha p}n^{\alpha+\lambda}\rangle$	$\lambda\geq 0,\ \left(\frac{\lambda^2+4\alpha}{p}\right)=1$
$F_5^{(\alpha)}(\lambda)$	$\langle x,y,z,n \mid x^{p^2}=y^p=1,\ z^p=x^{\alpha p}n,\ n \text{ central},\ [x,y]=n^{-\alpha},\ [x,z]=y,\ [y,z]=x^{\alpha p}n^{\alpha(\alpha+\lambda)}\rangle$	$\lambda\geq 0,\ \left(\frac{\lambda^2+4}{p}\right)=1$

Where a parameter λ appears in a presentation, it represents an integer in the range $[-(p-1)/2,\ldots,(p-1)/2]$ satisfying the conditions stated in the Notes column. Distinct values of λ yield presentations of non-isomorphic groups.

The groups named G_4 and G_6 appear twice in the table with different presentations, as these groups possess two non-isomorphic distinguished quotients. Furthermore the exceptional extensions of the groups $Q_1(p)$ and $Q_\alpha(p)$ are isomorphic in pairs; details of these isomorphisms are given in Section 4.4.

1.2. **Background.** Neumann [14] has pointed out that there exists a sequence of groups (G_i) with quotients (Q_i) such that $\mu(Q_i)$ grows exponentially with $\mu(G_i)$.

Neumann's example takes G_i to be the direct product, and Q_i to be the central product, of i copies of the dihedral group D_8. Holt and Walton [7] have proved the existence of a constant c such that $\mu(G/N) \leq c^{\mu(G)-1}$ for all groups G and normal subgroups N. The constant c is shown to be less than 4.5.

The second author [16] has recently described a general construction of exceptional groups which, like Neumann's construction, uses the idea of the central product as a quotient of the direct product. Instances of this construction are found to occur naturally in the context of binary polyhedral groups.

Recall that the *core* of a subgroup H of G is the intersection of the conjugates of H in G. For a permutation representation of a group G on a set Ω, let $\{H_1, \ldots, H_\ell\}$ be a set of point stabilizers, one for each orbit of G on Ω. These subgroups determine the representation up to equivalence. The representation is faithful if and only if the cores of the subgroups $H_1, \ldots, H_\ell$ intersect trivially. The degree of the representation is given by the sum $\sum_{i=1}^{\ell} |G : H_i|$, and so the minimal degree of G can be expressed as the minimum value taken by this sum over collections of subgroups $\{H_i\}$ whose cores have trivial intersection (see [15] for a fuller treatment).

We shall require the following theorem of Johnson [8].

Theorem 1.1 (Theorem 3 of [8])**.** *Let G be a p-group whose centre $Z(G)$ is minimally generated by d elements. Let $\{H_1, \ldots, H_\ell\}$ be point stabilizers for a minimal representation of G. Then*

(1) *if p is odd then $\ell = d$,*
(2) *if $p = 2$ then $\frac{d}{2} \leq \ell \leq d$, with the bound $\ell = d$ being achieved by some minimal representation of G.*

It will be helpful to collect together here a number of conditions which ensure that a quotient Q of a group G is not distinguished.

Lemma 1.2. *Let G be group, and Q a quotient of G. If any one of the following conditions is met, then Q is not a distinguished quotient of G.*

(1) *Q is isomorphic to a subgroup of G.*
(2) *G is abelian.*
(3) *Q is cyclic.*
(4) *Q is elementary abelian.*
(5) *G is a p-group where p is an odd prime, and Q has a maximal cyclic subgroup.*

Proof. (1) A faithful representation of G restricts to a faithful representation of any subgroup.
(2) This follows from the fact that every quotient of a finite abelian group G is isomorphic to a subgroup of G.
(3) If Q is cyclic then G has a subgroup isomorphic to Q.
(4) This is stated in [9] as a consequence of the main theorem.

(5) This appears in [12]. The proof is short and so we give it here for convenience. Suppose that $|Q| = p^n$ and that Q has a cyclic subgroup C of order p^{n-1}. It follows that G itself has a cyclic subgroup subgroup $\overline{C}$ of order p^{n-1}, and in particular that $\mu(G) \geq p^{n-1}$. We may assume that Q is not itself cyclic, and hence that Q is an extension of C by a group $H \cong C_p$. It is well-known (see [2, Theorem 4.1] for instance) that any such extension is split (since p is odd). If Q is not abelian, then its non-normal factor H is a core-free subgroup of index p^{n-1}, and so $\mu(Q) \leq p^{n-1} \leq \mu(G)$. The remaining case is that $Q \cong C \times H$, in which case $\mu(Q) = p^{n-1} + p$. Now if Q is distinguished, then we must have $\mu(G) = p^{n-1}$. Hence a minimal degree representation of G is transitive, and now by Theorem 1.1 it follows that G has a cyclic centre, and hence that G has a unique normal subgroup Z of order p. But Z is contained in the kernel of the canonical map onto Q, and hence intersects trivially with $\overline{C}$. So the subgroup $\overline{C}Z$ of G is isomorphic to $C_{p^{n-1}} \times C_p \cong Q$.

□

Kovács and Praeger [9] have conjectured that no abelian quotient is distinguished. In later work [10] they have shown that if a minimal counterexample G exists to this conjecture, then G is a p-group, with Q being the quotient by the commutator subgroup G', and with $\mu(Q) = \mu(G) + p$. Perhaps for this reason, the principal focus of work in this area has been on p-groups; however the conjecture remains open. Franchi [5] has shown that $\mu(G/G') \leq \mu(G)$ whenever G contains a maximal abelian subgroup.

The hypothesis that p is odd in Lemma 1.2(5) is necessary only to exclude the case that the quotient Q is a generalized quaternion group; it is known from [3] that these groups arise as distinguished quotients. Excepting these groups, the result holds when $p = 2$ as well.

1.3. **Organisation of the Paper.** In Section 2 we set out some preliminary results. We show that there are no exceptional p-groups of order at most p^4, and that if G is an exceptional group of order p^5 with distinguished quotient N, then N has order p. We classify the possible isomorphism classes of the quotient $Q = G/N$. Some of these results have appeared previously in [12]. We also deal with exceptional groups of order 3^5, which require special treatment. However groups of this order are easily handled by computer calculations, and we have not thought it necessary to give further justification for our results.

In Section 3 we consider exceptional extensions of the group we have named $Q(p)$, in the case $p > 3$. Similarly, in Section 4 we consider extensions of the two groups we have named $Q_1(p)$ and $Q_\alpha(p)$. These admit a common treatment, and indeed their exceptional extensions turn out to be the same up to isomorphism.

2. Preliminaries

We shall often use the following elementary observation.

Proposition 2.1. *Let P be a p-group. Either P is elementary abelian of rank less than p, or $\mu(P) \geq p^2$.*

Proof. The Sylow-p subgroups of S_n for $n < p^2$ are generated by $\lfloor n/p \rfloor$ disjoint p-cycles, and hence are elementary abelian. □

2.1. Groups of order at most p^4.

Proposition 2.2. *Let p be a prime, and let $Q = G/N$ be a distinguished quotient of a p-group G. Then $|Q| > p^3$.*

Proof. Let G be a p-group and $Q = G/N$ a proper quotient of order at most p^3. Suppose first that Q is abelian. Then since any abelian p-group of order p^3 is elementary abelian, or else has a maximal cyclic subgroup, we see from Lemma 1.2 that Q is not distinguished. But if Q is non-abelian then it is extraspecial of order p^3. If Q is not the quaternion group Q_8, then $\mu(G/N) = p^2$; but p^2 is the smallest possible degree of a non-abelian p-group acting faithfully, and so $\mu(G) \geq \mu(G/N)$. If $Q = Q_8$ then $\mu(Q) = 8$, and it is easy to check that no 2-group of degree less than 8 has Q as a quotient. □

It follows immediately from Proposition 2.2 that no p-group of order at most p^4 is exceptional.

2.2. Distinguished quotients.

Throughout this section, we suppose that p is an odd prime. The following result is essentially due to Lemieux [12]. However he mistakenly excludes from his list the group that we have called Q_{81} (called by him G_{28}). Also, one extra group in his list (which he calls G_{29}) is excluded by our arguments.

Proposition 2.3. *Suppose that G is an p-group of order p^5 with a distinguished subgroup N. Then N is cyclic and G/N is isomorphic to one of the following groups.*

$$\begin{aligned}
Q_{81} &= \langle x,y,z \mid x^9 = y^3 = z^3 = 1,\ [x,y] = 1,\ [x,z] = y,\ [y,z] = x^{-3} \rangle \ (p = 3),\\
Q(p) &= \langle x,y,z \mid x^{p^2} = y^p = z^p = [x,y] = [x,z] = 1,\ [y,z] = x^p \rangle,\\
Q_1(p) &= \langle x,y,z \mid x^{p^2} = y^p = 1,\ z^p = x^p,\ [x,y] = 1,\ [x,z] = y,\ [y,z] = x^p \rangle,\\
Q_\alpha(p) &= \langle x,y,z \mid x^{p^2} = y^p = 1,\ z^p = x^{\alpha p},\ [x,y] = 1,\ [x,z] = y,\ [y,z] = x^{\alpha p} \rangle,
\end{aligned}$$

where α is a quadratic non-residue modulo p.

Proof. From Proposition 2.2 we see that G/N has order p^4, and hence $|N| = p$. The groups of order p^4 are well known; a convenient reference for them is [13], who tabulates them with their minimal degrees. For the sake of brevity, we shall not here refer explicitly to individual groups.

Let $Q = G/N$. Then Lemma 1.2 tells us that Q is not elementary abelian, and contains no maximal cyclic subgroup. Since G is non-abelian, we see that $\mu(G) \geq p^2$, and so we must have $\mu(Q) > p^2$. These considerations suffice to rule out all but six of the groups of order p^4 for odd p, aside from the four groups listed in the proposition.

These six possibilities for Q each have the property that $\mu(Q) \leq 2p^2$. We must therefore have $\mu(G) < 2p^2$, and it follows that $\mu(G) = p^2 + cp$ for some $c < p$. Hence $G \cong H \times B$, where H is a non-abelian permutation group acting on p^2 points and B is elementary abelian, possibly trivial. The action of H is a minimal degree representation, and it is transitive. So Theorem 1.1 tells us that H has a unique central subgroup N, which clearly has order p. But now it is clear that N must be the distinguished subgroup of G. This implies that H is exceptional, and so $H = G$.

Now we see that G is a subgroup of $C_p \wr C_p$, and so G has an elementary abelian maximal subgroup V. If $g \in G \setminus V$ then g acts indecomposably on V, and its Jordan form comprises a single unipotent block of size 4. It then follows that the quotient G/N is isomorphic to an extension of a space of dimension 3 by a linear map of order 3 acting indecomposably. In particular, the centre $Z(G/N)$ is cyclic, and so a minimal permutation representation of G/N is transitive by Theorem 1.1. But this is not the case for any of the six possible groups Q under consideration, and so $G/N \ncong Q$, which is a contradiction. □

2.3. **Commutators and p-th powers.** Recall the well known commutator identity

$$[x, yz] = [x, z][x, y]^z. \tag{1}$$

In particular, if G is nilpotent of class 2, then commutators are central, and so $[x, yz] = [x, y][x, z]$.

The following fact is of great importance in what follows.

Proposition 2.4. *Let G be a p-group of nilpotency class at most $p-1$, such that G' has exponent at most p. Then the map $g \mapsto g^p$ is an endomorphism of G.*

Proof. For our purposes we shall require the result only in the case where $p > 3$ and G has class at most 3. In this case, since commutators of weight 2 are central in G, a straightforward induction establishes the following identity:

$$(gh)^a = g^a h^a [h, g]^{\binom{a}{2}} [[h, g], g]^{\binom{a}{3}} [[h, g], h]^{\binom{a}{3}+\binom{a}{2}}.$$

Now since G' has exponent dividing p, it follows for $p > 3$ that $(gh)^p = g^p h^p$.

The more general result stated in the proposition can be shown in a similar manner, using the commutator collection formula [11, Proposition 1.1.32(i)]. □

2.4. **Use of computation and the case $p = 3$.** The classification of exceptional groups for $p = 3$ stands alone since it does not comply with the general classification for $p \geq 5$. Since groups of order 3^5 are so readily dealt with computationally, we do not give full proofs of the results here. The classification of exceptional extensions of

the groups $Q(p)$, $Q_1(p)$ and $Q_\alpha(p)$ for $p = 3$ are presented in Table 1. We remark here that the groups $Q_1(3)$ and Q_{81} possess a common exceptional extension, the group which we have called G_4. Also, $Q_1(3)$ and $Q_\alpha(3)$ possess a common exceptional extension, which we have called G_6. These groups appear with distinct presentations in Table 1, reflecting the particular quotient maps, but we have used a consistent nomenclature.

For the rest of the paper, we assume $p > 3$. Our arguments depend no further on computation; however we have verified our classification of exceptional groups computationally for all primes p up to 19. For calculating minimal degrees we have used the procedure described in [4]. Our computations have been performed using the GAP [6] and Magma [1] computer algebra programs, and have made use of the library of small p-groups in the Small Groups Database of Besche, Eick and O'Brien.

3. Extensions of $Q(p)$

3.1. **First reduction.** Let p be an odd prime, and let Q be $Q(p)$ of order p^4, given by

$$Q = \langle x, y, z \mid x^{p^2} = y^p = z^p = [x, y] = [x, z] = 1, [y, z] = x^p \rangle.$$

A central extension of Q by a group of order p has the form

$$\begin{aligned} G = \langle x, y, z, n \mid n^p = 1, x^{p^2} = n^h, y^p = n^i, z^p = n^j, \\ n \text{ central}, [y, z] = x^p n^k, [x, z] = n^\ell, [x, y] = n^m \rangle \end{aligned} \tag{2}$$

for integers $h, i, j, k, \ell, m \in \{0, \ldots, p-1\}$. The generators of G in this presentation have been so labelled that the images of x, y, z, in the quotient of G by its central subgroup $\langle n \rangle$, correspond to the generators x, y, z of Q. We note that it is immediately clear from the presentation that G has nilpotency class 2, and that its derived group has exponent p. So Proposition 2.4 tells us that the p-power map is an endomorphism of G.

It is clear that a subgroup H of Q not containing the socle $\langle x^p \rangle$ has order at most p, from which it is clear that $\mu(Q) = p^3$. Suppose that $\mu(G) < \mu(Q)$; then it is clear that G can have no element of order p^3. In particular, the generator x has order p^2, and so we must have $h = 0$. In fact we may also assume that $m = 0$, and our next step is to justify this assertion.

Proposition 3.1. *Let $G(i, j, k, \ell, m)$ denote the group with the presentation (2) above, with $h = 0$. Then for all i, j, k, ℓ, m there exist i', j', ℓ' such that $G(i, j, k, \ell, m) \cong G(i', j', k, \ell', 0)$.*

Proof. Let $X = \langle y, z, n \rangle$. Then X has order p^4, and $Z(X) = \langle n, x^p \rangle$ has order p^2. Clearly the quotient $V = X/Z(X)$ is elementary abelian of order p^2. The derived subgroup X' is equal to the cyclic group $\langle x^p n^k \rangle$.

There is a well defined map $\phi : V \longrightarrow \langle n \rangle$ given by

$$\phi(v + Z(X)) = [x, v], \quad v \in X.$$

There is also a map $\vartheta : V \times V \longrightarrow X'$ defined by

$$\vartheta(u + Z(X), v + Z(X)) = [u, v].$$

We may consider V as a vector space, and the cyclic groups $\langle n \rangle$ and X' as copies of the field $\mathbb{F}_p$. It is now apparent, by (1), that ϕ is a linear functional, and ϑ a non-degenerate alternating form, on the space V. If we pick u to be a non-zero element of the kernel of ϕ, then there exists $v \in V$ such that $\vartheta(u, v) = x^p n^k$. Now we may construct a new presentation for the group G, on generators x, y', z', n, where $y' + Z(X) = u$ and $z' + Z(X) = v$. It is straightforward to check that this presentation gives the isomorphism claimed, for some values of i', j', ℓ'. □

In the light of Proposition 3.1, we may drop the parameter m from the notation introduced there, and write $G(i, j, k, \ell)$ for the group with the presentation (2) with $h = m = 0$. We call such a presentation a *distinguished presentation* with parameters (i, j, k, ℓ). The group affording such a presentation is a *candidate extension* of Q; these include all of the exceptional extensions of Q.

3.2. **Structure of a candidate extension of Q.** We record here some observations on the structure of a candidate extension which will be needed later. Throughout this section G is a candidate extension affording a distinguished presentation with generators x, y, z, n and parameters (i, j, k, ℓ).

Proposition 3.2. *G has order p^5 (that is to say, it is a proper central extension of Q).*

Proof. It is clear that $|G|$ is either p^4 or p^5. Consider the group K with presentation

$$K = \langle x, y, z, n \mid x^p = n^p = [x, y] = [x, n] = [y, n] = [z, n] = 1,$$
$$y^p = n^i, z^{p^2} = 1, [y, z] = n^k, [x, z] = n^\ell \rangle.$$

The subgroup L of K generated by its elements x, y, n is abelian of order p^3. It is easy to see that there is an automorphism of L of order p such that $x \mapsto xn^\ell$, $y \mapsto yn^k$, $n \mapsto n$; this holds regardless of whether y has order p or p^2. So K is a semidirect product of L by the group $\langle z \rangle$ of order p^2. The elements n and z^p are central in K. But we observe that the quotient $\overline{K}$ of K by $\langle z^p n^{-j} \rangle$ has a presentation obtained from the presentation for K simply by adding the relation $z^p n^{-j} = 1$, and it can be checked that this is also a presentation for the quotient of G by its subgroup $\langle x^p \rangle$. Now x^p has order p in G, since its image in Q has order p, and it follows easily that $|G| = p|\overline{K}| = |K| = p^2|L| = p^5$ as required. □

Proposition 3.3. *If $\ell \neq 0$ the the centre $Z(G)$ is elementary abelian of size p^2, and is equal to $\langle x^p, n \rangle$. If $\ell = 0$ then $Z(G) = \langle x, n \rangle$, which is isomorphic to $C_p \times C_{p^2}$.*

Proof. It is clear that $A = \langle x^p, n\rangle$ is a central elementary abelian subgroup of order p^2. A set of representatives for the cosets of A in G is $\{x^a y^b z^c \mid a, b, c \in \{0, \dots, p-1\}\}$. Now the element $x^a y^b z^c$ cannot commute with both y and z unless $b = c = 0$, and so $Z(G)$ is contained in $\langle x, n\rangle$. The result follows from the facts that x has order p^2, and that it is central if and only if $\ell = 0$. □

Proposition 3.4. *The subgroup $H = \langle x, y, n\rangle$ of G is an abelian subgroup of order p^4. If $\ell \neq 0$ then H is the unique abelian subgroup of G of order p^4. If $i = 0$ then $H \cong C_{p^2} \times C_p \times C_p$; otherwise $H \cong C_{p^2} \times C_{p^2}$.*

Proof. It is obvious that H has order p^4 and that it is abelian. Let $w \in G \setminus H$. Then $w \in Hz^c$ for some $c \in \{1, \dots, p-1\}$, and it is easy to check that if $\ell \neq 0$ then w centralizes no element of H outside $\langle x, n\rangle$. Since $|\mathrm{Cent}_G(w) \cap H| = p^2$ we must have $|\mathrm{Cent}_G(w)| \leq p^3$, and so w lies in no abelian subgroup of order p^4; it follows that H is the only such subgroup. If $i \neq 0$ then $H = \langle x, y\rangle$ and so $H \cong C_{p^2} \times C_{p^2}$. But if $i = 0$ then $\langle x^p, y, n\rangle$ is elementary abelian of order p^3, and so $H \cong C_{p^2} \times C_p \times C_p$. □

Proposition 3.5. *If $i = j = 0$ then the subgroup of p-th powers in G is $\langle x^p\rangle$ of order p; otherwise it is $\langle x^p, n\rangle$ of order p^2.*

Proof. This is obvious from the presentation for G. □

Proposition 3.6. *If G decomposes as a non-trivial direct product then one of the following statements holds.*

1. *$(i, j, k, \ell) = (0, 0, 0, 0)$. In this case $G \cong Q \times C_p$.*
2. *$\ell = 0 \neq k$. In this case $G \cong C_{p^2} \times E$, where E is an extraspecial group of order p^3. The group E has exponent p if and only $i = j = 0$.*

Proof. Suppose that $G \cong X \times Y$, where X and Y are non-trivial.

We observe first that a p-group of class 2 whose derived group is elementary abelian of rank 2 must have order at least p^5. Since the derived group $(X \times Y)'$ is equal to $X' \times Y'$, and since groups of order p^2 are abelian, it follows that $|G'| = p$. Since the element $x^p n^k$ is a non-trivial element of G', it must generate G'. Now n^ℓ lies in G', and so it follows that $\ell = 0$. This has the consequence, by Proposition 3.3, that $Z(G)$ is isomorphic to $C_{p^2} \times C_p$. Since $Z(X \times Y) = Z(X) \times Z(Y)$, we see that one of these summands—we may suppose it is X without loss of generality—has a centre isomorphic to C_{p^2}.

Suppose first that $|X| = p^4$ and $|Y| = p$. Then G has a central element u of order p which is not a p-th power in G. But since $u \in \langle x^p, n\rangle$, this implies that n is not a p-th power in G, and hence that $i = j = 0$. We see too that G' is contained in X, and so $x^p n^k \in X$. But the central elements of order p in X are those of $\langle x^p\rangle$, and so we must have $k = 0$. So all parameters are 0 in this case, and we see that $G \cong \langle x, y, z\rangle \times \langle n\rangle$, with the first summand being isomorphic to Q.

TABLE 2. Some generator maps with the associated changes of parameters.

Map	(x', y', z', n')	(i', j', k', ℓ')	Conditions
$A(\lambda)$	$(x, y, z, n^{\lambda^{-1}})$	$(\lambda i, \lambda j, \lambda k, \lambda \ell)$	$\lambda \neq 0$
$B(\lambda)$	$(x^\lambda, y^\lambda, z, n)$	$(\lambda i, j, \lambda k, \lambda \ell)$	$\lambda \neq 0$
$C(\lambda)$	$(x^\lambda, y, z^\lambda, n)$	$(i, \lambda j, \lambda k, \lambda^2 \ell)$	$\lambda \neq 0$
D	$(x, y, y^{-j/i} z, n)$	$(i, 0, k, \ell)$	$i \neq 0$
E	(x, z, y^{-1}, n)	$(j, -i, k, 0)$	$\ell = 0$

We cannot have $|X| = p^3$, since X has a centre of order p^2. So the only remaining possibility for the orders of X and Y is that $|X| = p^2$ and $|Y| = p^3$. Now since Y is non-abelian, it is extraspecial. Since $G' = \langle x^p n^k \rangle$ is contained in Y, it is clear that $k \neq 0$. If Y has exponent p then there is no element w of G such that $w^p = x^p n^k$, and it clearly follows that $i = j = 0$.

We conclude the proof by showing that the stated values for the parameters give decomposable groups G. The case $(i, j, k, \ell) = (0, 0, 0, 0)$ is obvious. Suppose that $\ell = 0 \neq k$. Then it is easily checked that G decomposes as

$$G = \langle x \rangle \times \langle x^i y^k, x^j z^k, x^p n^k \rangle.$$

The second summand is extraspecial, and has exponent p if and only if $i = j = 0$. □

3.3. **Parameters.** A candidate extension of Q may have several distinguished presentations with differing parameters. For each isomorphism class of extensions we shall isolate a particular set of parameters. It will be helpful for this purpose to to introduce some terminology. Let (x, y, z, n) and $(x'y'z'n')$ be the generators in two distinguished presentations of a group G, with parameters (i, j, k, l) and (i', j', k', ℓ') respectively. We say that the map $(x, y, z, n) \mapsto (x', y', z', n')$ induces the change of parameters $(i, j, k, l) \mapsto (i', j', k', \ell')$. We shall always treat parameters as elements of $\mathbb{Z}_p$, since they occur in the presentation (2) only as indices to elements of order p.

Some particular generator maps, with the associated change of parameters, are recorded in Table 2. It is a routine matter in each case to verify that the specified values of $(x', y'z', n')$ give generating sets for G, and that they afford a distinguished presentation with the claimed parameters (i', j', k', ℓ').

Lemma 3.7. *Let G be a candidate extension of Q. Let α be a quadratic non-residue modulo p. Then G has a distinguished presentation with parameters in Table 3.*

Proof. Suppose that G has a distinguished presentation P with parameters (i, j, k, ℓ). If $\ell = 0$ then it is a simple matter to transform P into one of P_0, P_1, P_2 or P_3 using the maps from Table 2, for suitable values of λ. Similarly, if $\ell \neq 0$ and $i = 0$ then P can be transformed into one of P_4, P_5, P_6 or P_7 using these maps. Suppose that ℓ and i are both non-zero. Suppose that $k = 0$. There exists an element

TABLE 3. Parameters for candidate extensions of $Q(p)$.

Presentation	(i,j,k,ℓ)	
P_0	$(0,0,0,0)$	
P_1	$(0,0,1,0)$	
P_2	$(1,0,1,0)$	
P_3	$(1,0,0,0)$	
P_4	$(0,0,0,1)$	
P_5	$(0,0,1,1)$	
P_6	$(0,1,0,1)$	
P_7	$(0,1,1,1)$	
$P_8(\lambda)$	$(1,0,0,\lambda)$	$\lambda \in \{1,\alpha\}$
$P_9(\lambda)$	$(1,0,1,\lambda)$	$\lambda \in \mathbb{Z}_p^\times$

$\lambda \in \mathbb{Z}_p^\times$ such that $\lambda^2 \in \{i\ell^{-1}, \alpha i\ell^{-1}\}$, and applying the transformations $C(\lambda)$, $A(i^{-1})$ and D transforms P to $P_8(\lambda)$ for some λ. Otherwise, if $k \neq 0$, then applying the transformations $C(ik^{-1})$, $A(i^{-1})$ and D transforms P to P_9, for $\lambda = i\ell k^{-1}$. □

3.4. **Non-isomorphic presentations.** We shall show that the presentations listed in Lemma 3.7 are irredundant, in that no two of them give rise to isomorphic extensions of Q. The observations collected in the following two propositions contain all that is required for this purpose.

Proposition 3.8. *Let G be a candidate extension.*

(1) *If G has a distinguished presentation with parameter $\ell = 0$ then all of its distinguished presentations have $\ell = 0$.*
(2) *If G has a distinguished presentation with $\ell \neq 0$ and with $i = 0$, then all of its distinguished presentations have $i = 0$.*
(3) *If G has a distinguished presentation with $i = j = 0$, then all of its distinguished presentations have $i = j = 0$.*
(4) *If G has a distinguished presentation with parameter $k = 0$ then all of its distinguished presentations have $k = 0$.*

Proof. The first three parts follow immediately from Propositions 3.3, 3.4 and 3.5. We prove the fourth part here.

If $\ell = 0$ then it is clear from Proposition 3.6 that G has direct factors of order p^2 and p^3 if and only if $k \neq 0$. So we may suppose that $\ell \neq 0$. By Proposition 3.4, G has a unique maximal abelian subgroup H. Suppose that $i = 0$; then H is isomorphic to $C_{p^2} \times C_p \times C_p$. If A is the elementary abelian subgroup of H of order p^3; then A is a characteristic subgroup of G. It is easy to check that $[G, A] = \langle x^p n^k \rangle$, and this lies in the Frattini subgroup of H if and only if $k = 0$. So we suppose instead that $i \neq 0$. Then $H \cong C_{p^2} \times C_{p^2}$. Let A be the elementary abelian subgroup of H of order p^2;

this is the subgroup of p-th powers in H. For a fixed element $w \in G \setminus H$ there is a well defined map $\psi_w : A \longrightarrow A$ given by

$$\psi_w(h^p) = [h, w] \quad h \in H.$$

If A is considered as a vector space over $\mathbb{F}_p$, then ψ_w is linear, and it is not hard to calculate that $\operatorname{tr} \phi_w = 0$ if and only if $k = 0$, irrespective of the choice of w (which may be assumed to be z^t for some $t \neq 0$). This completes the proof. □

The map ψ_w defined in the proof of Proposition 3.8 will play an important part in the analysis of the presentations $P_8(\lambda)$ and $P_9(\lambda)$.

Proposition 3.9. *The groups given by the presentations $P_8(1)$ and $P_8(\alpha)$ are non-isomorphic. The groups given by the presentations $P_9(\lambda)$ and $P_9(\mu)$ are non-isomorphic whenever $\lambda \neq \mu$.*

Proof. Suppose that G has a distinguished presentation with parameters $(1, 0, k, \ell)$, where $\ell \neq 0$. Let A be the subgroup and ψ_w the linear map $A \longrightarrow A$, which are defined in the proof of Proposition 3.8. It is straightforward to calculate that $\operatorname{tr} \phi_w = \tau k$ and $\det \phi_w = -\tau^2 \ell$, for some $\tau \in \mathbb{F}_p^\times$ which depends on the choice of w. It is clear from the expression for the determinant that whether or not ℓ is a quadratic residue modulo p is an invariant of the group. Furthermore, if we suppose that $k = 1$ then the value of τ is determined, and so ℓ itself is an invariant. The proposition follows immediately from these observations. □

Lemma 3.10. *Let G and H be candidate extensions with distinguished presentations from Table 3. If their parameters are not the same, then G and H are not isomorphic.*

Proof. This follows from Propositions 3.8 and 3.9. □

3.5. **Exceptional extensions.**

Lemma 3.11. *Let G be a candidate extension of Q. Then G is exceptional (that is, $\mu(G) < \mu(Q)$) if and only if G has two subgroups K_1 and K_2, each of order p^3, such that $K_1 \cap K_2$ has order p and is non-central in G.*

Proof. Since $Z(G)$ has rank 2, Theorem 1.1 tells us that a faithful permutation representation of G of minial degree has exactly two orbits. Let K_1 and K_2 be two non-conjugate point stabilizers. Then $\mu(G) = |G : K_1||G : K_2|$. If G us exceptional, then since $\mu(Q) = p^3$, we see that K_1 and K_2 must each have order at least p^3. So the intersection $Y = K_1 \cap K_2$ is non-trivial. Since the representation of G is faithful, it is clear that $Y \cap Z(G)$ is trivial. Since all p-th powers in G lie in $Z(G)$ it follows that Y has exponent p. Now YV has order $p^2|Y|$, and since it is clear that G has no elementary abelian subgroup of rank 4, we must have $|Y| = p$. It follows that $|K_1| = |K_2| = p^3$.

For the converse, suppose that K_1 and K_2 are subgroups of G of order p^3 such that $Y = K_1 \cap K_2$ is a non-central subgroup of order p. Then Y is not normal in G, and the permutation representation of G on the cosets of K_1 and K_2 is faithful. It follows that $\mu(G) \leq 2p^2$, and so G is exceptional. □

Proposition 3.12. *The candidate extension with presentation P_0 is not exceptional. The candidate extensions with presentations P_1 and P_2 are exceptional.*

Proof. These are the presentations which give rise to decomposable extensions, by Proposition 3.6. The presentation P_0 is afforded by $Q \times C_p$, which is clearly not exceptional. Each of P_1 and P_2 gives a group $G \cong C_{p^2} \times E$, where E is extraspecial of order p^3. Since both of the extraspecial groups of order p^3 have permutation representations of degree p^2, we see that $\mu(G) = 2p^2$ in each case, and so G is exceptional. □

The groups with presentations P_1 and P_2 appear in Table 1 as E_1 and E_2 respectively.

Proposition 3.13. *The candidate extension with presentation P_3 is not exceptional.*

Proof. Let G have presentation P_3. Then x is central, and $G' = \langle x^p \rangle$. Suppose that K is a subgroup of order p^3, such that $x^p \notin K$. Then K is abelian, and $G = K\langle x \rangle$. But G is not abelian, which is a contradiction. Thus every subgroup of G of order p^3 contains the central element x^p, and so by Lemma 3.11 G is not exceptional. □

Proposition 3.14. *The candidate extensions with presentations P_4 and P_6 are not exceptional.*

Proof. These are presentations for which $\ell \neq 0$ and $i = 0$. So by Proposition 3.4 the candidate subgroup G has an abelian subgroup $H = \langle x, y, n \rangle$ which has the structure $C_{p^2} \times C_p \times C_p$. Suppose that K is a subgroup of G of order p^3 which does not contain x^p. Then it is easy to see that $Y = K \cap H$ is elementary abelian of order p^2. Now Y contains an element of $H \setminus V$, whose centralizer in G is H. It follows that K is not abelian. But since $k = 0$ for these presentations, we see that $[Y, G] = \langle x^p \rangle$, and so $x^p \in K$, a contradiction. Hence the central element x^p lies in every subgroup of G of order p^3. □

Proposition 3.15. *The candidate extensions with presentations P_5 and P_7 are exceptional.*

Proof. It is easy to check that the subgroups $K_1 = \langle x, y \rangle$ and $K_2 = \langle x^p n^k, y, z \rangle$ satisfy the conditions stated in Lemma 3.11. □

The groups with presentations P_5 and P_7 appear in Table 1 as E_3 and E_4 respectively.

Proposition 3.16. *The candidate extension with presentation $P_8(\lambda)$ is exceptional if $\lambda = 1$, but not if $\lambda = \alpha$. The candidate extension with presentation $P_9(\lambda)$ is exceptional if and only if $1 + 4\lambda$ is a non-zero quadratic residue modulo p.*

Proof. These are the cases for which the parameters i and ℓ are non-zero. Let H be the subgroup form Proposition 3.4, and let $w \in G \setminus H$. We show that G is exceptional if and only if the map ψ_w defined in the proof of Proposition 3.8 is diagonalizable. (This does not depend on the choice of w, which affects ψ_w only up to scalar multiplication.)

Let G be a candidate extension with one of the stated presentations. Let K_1 and K_2 be subgroups of G of order p^3 whose intersection has order p and is non-central. Since H has the structure $C_{p^2} \times C_{p^2}$, we see that K_1 and K_2 cannot have exponent p. It follows that $K_1 \cap H$ and $K_2 \cap H$ are cyclic of order p. Let u_1 generate $K_1 \cap H$ and let u_2 generate $K_2 \cap H$. Then u_1^p and u_2^p are linearly independent elements of V, considered as a vector space. Choose w to be a generator of $K_1 \cap K_2$. Note that $w \notin H$, since the elements of order p in H are central in G. Now we observe that both u_1^p and u_2^p must be eigenvectors of the map ψ_w.

Conversely, suppose that $w \in G \setminus H$, and suppose that u_1 and u_2 are elements of H such that u_1^p and u_2^p are linearly independent eigenvectors of ψ_w. Then it is easy to check that the subgroups $K_1 = \langle u_1, w \rangle$ and $K_2 = \langle u_2, w \rangle$ satisfy the conditions of Lemma 3.11, and so G is exceptional.

Since the map ψ_w is not scalar for any $w \in G \setminus H$, it follows that G is exceptional if and only if the characteristic polynomial of ψ_w has distinct roots in $\mathbb{F}_p$. Taking $w = z$, we see that the characteristic polynomial is $X^2 - kX - \ell$, which has distinct roots if and only if $k^2 + 4\ell$ is a non-zero square in $\mathbb{F}_p$. Now substituting the appropriate values for k and ℓ establishes the proposition in all cases. □

The group with presentations $P_8(1)$ appears in Table 1 as E_5. For some values of λ the group with presentation $P_9(\lambda)$ is exceptional, and appears there as $E_6(\lambda)$, with the appropriate conditions on λ.

3.6. **Counting exceptional extensions.**

Proposition 3.17. *The number of groups G which are exceptional extensions of Q, up to isomorphism, is $(p + 7)/2$.*

Proof. There is an exceptional extension given by the presentation $P_9(\lambda)$ whenever $\lambda \neq 0$ and $1 + 4\lambda$ is a quadratic residue for p. Every quadratic residue for p except 1 is expressible as $1 + 4\lambda$ for some non-zero λ, and so there are $(p - 3)/2$ such presentations. The five groups with presentations P_1, P_2, P_6, P_7 and $P_8(1)$ are also exceptional, giving the total stated in the proposition. □

4. Extensions of $Q_1(p)$ and $Q_\alpha(p)$

Let p be a prime greater than 3, and let Q_ζ be the group of order p^4 given by

$$Q_\zeta = \langle x, y, z \mid x^{p^2} = y^p = [x, y] = 1, z^p = x^{\zeta p}, [x, z] = y, [y, z] = x^{\zeta p} \rangle,$$

where ζ is an integer coprime with p. The isomorphism class of Q_ζ depends only on whether or not ζ is a quadratic residue modulo p. The particular values $\zeta = 1$ and $\zeta = \alpha$ give the presentations defining the groups $Q_1(p)$ and $Q_\alpha(p)$ respectively.

A central extension of Q_ζ by a group of order p has the form

$$\begin{aligned} G = \langle x, y, z, n \mid n^p = 1, x^{p^2} = n^h, y^p = n^i, z^p = x^{\zeta p} n^j, \ n \text{ central}, \\ [x, z] = y n^\ell, [x, y] = n^{-m}, [y, z] = x^{\zeta p} n^{\zeta m + k} \rangle \end{aligned} \tag{3}$$

for integers $h, i, j, k, \ell, m \in \{0, \ldots, p-1\}$. The generators of G in this presentation have been so labelled that the images of x, y, z, in the quotient of G by its central subgroup $\langle n \rangle$, correspond to the generators x, y, z of Q_ζ; the exponents of n have been chosen for convenience at a later point of the argument.

It is clear that a subgroup H of Q_ζ not containing the socle $\langle x^p \rangle$ has order at most p, from which it is clear that $\mu(Q_\zeta) = p^3$. Suppose that $\mu(G) < \mu(Q_\zeta)$; then it is clear that G can have no element of order p^3. In particular, the generator x has order p^2, and so we must have $h = 0$.

It is easy to see that the centre Z of G is $\langle x^p, n \rangle$, and that G/Z is an extraspecial group with centre $\langle yZ \rangle$. Any subgroup of G/Z of order greater than p contains yZ, and it follows easily that any subgroup of Z of order greater than p^2 contains y^p. So n^i is contained in the kernel of any permutation representation of G of degree less than p^3. Hence if G is exceptional, then $i = 0$.

Now we observe that G has nilpotency class 3 and (since $h = i = 0$) that its derived subgroup has exponent at most p. So Proposition 2.4 applies, and we have that the p-power map on G is an endomorphism.

We may also suppose that $\ell = 0$, simply by replacing the generator y with yn^ℓ. Thus we may drop three parameters from our notation, and write $G(j, k, m)$ for the group with the presentation (3) with $h = i = \ell = 0$. These are our *distinguished presentations* in this case, with parameters (j, k, m). We call groups affording such a presentation candidate extensions of Q_ζ; these include all of the exceptional extensions of Q_ζ.

Proposition 4.1. *A candidate extension G of Q_ζ has order p^5.*

Proof. Consider the group

$$W = \langle x, y, n \mid x^p = y^p = n^p = [x, n] = [y, n] = 1, [x, y] = n^{-m} \rangle.$$

It is clear that W has order p^3 and exponent p. We observe that $[xy, yn^{\zeta m + k}] = [x, y]$ in W, and so there exists an automorphism z of W such that $x^z = xy$ and $y^z = yn^{\zeta m + k}$.

TABLE 4. Some generator maps with the associated changes of parameters.

Map	(x', y', z', n')	(j', k', m')	Conditions
$A(\lambda)$	$(x, y, z, n^{\lambda^{-1}})$	$(\lambda j, \lambda k, \lambda m)$	$\lambda \neq 0$
$B(\lambda)$	$(x^\lambda, y^\lambda n^{m\binom{\lambda}{2}}, x^{\zeta(\lambda-1)}z, n)$	$(j, \lambda k, \lambda^2 m)$	$\lambda \neq 0$

It is easy to check that $x^{z^a} = xy^a n^{\binom{a}{2}}$ for any integer a, and it follows easily that z has order p. Now the extension of W by the automorphism z has the presentation

$$\langle x, y, z, n | x^p = y^p = z^p = n^p = 1,\ n \text{ central}, [x, y] = n^{-m}, [x, z] = y, [y, z] = n^{\zeta m+k} \rangle,$$

and we see that this is the quotient of G by the subgroup $\langle x^p \rangle$. Since x^p is non-trivial in Q_ζ, it is non-trivial in G, and so $|G| = p|W| = p^5$ as required. □

4.1. **Parameters.** If (x, y, z, n) and $(x'y'z'n')$ are the generators in two distinguished presentations of a group G, with parameters (j, k, m) and (j', k', m') respectively, then we say that the map $(x, y, z, n) \mapsto (x', y', z'n,')$ induces the change of parameters $(j, k, m) \mapsto (j', k', m')$.

Some particular generator maps, with the associated change of parameters, are recorded in Table 4. It is a routine matter to verify that the map $A(\lambda)$ gives a distinguished presentation with the parameters claimed. For $B(\lambda)$, we observe that

$$[x^\lambda, x^{\zeta(\lambda-1)}z] = [x^\lambda, z] = y^\lambda n^{m\binom{\lambda}{2}},$$

with the second equality given by an easy induction. So we have $[x', z'] = y'$, and it is straightforward to check that the other relations of a distinguished presentation are satisfied with the parameters stated.

Proposition 4.2. *Let G be a candidate extension. If G has a distinguished presentation with one of its parameters j, k, m equal to 0, then all of its distinguished presentations have that parameter equal to 0.*

Proof. Let G have a distinguished presentation with parameters j, k, m. We observe that if $j = 0$ then the image J of the endomorphism $g \mapsto g^p$ is the subgroup $\langle x^p \rangle$ of order p, whereas if $j \neq 0$ then this image coincides with the centre Z, of order p^2. If $m = 0$ then the derived group G' is $\langle y, x^{\zeta p} n^k \rangle$ of order p^2, whereas if $m \neq 0$ then $G' = \langle y, n, x^p \rangle$ of order p^3. Clearly these are invariants of the group G.

For the parameter k, let w be any non-central element of G contained in the derived group G'. (The generator y in any distinguished presentation for G is such an element.) We consider separately the cases that $j = 0$ and that $j \neq 0$. When $j = 0$, the image J of the p-power endomorphism is a central subgroup of order p. The map $G \longrightarrow Z/J$ given by $g \mapsto [w, g]J$ is a homomorphism with kernel $\langle x^{\zeta m+k} z^{-m}, y, x^p, n \rangle$. This kernel is independent of the element w, and we observe that it has exponent p

if and only if the first of the given generators has order p; this occurs if and only if $k = 0$.

Suppose next that $j \neq 0$. By applying the generator map $A(1/j)$ from Table 4, we see that we may assume that $j = 1$. We have $J = Z$, and so every central element has a p-th root in G. We observe that the map $\psi_w : Z \longrightarrow Z$ given by $\psi_w(u^p) = [w, u]$ is a well defined homomorphism, since w is centralized by the kernel $\langle y, x^p, n\rangle$ of the p-power endomorphism. We may consider Z as a 2-dimensional vector space over $\mathbb{F}_p$, and now the map ψ_w becomes a linear transformation of Z. Let t be such that $w \in y^t Z$. Then with respect to the basis (x^p, n) for Z, the map ψ_w has the matrix

$$M_t = t \begin{pmatrix} 0 & \zeta \\ m & k \end{pmatrix}.$$

Now this map has trace 0 if and only if $k = 0$, regardless of the choice of w. □

The map ϕ_w plays a similar role here as in Section 3; it will be essential to the analysis of the presentations $P_6(\lambda)$ $P_7(\lambda)$.

Proposition 4.3. *Let G have two distinguished presentations, each with parameter $j = 1$. Let m_1 and m_2 be the values for the parameter m in these presentations. Then $\left(\frac{m_1}{p}\right) = \left(\frac{m_2}{p}\right)$, where $\left(\frac{a}{p}\right)$ is the Legendre symbol.*

Proof. By Proposition 4.2 we may suppose that m_1 and m_2 are both non-zero. Since $j = 1$, we may construct the transformation ψ_w from the proof of Proposition 4.2. We see that $\det \psi_w = -t^2\zeta m$, which is independent of w modulo squares in $\mathbb{Z}_p^\times$. □

Proposition 4.4. *Let G have two distinguished presentations, each with parameter $j = 1$, and with the same non-zero value for the parameter m. Let k_1 and k_2 be the values for the parameter k in these presentations. Then $k_2 = \pm k_1$.*

Proof. Since $j = 1$, we can construct the transformation ψ_w from the proof of Proposition 4.2. Now we see that

$$\frac{(\operatorname{tr} \psi_w)^2}{\det \psi_w} = -\frac{k^2}{\zeta m},$$

and so we must have $k_1^2 = k_2^2$. □

Lemma 4.5. *Let G be a candidate extension of Q_ζ. Let α be a quadratic non-residue modulo p. Then G has a distinguished presentation with parameters in Table 5.*

Proof. It follows from Propositions 4.2, 4.3 and 4.4 that no two of the sets of parameters listed give rise to isomorphic groups. It is a routine matter to show that any set of parameters may be transformed into one of the listed sets by means of the generator maps listed in Table 4. □

TABLE 5. Parameters for candidate extensions of Q_ζ.

Presentation	(j,k,m)	
P_0	$(0,0,0)$	
P_1	$(0,0,1)$	
P_2	$(0,1,0)$	
P_3	$(1,0,0)$	
P_4	$(0,1,1)$	
P_5	$(1,1,0)$	
$P_6(\lambda)$	$(1,\lambda,1)$	$\lambda \in \{0,\dots,(p-1)/2\}$
$P_7(\lambda)$	$(1,\lambda,\alpha)$	$\lambda \in \{0,\dots,(p-1)/2\}$

4.2. **Exceptional extensions.**

Proposition 4.6. *Let G be a candidate extension with parameter $j = 0$. Then G is exceptional if and only if parameter $k \neq 0$.*

Proof. The group G is exceptional if and only if has subgroups H_1 and H_2, each of order p^3, such that the intersection $H_1 \cap H_2 \cap Z$ is trivial.

The image J of the p-power endomorphism is generated by x^p. It follows that any subgroup of G not containing x^p has exponent p. Now the kernel of the p-power endomorphism is $K = \langle y, x^{-\zeta}z, x^p, n\rangle$, which factorizes as

$$\langle y, x^{-\zeta}z, x^{\zeta p}n^k\rangle \times \langle n\rangle.$$

Let L be the factor $\langle y, x^{-\zeta}z, x^{\zeta p}n^k\rangle$. Then L is extraspecial, with centre $\langle x^{\zeta p}n^k\rangle$. Let H be a subgroup of K of order p^3. Then $|H \cap L| \geq p^2$, and so $x^{\zeta p}n^k \in H$. It follows that if $k = 0$, then every subgroup of G of order p^3 contains the central element x^p, and hence G is not exceptional.

Conversely, if $k \neq 0$, then it is easily checked that the subgroups

$$H_1 = \langle y, x^{-\zeta}z, x^{\zeta p}n^k\rangle, \quad H_2 = \langle x^{-(\zeta m+k)}z^m, y\rangle,$$

both have order p^3, and their intersection is the non-central subgroup $\langle y\rangle$. Hence G is exceptional in this case. □

Proposition 4.6 tells is that the group with presentations P_2 and P_4 are exceptional. Taking ζ to be either 1 or α, these groups appear in Table 1 as $F_1^{(\zeta)}$ and $F_2^{(\zeta)}$ respectively.

Proposition 4.7. *Let G be a candidate extension with parameter $j = 1$, and parameters k, m. Then G is exceptional if and only if $k^2 + 4\zeta m$ is a non-zero quadratic residue modulo p.*

Proof. Let H_1 and H_2 be subgroups of G of order p^3, such that $H_1 \cap H_2 \cap Z$ is trivial. It is clear that $H_1 \cap H_2$ has exponent p (since the image J of the p-power endomorphism

is central). Since $j \neq 0$, the kernel of the p-power endomorphism is $\langle Z, y\rangle$, and so $H_1 \cap H_2$ contains an element $w \in yZ$. We may now construct the map ψ_w from the proof of Proposition 4.2. (The value of t is quite unimportant, but as it happens our choice of w ensures that $t = 1$.)

It is clear, since any subgroup of G of order p^3 intersects the centre non-trivially, that each of $H_1 \cap Z$ and $H_2 \cap Z$ must have order p. Let these intersections be generated by u_1 and u_2 respectively. In particular, neither H_1 nor H_2 can be contained in the kernel of the p-power endomorphism, and so each has exponent p^2. It follows that u_1 and u_2 have p-th roots $v_1 \in H_1$ and $v_2 \in H_2$ respectively. It follows from the definition of the map ψ_w that $\psi_w(u_1) = [w, v_1] \in H_1 \cap Z$, and $\psi_w(u_2) = [w, v_2] \in H_2 \cap Z$. Hence each of u_1 and u_2 is an eigenvector of the map ψ_w.

As a converse, we note that if ψ_w has linearly independent eigenvectors u_1 and u_2, with p-th roots v_1 and v_2 in G respectively, then the subgroups $H_1 = \langle v_1, w\rangle$ and $H_2 = \langle v_2, w\rangle$ both have order p^3, and their intersection $\langle w\rangle$ is non-central. Hence G is exceptional if and only if ψ_w is diagonalizable. The proposition now follows from the observations that the discriminant of ψ_w is $k^2 + 4\zeta m$, and that since ψ_w is not scalar, a discriminant of 0 implies that ψ_w is not diagonalizable. □

Let $\zeta \in \{1, \alpha\}$. The presentation P_5 gives an exceptional group, which appears in Table 1 as $F_3^{(\zeta)}$. For suitable values of λ the groups with presentations $P_6(\lambda)$ or $P_7(\lambda)$ are exceptional; these appear as $F_4^{(\zeta)}(\lambda)$ and $F_5^{(\zeta)}(\lambda)$ respectively, with the appropriate conditions on λ.

4.3. **Counting exceptional extensions.**

Proposition 4.8. *The number of groups G which are exceptional extensions of Q_ζ, up to isomorphism, is $(p + 5)/2$.*

Proof. From Propositions 4.6 and 4.7 we see that the presentations P_2, P_4 and P_5 give exceptional extensions, whereas P_0, P_1 and P_3 do not. It remains to deal with the presentations $P_6(\lambda)$ and $P_7(\lambda)$.

Working in the set $\mathbb{Z}_p$ of integers modulo p, let t be non-zero, and let

$$S_t := \{(r, \lambda) \mid r \neq 0, t = r^2 - \lambda^2\}.$$

Then it is clear that $|S_t|$ is the number of (ordered) factorizations of t as a product of distinct elements of $\mathbb{Z}_p$. This number is $p - 3$ if t is a square, and $p - 1$ otherwise. Now define

$$T = \{(\mu, r, \lambda) \mid \mu \in \{1, \alpha\}, r \neq 0, r^2 - \lambda^2 = 4\zeta\mu\}.$$

Since 4ζ and $4\zeta\alpha$ are non-zero, and exactly one of them is a square, we see that $|T| = 2p - 4$. Each element of T yields a distinguished presentation with parameters $(j, k, m) = (1, \pm\lambda, \mu)$ (where the sign in the second parameter is chosen to put it in the range $\{0, \ldots, \frac{p-1}{2}\}$). Since the discriminant $k^2 + 4\zeta m$ for this presentation is r^2, Proposition 4.7 tells us that the corresponding extension is exceptional; moreover it

is clear that all the exceptional extensions with presentations $P_6(\lambda)$ or $P_7(\lambda)$ arise in this way. Now two elements (μ, r, λ) and (μ', r', λ') of T yield the same presentation if and only if $\mu = \mu'$, $r = \pm r'$ and $\lambda = \pm\lambda'$. Exactly two elements of T have $\lambda = 0$. So the number of exceptional extensions arising from T is $1 + (|T| - 2)/4$, which is $(p-1)/2$. Together with the three exceptional extensions already found, this makes up the number $(p+5)/2$ stated in the proposition. □

4.4. **Isomorphisms of exceptional extensions of $Q_1(p)$ and $Q_\alpha(p)$.** Recall that α is a quadratic non-residue modulo p. In this section we establish the following fact.

Proposition 4.9. *Let G be a group of order p^5. Then G is an exceptional extension of Q_α if and only if it is an exceptional extension of Q_1.*

We show directly that every exceptional extension of Q_α is isomorphic to an exceptional extension of Q_1. Since Q_α and Q_1 have the same number of exceptional extensions by Proposition 4.8, it follows that the converse also holds.

Proposition 4.10. *Let G be an exceptional extension of Q_α affording a distinguished presentation with parameters (j, k, m), where $j = 1$. Then G is an exceptional extension of Q_1.*

Proof. Pick $w \in G$ such that $w \notin Z(G)$ and $w^p = 1$. Then the map ψ_w is diagonalizable by Proposition 4.7. So there exist elements u and v of $Z(G)$ such that $\psi_w(u) = u^\gamma$ and $\psi_w(v) = v^\delta$, for some integers γ, δ. Let $s^p = u$ and $t^p = v$. Then $[s,t] \in w^i Z(G)$ for some i coprime with p. If $ij \cong 1 \bmod p$ then it is easy to check that $[s^j, t] \in wZ(G)$. Replacing s with s^j, and then replacing w with $[s,t]$ (which does not effect the map ψ_w), we see that G has a presentation

$$G = \langle s, t, w | s^{p^2} = t^{p^2} = w^p = 1, [s,t] = w, [w,s] = s^{p\gamma}, [w,t] = t^{p\delta} \rangle.$$

This presentation is dependent only on the eigenvalues of the map ψ_w. But from the matrix for ψ_w given in the proof of Proposition 4.2, we see that these depend on α only insofar as they depend on αm. So if we take a distinguished presentation with parameters $(1, k, \alpha m)$ for an extension E of Q_1, then it is clear that $E \cong G$. It remains only to note that E is an exceptional extension of Q_1 by Proposition 4.7. □

There are two exceptional extensions of Q_α not covered by Proposition 4.10, given by presentations P_2 and P_4 in Table 5.

Proposition 4.11. *The extension of Q_α with presentation P_2 is an exceptional extension of Q_1.*

Proof. Let x, y, z, n be the generators of a group G given by the presentation P_2. Define elements $\tilde{z} = x^{1-\alpha} z$ and $\tilde{n} = x^{(\alpha-1)p} n^k$. It is easy to check that in terms of the

generators $x, y, \tilde{z}, \tilde{n}$, the group G affords the presentation

$$G = \langle x, y, \tilde{z}, \tilde{n} \mid \tilde{n}^p = x^{p^2} = y^p = 1, \tilde{z}^p = x^p, [x, \tilde{z}] = y, [x, y] = 1,$$
$$[y, \tilde{z}] = x^p n, [x, \tilde{n}] = [y, \tilde{n}] = [\tilde{z}, \tilde{n}] = 1\rangle.$$

This is a distinguished presentation with parameters $(0, 1, 0)$ for an extension of Q_1, and as such is exceptional by Proposition 4.6. □

Proposition 4.12. *The extension of Q_α with presentation P_4 is an exceptional extension of Q_1*

Proof. There exist elements t and b of C_p such that $t^2 - b^2 = 4\alpha$. Define

$$a = \frac{t - (2\alpha + 1)b}{2}, \quad c = -(\alpha + 1)b, \quad d = \frac{t + (2\alpha + 1)b}{2\alpha}.$$

It is straightforward to check that these values satisfy the following equations:

$$a + \alpha b = c + \alpha d = \frac{t - b}{2} \tag{4}$$

$$ad - bc = 1 \tag{5}$$

Let G be given by a distinguished presentation P_4. Define elements

$$\tilde{x} = x^a z^b, \quad \tilde{z} = x^c z^d, \quad \tilde{y} = [x, z], \quad \tilde{n} = x^{pb} n^{d-b}.$$

Note that $\tilde{z}^p = \tilde{x}^p = x^{p(t-b)/2}$ by (4). Since $t \neq b$, it is clear that $\tilde{x}$ and $\tilde{z}$ have order p^2. Furthermore, it follows from (5) that $\tilde{y} \in yZ(G)$, and so $[\tilde{y}, g] = [y, g]$ for all $g \in G$. We also note that since 4α is a quadratic non-residue modulo p, we must have $b \neq 0$, and so $\tilde{n}$ is a central element of order p. It is straightforward to check the identities

$$[\tilde{x}, \tilde{y}] = \tilde{n}^{-\alpha}, \quad [\tilde{y}, \tilde{z}] = \tilde{x}^p \tilde{n}^{\alpha+1}.$$

With respect to the generators $\tilde{x}, \tilde{y}, \tilde{z}, \tilde{n}$, the group G affords the presentation

$$G = \langle \tilde{x}, \tilde{y}, \tilde{z}, \tilde{n} \mid \tilde{n}^p = \tilde{x}^{p^2} = \tilde{y}^p = 1, \tilde{z}^p = \tilde{x}^p, [\tilde{x}, \tilde{z}] = \tilde{y}, [\tilde{x}, \tilde{y}] = \tilde{n}^{-\alpha},$$
$$[\tilde{y}, \tilde{z}] = \tilde{x}^p \tilde{n}^{\alpha+1}, [\tilde{x}, \tilde{n}] = [\tilde{y}, \tilde{n}] = [\tilde{z}, \tilde{n}] = 1\rangle.$$

This is a distinguished presentation with parameters $(0, 1, \alpha)$ for an extension of Q_1, and as such is exceptional by Proposition 4.6. □

In the nomenclature of Table 1, we have that $F_1^{(1)} \cong F_1^{(\alpha)}$, $F_2^{(1)} \cong F_2^{(\alpha)}$, and $F_3^{(1)} \cong F_3^{(\alpha)}$. Each group in $\{F_4^{(1)}(\lambda)\}$ is isomorphic with a group in $\{F_5^{(\alpha)}(\lambda)\}$, while each group in $\{F_5^{(1)}(\lambda)\}$ is isomorphic with a group in $\{F_4^{(\alpha)}(\lambda)\}$.

4.5. **The number of exceptional groups of order p^5.** It remains only to marshal the various results which together establish Theorem 2. For $p = 2$, the result is from [3]. For $p = 3$, it is given by the computation described in Section 2.4. For larger primes it follows easily from Propositions 3.17 and 4.8 together with Proposition 4.9.

References

[1] Wieb Bosma, John Cannon, and Catherine Playoust, The Magma algebra system. I. The user language, *J. Symbolic Comput.* **24** (1997), 235–265.

[2] Kenneth S. Brown, *Cohomology of groups*, Graduate Texts in Mathematics 87, Springer, New York, 1982.

[3] David Easdown and Cheryl E. Praeger, On minimal faithful permutation representations of finite groups, *Bull. Austral. Math. Soc.* **38** (1988) no. 2, 207–220.

[4] Ben Elias, Lior Silberman and Ramin Takloo-Bighash, Minimal Permutation Representations of Nilpotent Groups, *Exp. Math.* **19** (2010) no. 1, 121–128.

[5] Clara Franchi, On minimal permutations representations of abelian quotients of finite groups, *Bull. Aust. Math. Soc.* **84** (2011) no. 3, 408–413.

[6] The GAP Group, *GAP—Groups, Algorithms, and Programming, Version 4.7.5*, 2014. `http://www.gap-system.org`

[7] Derek F. Holt and Jacqueline Walton, Representing the quotient groups of a finite permutation group, *J. Algebra* **248** (2002) no. 1, 307–333.

[8] D. L. Johnson, Minimal permutation representations of finite groups, *Amer. J. Math.* **93** (1971), 857–866.

[9] L. G. Kovács and Cheryl E. Praeger, Finite permutation groups with large abelian quotients, *Pacific J. Math.* **136** (1989) no. 2, 283–292.

[10] L. G. Kovács and Cheryl E. Praeger, On minimal faithful permutation representations of finite groups, *Bull. Austral. Math. Soc.* **62** (2000) no. 2, 311–317.

[11] C. R. Leedham-Green and S. McKay, *The structure of groups of prime power order*, London Mathematical Monographs New Series 27, Oxford Science Publications, Oxford University Press, Oxford, 2002.

[12] Stéphane R. Lemieux, *Minimal degree of faithful permutation representations of finite groups*, MSc. thesis, Carleton University, Ottawa, 1999.

[13] Stéphane Lemieux, Finite exceptional p-groups of small order, *Comm. Algebra* **35** (2007) no. 6, 1890–1894.

[14] Peter M. Neumann, Some algorithms for computing with finite permutation groups, *Proceedings of Groups–St Andrews 1985*, 59–92, London Math. Soc. Lecture Note Ser. 121, Cambridge Univ. Press, Cambridge, 1986.

[15] Neil Saunders, Minimal faithful permutation degrees of finite groups, *Austral. Math. Soc. Gaz.* **35** (2008) no. 5, 332–338.

[16] Neil Saunders, Minimal faithful permutation degrees for irreducible Coxeter groups and binary polyhedral groups, *J. Group Theory* **17** (2014) no. 5, 805–832.

Department of Mathematics, Imperial College London, South Kensington Campus, London SW7 2AZ, United Kingdom

E-mail address: `j.britnell@imperial.ac.uk`

Department of Mathematics, City University London, Northampton Square, London EC1V 0HB, United Kingdom

E-mail address: `neil.saunders@city.ac.uk`

Heilbronn Institute for Mathematical Research, University of Bristol, School of Mathematics, University Walk, Bristol BS8 1TW, United Kingdom

E-mail address: `tony.skyner@bristol.ac.uk`