Journal of Symbolic Computation 108 (2022) 23–40

Contents lists available at ScienceDirect

Journal of Symbolic Computation

www.elsevier.com/locate/jsc

Groups whose orders factorise into at most four primes ☆

Handwritten corrections:

× Table 4, Cluster 6: one typo
Cluster 7: two typos

Heiko Dietrich [a], Bettina Eick [b], Xueyu Pan [a]

[a] School of Mathematics, Monash University, VIC 3800, Australia
[b] Institut Computational Mathematics, Technische Universität Braunschweig, Germany

A R T I C L E   I N F O

Article history:
Received 4 December 2020
Received in revised form 30 April 2021
Accepted 30 April 2021
Available online 13 May 2021

Dedicated to the memories of John H. Conway and Peter M. Neumann

Keywords:
Group determination
Group enumeration
SmallGroup database

A B S T R A C T

The groups whose orders factorise into at most four primes have been described (up to isomorphism) in various papers. Given such an order n, this paper exhibits a new explicit and compact determination of the isomorphism types of the groups of order n together with effective algorithms to enumerate, construct, and identify these groups. The algorithms are implemented for the computer algebra system GAP.

1. Introduction

It is a major theme in group theory to enumerate and construct all groups of a given order up to isomorphism. This has been initiated by Cayley (1854) who determined the groups of order at most 6. Many publications have followed Cayley's work; a survey is given in Besche et al. (2002). The enumeration of the (isomorphism types of) groups of order n is a related problem: The number $\mathcal{N}(n)$ of (isomorphism types of) groups of order n is known for all $n \leqslant 2000$, see Besche et al. (2002), and for most n at most 20000, see Eick et al. (2017), but no closed formula is known for general n. We refer to the book of Blackburn et al. (2007) and the papers by Conway et al. (2008), Eick and Moede (2018) for more information on group enumeration.

☆ The first author was supported by an Australian Research Council grant DP190100317. The third author was supported by an Australian RTP scholarship; part of this work is based on the MPhil thesis of the third author, see Pan (2021). The authors thank Mike Newman for various helpful discussions.

E-mail addresses: heiko.dietrich@monash.edu (H. Dietrich), beick@tu-bs.de (B. Eick), xpan.eileen@gmail.com (X. Pan).

https://doi.org/10.1016/j.jsc.2021.04.005
0747-7171/© 2021 Elsevier Ltd. All rights reserved.

Modern computer algebra systems such as GAP (GAP, Version 4.11.0) and Magma (Bosma et al., 1997) contain (different though overlapping parts of) a database of groups of "small order": the SmallGroups Library Besche et al.. Given a "small" order n, this library contains a list of isomorphism type representatives for the groups of order n. The library also contains an identification function for these groups: given a group G, one can determine its ID (n, i), meaning that G is isomorphic to the i-th group in the database list of groups of order n. The SmallGroups Library has become highly popular in the research community. It is therefore an important topic in computational group theory to extend this library.

Our aim here is to present a new extension to the SmallGroups Library in form of the GAP package `SOTGrps` (Pan, 2021): we describe effective construction and identification methods for the groups of order n, where n factorises into at most four primes. This is underpinned by a new explicit enumeration and a new compact determination of the groups of such orders.

If n factorises into at most four primes, then its factorisation is of one of the following types: p, pq, p^2, pqr, p^2q, p^3, $pqrs$, p^2qr, p^2q^2, p^3q, and p^4, where p, q, r, s are distinct primes. The groups of the square-free orders p, pq, pqr, and $pqrs$ and those of prime-power orders p, p^2, p^3 and p^4 have been determined by Hölder (1893, 1895) and this is included in the SmallGroups library already. We refer to Slattery (2007) for a recent discussion of the groups of square-free orders and to Dietrich and Low (2021) for a generalisation of Slattery (2007). For a recent and accessible determination of the groups of order dividing p^5 we refer to Girnat (2003). It remains to consider the orders in

$$\mathcal{O} = \{p^2q,\ p^3q,\ p^2q^2,\ p^2qr\ :\ p, q, r \text{ distinct primes}\}.$$

These orders have also already been considered in the past: Cole and Glover (1893) and Hölder (1893) determined the groups of order p^2q, Western (1899) those of order p^3q, Le Vavasseur (1899, 1902) and Lin (1974) those of order p^2q^2, and Glenn (1906) those of order p^2qr. Moreover, Laue (1982) considered all orders p^aq^b with $a + b \leqslant 6$ and $a, b < 5$. In an arXiv article, Eick (2017) provided a compact and uniform enumeration of the orders in $\mathcal{O}$. Our results here include this and extend it to a full determination. Since many of the orders in $\mathcal{O}$ are cube-free, we mention that Dietrich and Eick (2005) and Dietrich and Wilson (2020) developed a construction algorithm and isomorphism test for groups of cube-free order; however, these works do not naturally lead to efficient identification functionality, cf. Section 4.3.

We proceed as follows. In Section 2 we describe our main results. In Section 3 we prove our enumeration; a proof of the determination follows the same arguments. Our algorithms are discussed in Section 4.

2. Main results

For every $n \in \mathcal{O}$ we provide an explicit closed formula for the number $\mathcal{N}(n)$ of groups of isomorphism types of order n, see Section 2.1; each of these formulas is a generalisation of a PORC function (a polynomial on residue classes), that is, there are finitely many sets of number-theoretic conditions on the involved primes so that $\mathcal{N}(n)$ is a polynomial in the involved primes for each of the condition-sets. The proof of our enumeration translates to new explicit group presentations, which we present in Section 2.2. These, in turn, lead to new efficient construction and identification algorithms, see Section 2.3.

2.1. Enumeration

For integers $u, v \in \mathbb{N}$ the *divisibility Kronecker delta* is

$$\Delta_u^v = \begin{cases} 1 & (\text{if } v \mid u) \\ 0 & (\text{otherwise.}) \end{cases}$$

Our first main result is the following theorem; we prove it in Sections 3.4–3.7.

Theorem 2.1. *Let p, q, and r be distinct primes.*

a) ***Order** p^2q:*
- $\mathcal{N}(p^2q) = 5$ *for* $q = 2$.
- $\mathcal{N}(p^2q) = 2 + \frac{q+5}{2}\Delta^q_{p-1} + \Delta^q_{p+1} + 2\Delta^p_{q-1} + \Delta^{p^2}_{q-1}$ *for* $q > 2$.

b) ***Order** p^3q:*
- *There are two special cases* $\mathcal{N}(2^3.3) = 15$ *and* $\mathcal{N}(2^3.7) = 13$.
- $\mathcal{N}(p^3q) = 15$ *if* $q = 2$.
- $\mathcal{N}(p^3q) = 12 + 2\Delta^4_{q-1} + \Delta^8_{q-1}$ *if* $p = 2$ *and* $q \notin \{3, 7\}$.
- *If p and q are both odd, then*

$$\mathcal{N}(p^3q) = 5 + \frac{q^2+13q+36}{6}\Delta^q_{p-1} + (p+5)\Delta^p_{q-1} + \frac{2}{3}\Delta^3_{q-1}\Delta^q_{p-1}$$
$$+\Delta^q_{(p+1)(p^2+p+1)}(1 - \Delta^q_{p-1}) + \Delta^q_{p+1} + 2\Delta^{p^2}_{q-1} + \Delta^{p^3}_{q-1}.$$

c) ***Order** p^2q^2 **with** $p > q$:*
- *There is one special case* $\mathcal{N}(3^2.2^2) = 14$.
- $\mathcal{N}(p^2q^2) = 12 + 4\Delta^4_{p-1}$ *if* $q = 2$ *and* $p \neq 3$.
- $\mathcal{N}(p^2q^2) = 4 + \frac{1}{2}(q^2 + q + 4)\Delta^{q^2}_{p-1} + (q+6)\Delta^q_{p-1} + 2\Delta^q_{p+1} + \Delta^{q^2}_{p+1}$ *if* $q > 2$.

d) ***Order** p^2qr **with** $q < r$:*
- *There is one special case* $\mathcal{N}(2^2.3.5) = 13$.
- $\mathcal{N}(p^2qr) = 10 + (2r+7)\Delta^r_{p-1} + 3\Delta^r_{p+1} + 6\Delta^p_{r-1} + 2\Delta^{p^2}_{r-1}$ *if* $q = 2$.
- *If* $q > 2$ *and* $(p, q, r) \neq (2, 3, 5)$, *then*

$$\mathcal{N}(p^2qr) = 2 \; + \; (p^2 - p)\Delta^{p^2}_{q-1}\Delta^{p^2}_{r-1} \; + \; \Delta^r_{p+1} \; + \; \Delta^q_{p+1} \; + \; \Delta^{p^2}_{r-1} \; + \; \Delta^{p^2}_{q-1}$$
$$+ (p-1)\big(\Delta^{p^2}_{q-1}\Delta^p_{r-1} \; + \; \Delta^{p^2}_{r-1}\Delta^p_{q-1} \; + \; 2\Delta^p_{r-1}\Delta^p_{q-1}\big)$$
$$+ \Delta^p_{r-1}\Delta^p_{q-1} \; + \; \Delta^p_{r-1}\Delta^q_{p-1} \; + \; \frac{1}{2}(q-1)(q+4)\Delta^q_{p-1}\Delta^q_{r-1}$$
$$+ \frac{1}{2}(q-1)\big(\Delta^q_{p+1}\Delta^q_{r-1} \; + \; \Delta^q_{p-1} \; + \; \Delta^{qr}_{p-1} \; + \; 2\Delta^{pq}_{r-1}\Delta^q_{p-1}\big)$$
$$+ \frac{1}{2}(qr+1)\Delta^{qr}_{p-1} \; + \; \frac{1}{2}(r+5)\Delta^r_{p-1}(1 + \Delta^q_{p-1}) \; + \; 2\Delta^q_{r-1}$$
$$+ \Delta^{qr}_{p^2-1} \; + \; 2\Delta^{pq}_{r-1} \; + \; \Delta^{p^2q}_{r-1} \; + \; 2\Delta^p_{q-1} \; + \; 3\Delta^q_{p-1} \; + \; 2\Delta^p_{r-1}.$$

2.2. Presentations

The next theorem follows from our proof of Theorem 2.1 and is discussed in Section 4.

Theorem 2.2. *Presentations for the groups of order $n \in \mathcal{O}$, up to isomorphism, are given in Tables 1–4. The groups listed in the left column only exist if the number in the right column is greater than* 0.

Throughout the paper, p, q, r denote distinct primes, and C_n^m denotes the m-fold direct product of the cyclic group C_n of order n. We write $\mathbb{Z}_n = \{0, \ldots, n-1\}$ for the ring of integers modulo n, and $\mathbb{Z}_n^*$ for its group of units. The general linear group of $n \times n$ matrices over the field $\mathbb{Z}_p$ is denoted $\mathrm{GL}_n(p)$; we write $\mathrm{diag}(a_1, \ldots, a_n)$ for the diagonal matrix with diagonal entries $a_1, \ldots, a_n$.

Notation 2.3. All solvable groups in Tables 1–4 are specified by a polycyclic presentation, with the following convention: first, we only list the power relations and non-trivial commutator relations, so that the set of generators is implicitly defined by the power relations: e.g. $\{a^p, b^p\}$ defines $\langle a, b \mid a^p, b^p, a^b = a\rangle \cong C_p^2$. Secondly, we abbreviate a relation $a = b$ by a/b, and if a acts on $b, c \in C_p^2$ via

Table 1
Groups of order p^2q.

Groups of order p^2q using Notation 2.3.

PC-relators	Parameters	Number of groups
Cluster 1: nilpotent		
a^{p^2q}		1
a^{pq}, b^p		1
Cluster 2: non-nilpotent, normal $P = C_p^2$		
$a^q, b^p, c^p, b^a/b^{\rho(p,q)}$		Δ_{p-1}^q
$a^q, b^p, c^p, (b^a, c^a)/(b, c)^{M(p,q,\sigma_q^k)}$	$0 \le k \le \frac{1}{2}(q-1)$	$\frac{1}{2}(q+1-\Delta_q^2)\Delta_{p-1}^q$
$a^q, b^p, c^p, (b^a, c^a)/(b, c)^{I_2(p,q)}$		$(1-\Delta_q^2)\Delta_{p+1}^q$
Cluster 3: non-nilpotent, normal $P = C_{p^2}$		
$a^q, b^{p^2}, b^a/b^{\rho(p^2,q)}$		Δ_{p-1}^q
Cluster 4: non-nilpotent, normal Q with complement $P = C_p^2$		
$a^p, b^p, c^q, c^a/c^{\rho(q,p)}$		Δ_{q-1}^p
Cluster 5: non-nilpotent, normal Q with complement $P = C_{p^2}$		
$a^{p^2}, b^q, b^a/b^{\rho(q,p)}$		Δ_{q-1}^p
$a^{p^2}, b^q, b^a/b^{\rho(q,p^2)}$		$\Delta_{q-1}^{p^2}$

a matrix M, then we specify these conjugacy relations by $(b^a, c^a)/(b, c)^M$. For example, $b^a = c$ and $c^a = b^2c^3$ is denoted by

$$(b^a, c^a)/(b, c)^M$$

where $M = \begin{pmatrix} 0 & 1 \\ 2 & 3 \end{pmatrix}$. The remaining notation is as follows.

- Throughout, P is a Sylow p-subgroup, Q is a Sylow q-subgroup, and F is the Fitting subgroup.
- If $\mathbb{Z}_a^*$ is cyclic, then the *canonical generator* $\sigma_a \in \mathbb{Z}_a^*$ is the smallest generator in $\{1, \ldots, a-1\}$. If b divides $\phi(a) = |\mathbb{Z}_a^*|$ and k is an integer, then we define
$$\rho(a, b, k) = \sigma_a^{k\phi(a)/b} \quad \text{and} \quad \rho(a, b) = \rho(a, b, 1).$$
- For $k \in \{2, 3\}$ fix a generator $\tau \in \mathrm{GF}(p^k)^*$. If $c \mid (p^k - 1)$ but $c \nmid (p^{k-1} - 1)$, then let $\gamma = \tau^{(p^k-1)/c}$ and define $I_k(p, c) \in \mathrm{GL}_k(p)$ to be the companion matrix of the characteristic polynomial of $\mathrm{diag}(\gamma, \gamma^p, \ldots, \gamma^{p^{k-1}})$; this matrix generates a subgroup of order c of a Singer cycle in $\mathrm{GL}_k(p)$. For example, if $p = 5$, $k = 2$, and $c = 3$, then $I_2(5, 3) = \begin{pmatrix} 0 & 4 \\ 1 & 4 \end{pmatrix}$.
- If $c \mid (p-1)$ such that $\mathbb{Z}_c^*$ is cyclic, then for an integer k we define
$$M(p, c, k) = \mathrm{diag}(\sigma_p^{(p-1)/c}, \sigma_p^{k(p-1)/c}) \quad \text{and} \quad M(p, c) = M(p, c, 1).$$

For example, if $p = 7$ and $q = 3$, then, using the above conventions, $\{a^q, b^{p^2}, c^p, b^a/b^{\rho(p^2,q)}\}$ encodes the group

$$\langle a, b, c \mid a^3, b^{49}, c^7, b^a = b^{30}, c^a = c, c^b = c \rangle;$$

note that $\sigma_{7^2} = 3$, so $\rho(p^2, q) = \sigma_{7^2}^{\phi(7^2)/3} = 3^{14} \bmod 49 = 30$.

2.3. Algorithms

Theorem 2.1 yields an enumeration formula for the groups of order $n \in \mathcal{O}$, and our proof of Theorem 2.1 directly translates to a construction algorithm for one or all groups of order n. If only one specific group is to be constructed, then the clusters and enumeration formulas listed in Tables 1–4

Table 2
Groups of order p^3q.

Groups of order p^3q, using Notation 2.3.

PC-relators	Parameters	Number of groups
Cluster 1: nilpotent		
a^{p^3q}		1
a^{p^2}, b^{pq}		1
a^p, b^p, c^{pq}		1
$a^p, b^p, c^p, d^q, b^a/bc$		$1-\Delta_p^2$
$a^p/c, b^p, c^p, d^q, b^a/bc$		$1-\Delta_p^2$
$a^2, b^4, c^q, b^a/b^3$		Δ_p^2
$a^2/b^2, b^4, c^q, b^a/b^3$		Δ_p^2
Cluster 2: non-nilpotent, normal Q with complement $P = C_{p^3}$		
$a^{p^3}, b^q, b^a/b^{\rho(q,p)}$		Δ_{q-1}^{p}
$a^{p^3}, b^q, b^a/b^{\rho(q,p^2)}$		$\Delta_{q-1}^{p^2}$
$a^{p^3}, b^q, b^a/b^{\rho(q,p^3)}$		$\Delta_{q-1}^{p^3}$
Cluster 3: non-nilpotent, normal Q with complement $P = C_{p^2} \times C_p$		
$a^{p^2}, b^p, c^q, c^b/c^{\rho(q,p)}$		Δ_{q-1}^{p}
$a^{p^2}, b^p, c^q, c^a/c^{\rho(q,p)}$		Δ_{q-1}^{p}
$a^{p^2}, b^p, c^q, c^a/c^{\rho(q,p^2)}$		$\Delta_{q-1}^{p^2}$
Cluster 4: non-nilpotent, normal Q with complement $P = C_p^3$		
$a^p, b^p, c^p, d^q, d^a/d^{\rho(q,p)}$		Δ_{q-1}^{p}
Cluster 5: non-nilpotent, normal Q with complement $P = p_+^{1+2}$ or $P = D_8$		
$a^p, b^p, c^p, d^q, c^a/bc, d^a/d^{\rho(q,p)}$		Δ_{q-1}^{p}
$a^2, b^4, c^q, b^a/b^3, c^a/c^{-1}$		Δ_p^2
Cluster 6: non-nilpotent, normal Q with complement $P = p_-^{1+2}$ or $P = Q_8$		
$a^p, b^{p^2}, c^q, b^a/b^{p+1}, c^a/c^{\rho(q,p,k)}$	$k \in \mathbb{Z}_p^*$	$(1-\Delta_p^2)(p-1)\Delta_{q-1}^{p}$
$a^p, b^{p^2}, c^q, b^a/b^{p+1}, c^b/c^{\rho(q,p)}$		$(1-\Delta_p^2)\Delta_{q-1}^{p}$
$a^2/b^2, b^4, b^a/b^3, c^q, c^a/c^{-1}$		Δ_p^2
Cluster 7: non-nilpotent, normal $P = C_{p^3}$		
$a^q, b^{p^3}, b^a/b^{\rho(p^3,q)}$		Δ_{p-1}^{q}
Cluster 8: non-nilpotent, normal $P = C_{p^2} \times C_p$		
$a^q, b^{p^2}, c^p, c^a/c^{\rho(p,q)}$		Δ_{p-1}^{q}
$a^q, b^{p^2}, c^p, b^a/b^{\rho(p^2,q)}$		Δ_{p-1}^{q}
$a^q, b^{p^2}, c^p, b^a/b^{\rho(p^2,q)}, c^a/c^{\rho(p,q,k)}$	$k \in \mathbb{Z}_q^*$	$(q-1)\Delta_{p-1}^{q}$
Cluster 9: non-nilpotent, normal $P = C_p^3$		
$a^q, b^p, c^p, d^p, b^a/b^{\rho(p,q)}$		Δ_{p-1}^{q}
$a^q, b^p, c^p, d^p, b^a/b^{\rho(p,q)}, c^a/c^{\rho(p,q,\sigma_q^k)}$	$0 \le k \le \frac{1}{2}(q-1)$	$\frac{1}{2}(q+1-\Delta_q^2)\Delta_{p-1}^{q}$
$a^q, b^p, c^p, d^p, b^a/b^{\rho(p,q)}, c^a/c^{\rho(p,q)}, d^a/d^{\rho(p,q,k)}$	$k \in \mathbb{Z}_q^*$	$(q-1)\Delta_{p-1}^{q}$
$a^q, b^p, c^p, d^p, b^a/b^{\rho(p,q)}, c^a/c^{\rho(p,q,\sigma_q^k)}, d^a/d^{\rho(p,q,\sigma_q^\ell)}$	$(k,\ell) \in \mathcal{P}$	$\frac{1}{6}(q^2-5q+6+4\Delta_{q-1}^3)\Delta_{p-1}^{q}$
$a^q, b^p, c^p, d^p, (b^a, c^a)/(b,c)^{I_2(p,q)}$		$(1-\Delta_q^2)\Delta_{p+1}^{q}$
$a^q, b^p, c^p, d^p, (b^a, c^a, d^a)/(b,c,d)^{I_3(p,q)}$		$(1-\Delta_q^2)(1-\Delta_q^3)\Delta_{p^2+p+1}^{q}$
Cluster 10: non-nilpotent, normal $P = p_+^{1+2}$		
$a^q, b^p, c^p, d^p, c^b/cd, b^a/b^{\rho(p,q,q-1)}, c^a/c^{\rho(p,q)}$		Δ_{p-1}^{q}
$a^q, b^p, c^p, d^p, c^b/cd, b^a/b^{\rho(p,q)}, d^a/d^{\rho(p,q)}$		Δ_{p-1}^{q}
$a^q, b^p, c^p, d^p, c^b/cd, b^a/b^{\rho(p,q,k)}, c^a/c^{\rho(p,q,q+1-k)}, d^a/d^{\rho(p,q)}$	$2 \le k \le \frac{1}{2}(q+1)$	$\frac{1}{2}(q-1-\Delta_q^2)\Delta_{p-1}^{q}$
$a^q, b^p, c^p, d^p, c^b/cd, (b^a, c^a)/(b,c)^{I_2(p,q)}$		$(1-\Delta_q^2)(1-\Delta_p^2)\Delta_{p+1}^{q}$
Cluster 11: non-nilpotent, normal $P = p_-^{1+2}$ or normal $P = Q_8$		
$a^q, b^p, c^{p^2}, c^a/c^{\rho(p^2,q)}, c^b/c^{p+1}.$		Δ_{p-1}^{q}
$a^3, b^2/c^2, c^4, c^b/c^3, b^a/c, c^a/bc$		$\Delta_p^2\Delta_q^3$
Cluster 12: no normal Sylow subgroups		
$a^2, b^3, c^2, d^2, b^a/b^2, c^a/d, c^b/d, d^a/c, d^b/cd$		$\Delta_p^2\Delta_q^3$
Parameter sets		
$\mathcal{P} = \begin{cases} \{(x,y) \in \mathbb{Z}_{q-1}^2 \;:\; 1 \le x \le \frac{1}{3}(q-2),\; 2x \le y \le q-2-x\} & (q \equiv 2 \bmod 3) \\ \{(x,y) \in \mathbb{Z}_{q-1}^2 \;:\; 1 \le x \le \frac{1}{3}(q-1),\; 2x \le y \le q-2-x\} \cup \{(\frac{1}{3}(q-1), \frac{2}{3}(q-1))\} & (q \equiv 1 \bmod 3). \end{cases}$		

Table 3
Groups of order p^2q^2 with $p > q$.

Groups of order p^2q^2 with $p > q$, using Notation 2.3.		
PC-relators	Parameters	Number of groups
Cluster 1: nilpotent		
$a^{p^2q^2}$		1
a^p, b^{pq^2}		1
a^{p^2q}, b^q		1
a^{pq}, b^{pq}		1
Cluster 2: non-nilpotent, normal $P = C_{p^2}$ with complement $Q = C_{q^2}$		
$a^{q^2}, b^{p^2}, b^a/b^{\rho(p^2,q)}$		Δ_{p-1}^{q}
$a^{q^2}, b^{p^2}, b^a/b^{\rho(p^2,q^2)}$		$\Delta_{p-1}^{q^2}$
Cluster 3: non-nilpotent, normal $P = C_{p^2}$ with complement $Q = C_q^2$		
$a^q, b^q, c^{p^2}, c^a/c^{\rho(p^2,q)}$		Δ_{p-1}^{q}
Cluster 4: non-nilpotent, normal $P = C_p^2$ with complement $Q = C_{q^2}$, or $(p,q) = (3,2)$		
$a^{q^2}, b^p, c^p, b^a/b^{\rho(p,q)}$		Δ_{p-1}^{q}
$a^{q^2}, b^p, c^p, (b^a, c^a)/(b,c)^{M(p,q,\sigma_q^k)}$	$0 \leq k \leq \frac{1}{2}(q-1)$	$\frac{1}{2}(q+1-\Delta_q^2)\Delta_{p-1}^{q}$
$a^{q^2}, b^p, c^p, b^a/b^{\rho(p,q^2)}$		$\Delta_{p-1}^{q^2}$
$a^{q^2}, b^p, c^p, (b^a, c^a)/(b,c)^{M(p,q^2,\sigma_{q^2}^k)}$	$0 \leq k \leq \frac{1}{2}(q^2-q)$	$\frac{1}{2}(q^2-q+2)\Delta_{p-1}^{q^2}$
$a^{q^2}, b^p, c^p, (b^a, c^a)/(b,c)^{M(p,q^2,kq)}$	$k \in \mathbb{Z}_q^*$	$(q-1)\Delta_{p-1}^{q^2}$
$a^9, b^2, c^2, b^a/c, c^a/bc$		$\Delta_p^3\Delta_q^2$
$a^{q^2}, b^p, c^p, (b^a, c^a)/(b,c)^{I_2(p,q)}$		$(1-\Delta_q^2)\Delta_{p+1}^{q}$
$a^{q^2}, b^p, c^p, (b^a, c^a)/(b,c)^{I_2(p,q^2)}$		$\Delta_{p+1}^{q^2}$
Cluster 5: non-nilpotent, normal $P = C_p^2$ with complement $Q = C_q^2$, or $(p,q) = (3,2)$		
$a^q, b^q, c^p, d^p, c^a/c^{\rho(p,q)}$		Δ_{p-1}^{q}
$a^q, b^q, c^p, d^p, (c^a, d^a)/(c,d)^{M(p,q,\sigma_q^k)}$	$0 \leq k \leq \frac{1}{2}(q-1)$	$\frac{1}{2}(q+1-\Delta_q^2)\Delta_{p-1}^{q}$
$a^q, b^q, c^p, d^p, c^a/c^{\rho(p,q)}, d^b/d^{\rho(p,q)}$		Δ_{p-1}^{q}
$a^3, b^3, c^2, d^2, c^a/d, d^a/cd$		$\Delta_p^3\Delta_q^2$
$a^q, b^q, c^p, d^p, (c^a, d^a)/(c,d)^{I_2(p,q)}$		$(1-\Delta_q^2)\Delta_{p+1}^{q}$

are used: If the group with ID[1] (n, i) is requested, then the counting formulas in the right columns of the tables allow us to directly determine the i-th group presentation. Conversely, if a group G of order n is given, then its ID (n, i) can be computed by, firstly, determining the cluster that contains G, and, secondly, deciding to which group in the cluster the given group is isomorphic to; this can be done by computing various invariants of G and comparing these with the choices made in Notation 2.3. In Section 4 we give more details and exemplify these construction and identification processes. A GAP implementation of our algorithms is available online, see Pan (2021); we comment on its performance in Section 4.3.

3. Counting results

The aim of this section is to provide proofs for the various parts of Theorem 2.1. Many of the groups we consider are split extensions $G = H \ltimes S$ with S being a Sylow subgroup. If $S \cong C_p^m$ is elementary abelian, then H acts on S as a subgroup of $\mathrm{Aut}(S) \cong \mathrm{GL}_m(p)$. We therefore start this section by discussing some preliminary enumeration results for split extensions and subgroups of linear groups.

3.1. Counting subgroups of linear groups

The next lemma is from Short (1992, Theorems 2.3.2 & 2.3.3).

[1] From Section 2.3 onwards "ID" always refers to the ordering used in our GAP implementation Pan (2021); due to different construction algorithms, our ID can be different to the ID used in the SmallGroups Library.

Table 4
Groups of order p^2qr with $r > q$.

Groups of order p^2qr with $r > q$, using Notation 2.3.

PC-relators	Parameters	Number of groups
Cluster 1: $F = G$		
a^{p^2qr}		1
a^p, b^{pqr}		1
Cluster 2: $\vert F\vert = r$		
$a^{p^2q}, b^r, b^a/b^{\rho(r,p^2q)}$		$\Delta_{r-1}^{p^2q}$
Cluster 3: $\vert F\vert = qr$		
$a^{p^2}, b^q, c^r, b^a/b^{\rho(q,p^2)}$		$\Delta_{q-1}^{p^2}$
$a^{p^2}, b^q, c^r, b^a/b^{\rho(q,p^2)}, c^a/c^{\rho(r,p,k)}$	$k \in \mathbb{Z}_p^*$	$(p-1)\Delta_{q-1}^{p^2}\Delta_{r-1}^{p}$
$a^{p^2}, b^q, c^r, b^a/b^{\rho(q,p^2)}, c^a/c^{\rho(r,p^2,k)}$	$k \in \mathbb{Z}_{p^2}^*$	$(p^2-p)\Delta_{r-1}^{p^2}\Delta_{q-1}^{p^2}$
$a^{p^2}, b^q, c^r, c^a/c^{\rho(r,p^2)}$		$\Delta_{r-1}^{p^2}$
$a^{p^2}, b^q, c^r, b^a/b^{\rho(q,p)}, c^a/c^{\rho(r,p^2,k)},$	$k \in \mathbb{Z}_p^*$	$(p-1)\Delta_{r-1}^{p^2}\Delta_{q-1}^{p}$
$a^p, b^p, c^q, d^r, c^a/c^{\rho(q,p)}, d^b/d^{\rho(r,p)}$		$\Delta_{q-1}^{p}\Delta_{r-1}^{p}$
Cluster 4: $\vert F\vert = p^2$		
$a^{qr}, b^{p^2}, b^a/b^{\rho(p^2,qr)}$		Δ_{p-1}^{qr}
$a^q, b^r, c^p, d^p, c^a/c^{\rho(p,q)}, d^b/d^{\rho(p,r)}$		Δ_{p-1}^{qr}
$a^q, b^r, c^p, d^p, c^a/c^{\rho(p,q)}, c^b/c^{\rho(p,r)}$		Δ_{p-1}^{qr}
$a^q, b^r, c^p, d^p, (c^a, d^a)/(c, d)^{M(p,q,k)}, c^b/c^{\rho(p,r)}$	$k \in \mathbb{Z}_q^*$	$(q-1)\Delta_{p-1}^{qr}$
$a^q, b^r, c^p, d^p, c^a/c^{\rho(p,q)}, (c^b, d^b)/(c, d)^{M(p,r,k)}$	$k \in \mathbb{Z}_r^*$	$(r-1)\Delta_{p-1}^{qr}$
$a^q, b^r, c^p, d^p, (c^a, d^a)/(c, d)^{M(p,q,\sigma_q^k)}, (c^b, d^b)/(c, d)^{M(p,r,\sigma_r^\ell)}$	$(k, \ell) \in \mathcal{P}_1$	$\frac{1}{2}(qr-q-r+5-2\Delta_q^2)\Delta_{p-1}^{qr}$
$a^2, b^r, c^p, d^p, b^a/b^{-1}, (c^a, d^a)/(d, c), (c^b, d^b)/(c, d)^{M(p,r,r-1)}$		$\Delta_q^2\Delta_{p-1}^{r}$
$a^{qr}, b^p, c^p, (b^a, c^a)/(b, c)^{I_2(p,qr)}$		$(1-\Delta_q^2)\Delta_{p+1}^{qr}$
$a^q, b^r, c^p, d^p, (c^a, d^a)/(c, d)^{M(p,q)}, (c^b, d^b)/(c, d)^{I_2(p,r)}$		$\Delta_{p-1}^{q}\Delta_{p+1}^{r}$
$a^2, b^r, c^p, d^p, b^a/b^{-1}, (c^a, d^a)/(d, c), (c^b, d^b)/(c, d)^{I_2(p,r)}$		$\Delta_q^2\Delta_{p+1}^{r}$
$a^q, b^r, c^p, d^p, (c^a, d^a)/(c, d)^{I_2(p,q)}, (c^b, d^b)/(c, d)^{M(p,r)}$		$(1-\Delta_q^2)\Delta_{p+1}^{q}\Delta_{p-1}^{r}$
Cluster 5: $\vert F\vert = p^2q$		
$a^r, b^{p^2}, c^q, b^a/b^{\rho(p^2,r)}$		Δ_{p-1}^{r}
$a^r, b^p, c^p, d^q, b^a/b^{\rho(p,r)}$		Δ_{p-1}^{r}
$a^r, b^p, c^p, d^q, (b^a, c^a)/(b, c)^{M(p,r,\sigma_r^k)}$	$0 \le k \le \frac{1}{2}(r-1)$	$\frac{1}{2}(r+1)\Delta_{p-1}^{r}$
$a^r, b^p, c^p, d^q, (b^a, c^a)/(b, c)^{I_2(p,r)}$		Δ_{p+1}^{r}
Cluster 6: $\vert F\vert = p^2r$		
$a^q, b^r, c^{p^2}, b^a/b^{\rho(r,q)}$		Δ_{r-1}^{q}
$a^q, b^r, c^{p^2}, c^a/c^{\rho(p^2,q)}$		Δ_{p-1}^{q}
$a^q, b^r, c^{p^2}, b^a/b^{\rho(r,q,k)}, c^a/c^{\rho(p^2,q)}$	$k \in \mathbb{Z}_q^*$	$(q-1)\Delta_{r-1}^{q}\Delta_{p-1}^{q}$
$a^q, b^r, c^p, d^p, c^a/c^{\rho(p,q)}$		Δ_{p-1}^{q}
$a^q, b^r, c^p, d^p, (c^a, d^a)/(c, d)^{M(p,q,\sigma_q^k)}$	$0 \le k \le \frac{1}{2}(q-1)$	$\frac{1}{2}(q+1-\Delta_q^2)\Delta_{p-1}^{q}$
$a^q, b^r, c^p, d^p, (c^a, d^a)/(c, d)^{I_2(p,q)}$		$\Delta_{p+1}^{q} \cdot (1-\Delta_q^2)$
$a^q, b^r, c^p, d^p, b^a/b^{\rho(r,q)}$		Δ_{r-1}^{q}
$a^q, b^r, c^p, d^p, b^a/b^{\rho(r,q)}, c^a/c^{\rho(p,q,k)}$	$k \in \mathbb{Z}_q^*$	$(q-1)\Delta_{r-1}^{q}\Delta_{p-1}^{q}$
$a^q, b^r, c^p, d^p, b^a/b^{\rho(r,q,\sigma_q^\ell)}, (c^a, d^a)/(c, d)^{M(p,q,\sigma_q^k)}$	$(k, \ell) \in \mathcal{P}_2$	$\frac{1}{2}q(q-1-\Delta_q^2)\Delta_{r-1}^{q}\Delta_{p-1}^{q}$
$a^2, b^r, c^p, d^p, b^a/b^{-1}, c^a/c^{-1}, d^a/d^{-1}$		Δ_q^2
$a^q, b^r, c^p, d^p, b^a/b^{\rho(r,q)}, (c^a, d^a)/(c, d)^{(I_2(p,q)^k)}$	$1 \le k \le \frac{1}{2}(q-1)$	$\frac{1}{2}(q-1-\Delta_q^2)\Delta_{r-1}^{q}\Delta_{p+1}^{q}$
Cluster 7: $\vert F\vert = pr$		
$a^q, b^p, c^p, d^r, d^a/d^{\rho(r,q)}, d^b/d^{\rho(r,p)}$		Δ_{r-1}^{pq}
$a^q, b^{p^2}, c^r, c^a/c^{\rho(r,q)}, c^b/c^{\rho(r,p)}$		Δ_{r-1}^{pq}
$a^q, b^p, c^p, d^r, c^a/c^{\rho(p,q)}, d^b/d^{\rho(r,p)}$		$\Delta_{r-1}^{p}\Delta_{p-1}^{q}$
$a^q, b^p, c^p, d^r, c^a/c^{\rho(p,q,k)}, d^a/d^{\rho(r,q)}, d^b/d^{\rho(r,p)}$	$k \in \mathbb{Z}_q^*$	$(q-1)\Delta_{r-1}^{pq}\Delta_{p-1}^{q}$
Cluster 8: $\vert F\vert = pqr$		
$a^{p^2}, b^q, c^r, c^a/c^{\rho(r,p)}$		Δ_{r-1}^{p}
$a^{p^2}, b^q, c^r, b^a/b^{\rho(q,p)}$		Δ_{q-1}^{p}

(continued on next page)

Table 4 (*continued*)

Groups of order p^2qr with $r > q$, using Notation 2.3.

PC-relators	Parameters	Number of groups
$a^{p^2}, b^q, c^r, b^a/b^{\rho(q,p)}, c^a/c^{\rho(r,p,k)}$	$k \in \mathbb{Z}_p^*$	$(p-1)\Delta_{r-1}^p\Delta_{q-1}^p$
$a^p, b^p, c^q, d^r, d^a/d^{\rho(r,p)}$		Δ_{r-1}^p
$a^p, b^p, c^q, d^r, c^a/c^{\rho(q,p)}$		Δ_{q-1}^p
$a^p, b^p, c^q, d^r, c^a/c^{\rho(q,p)}, d^a/d^{\rho(r,p,k)}$	$k \in \mathbb{Z}_p^*$	$(p-1)\Delta_{r-1}^p\Delta_{q-1}^p$
Cluster 9: $F = 1$		
Alt_5 (not solvable)		$\Delta_p^2\Delta_q^3\Delta_r^5$
Parameter sets		
$\mathcal{P}_1 = \{(x,y) : 0 \le x \le \frac{1}{2}(q-1),\ 0 \le y \le \frac{1}{2}(r-1)\} \cup \{(x,y) : 1 \le x \le \frac{1}{2}(q-3),\ \frac{1}{2}(r+1) \le y \le r-2\}$		
$\mathcal{P}_2 = \{(x,0) : 0 \le x \le \frac{1}{2}(q-3)\} \cup \{(x,y) : 0 \le x \le \frac{1}{2}(q-1),\ 1 \le y \le \frac{1}{2}(q-3)\} \cup \{(\frac{1}{2}(q-1), \frac{1}{2}(q-1))\}$ $\cup\ \{(x,y) : 0 \le x \le \frac{1}{2}(q-3),\ \frac{1}{2}(q-1) \le y \le q-2\}$		

Lemma 3.1. *There is an irreducible cyclic subgroup of order m in $\mathrm{GL}_n(p)$ if and only if $m \mid (p^n-1)$ and $m \nmid (p^d-1)$ for each $d \in \{1,\dots,n-1\}$; if such a subgroup exists, then it is unique up to conjugacy.*

We now determine the number of conjugacy classes of certain subgroups of $\mathrm{GL}_2(p)$ and $\mathrm{GL}_3(p)$.

Proposition 3.2. *For a group G and integer m write $s_m(G)$ for the number of conjugacy classes of subgroups of order m in G. If p, q, and r are distinct primes, then the following hold.*

a) *If $q=2$, then $s_q(\mathrm{GL}_2(p)) = 2$; if $q>2$, then $s_q(\mathrm{GL}_2(p)) = \frac{q+3}{2}\Delta_{p-1}^q + \Delta_{p+1}^q$. If $H \leqslant \mathrm{GL}_2(p)$ has order q, then $|N_{\mathrm{GL}_2(p)}(H)/C_{\mathrm{GL}_2(p)}(H)| \leqslant 2$ with equality for $q>2$ and $\Delta_{p-1}^q + \Delta_{p+1}^q$ subgroup classes.*

b) *We have $s_{q^2}(\mathrm{GL}_2(p)) = \Delta_{p-1}^q + \frac{q^2+q+2}{2}\Delta_{p-1}^{q^2} + \Delta_{p+1}^{q^2}$.*

c) *If $q=2$, then $s_{qr}(\mathrm{GL}_2(p)) = \frac{3r+7}{2}\Delta_{p-1}^r + 2\Delta_{p+1}^r$; if $r,q>2$, then*

$$s_{qr}(\mathrm{GL}_2(p)) = \frac{qr+q+r+5}{2}\Delta_{p-1}^{qr} + \Delta_{p^2-1}^{qr}(1-\Delta_{p-1}^{qr}).$$

d) *If $q=2$, then $s_q(\mathrm{GL}_3(p)) = 3$; if $q \geqslant 3$, then*

$$s_q(\mathrm{GL}_3(p)) = \frac{q^2+4q+9+4\Delta_{q-1}^3}{6}\Delta_{p-1}^q + \Delta_{(p+1)(p^2+p+1)}^q(1-\Delta_{p-1}^q).$$

Proof. Let $S \cong C_{p^2-1}$ be a Singer cycle in $\mathrm{GL}_2(p)$ and let $D \cong C_{p-1}^2$ be the subgroup of diagonal matrices. Let $U \leqslant \mathrm{GL}_2(p)$ be of cubefree order m with $p \nmid m$. It follows from Dietrich and Eick (2005, Lemma 8) that every such U is conjugate to a subgroup of $N = C_2 \ltimes S$ (Singer normaliser) or of $I = C_2 \ltimes D$ (maximal imprimitive). Recall that $D \cap S = Z(\mathrm{GL}_2(p))$ and I/D swaps the diagonal entries of elements in D. Suppose now that U is reducible. Then, up to conjugacy, $U \leqslant D$; if U is cyclic of prime power order m, then, up to conjugacy, $U = \langle \mathrm{diag}(a, a^\ell)\rangle$ for some $\ell \in \{0,\dots,m-1\}$ where $a \in \mathbb{Z}_p^*$ has order m. Note that two such groups $\langle \mathrm{diag}(a,a^\ell)\rangle$ and $\langle \mathrm{diag}(a,a^k)\rangle$ are conjugate if and only if $\ell = k$ or there is $x \in \mathbb{Z}_m^*$ with $\ell = x$ and $k \equiv x^{-1} \bmod m$. Thus, the conjugation action partitions these subgroups in pairs, unless the parameter $\ell \in \mathbb{Z}_m^*$ has order dividing 2. We use these results freely in the proof below.

a) Every group of order q is cyclic. There exists a (unique) class of irreducible subgroups of order q if and only if $q \mid (p+1)$ and $q \nmid (p-1)$; this requires $q \neq 2$. Now suppose $q \mid (p-1)$ and let $a \in \mathbb{Z}_p^*$ be of order q. If $q=2$, then there are two classes of reducible subgroups, generated by $\mathrm{diag}(-1,-1)$ and $\mathrm{diag}(-1,1)$, respectively. If $q>2$ and $\sigma \in \mathbb{Z}_q^*$ is a generator, then there are $1+(q+1)/2$ classes of reducible subgroups, generated by $\mathrm{diag}(a,1)$ and $\mathrm{diag}(a, a^{(\sigma^k)})$ with $k \in \{0,\dots,(q-1)/2\}$. For the last claim, write $G = \mathrm{GL}_2(p)$ and let $H \leqslant G$ be of order q. If $q=2$, then $N_G(H) = C_G(H)$, so let $q>2$. Up

to conjugacy, if H is irreducible, then $H \leqslant S$ is unique and $N_G(H)/C_G(H) \cong C_2$; if H is reducible, then $H = \langle \mathrm{diag}(a, a^{-1})\rangle \leqslant D$ with $a \in \mathbb{Z}_p^*$ of order q is the unique such subgroup with $|N_G(H)/C_G(H)| = 2$.
b) Any non-cyclic subgroup of order q^2 is reducible and exists if $q \mid (p-1)$; it is unique up to conjugacy. A cyclic irreducible subgroup of order q^2 exists if and only if $q^2 \mid (p^2-1)$ and $q^2 \nmid (p-1)$; this forces $q = 2$ and $4 \nmid (p-1)$, or $q > 2$ and $q^2 \mid (p+1)$. A cyclic reducible subgroup of order q^2 requires $q^2 \mid (p-1)$. If $a \in \mathbb{Z}_p^*$ has order q^2 and $\sigma \in \mathbb{Z}_{q^2}^*$ is a generator, then there are $(q^2+q+2)/2$ classes of these subgroups, generated by $\mathrm{diag}(a, a^x)$ with $x \in \mathbb{Z}_{q^2} \setminus \mathbb{Z}_{q^2}^*$ and $\mathrm{diag}(a, a^{(\sigma^k)})$ with $k \in \{0, \dots, q(q-1)/2\}$.
c) First, suppose $q, r > 2$. By Lemma 3.1, there is one class of irreducible cyclic subgroups of order qr if and only if $qr \mid (p^2-1)$ but $qr \nmid (p-1)$; this is the unique subgroup of order qr in N, which yields a summand $\Delta_{p^2-1}^{qr}(1 - \Delta_{p-1}^{qr})$. Looking at reducible cyclic subgroups, we require $qr \mid (p-1)$, and it remains to consider generators $\mathrm{diag}(a, a^\ell)$ with $a \in \mathbb{Z}_p^*$ of order qr and $\mathrm{diag}(b, c)$ with $b, c \in \mathbb{Z}_p^*$ of order q and r, respectively. In the latter case, there is a unique such subgroup. In the former case, we have to consider $q + r - 1$ non-units $\ell \in \mathbb{Z}_{qr} \setminus \mathbb{Z}_{qr}^*$ and $qr - r - q + 1$ units $\ell \in \mathbb{Z}_{qr}^*$, including four elements of order dividing 2. Together, we obtain $1 + 4 + (qr - q - r - 3)/2 + (q + r - 1) = (qr + r + q + 5)/2$ classes of cyclic groups. Since $2 \nmid qr$, there is no non-cyclic subgroup of order qr; this proves the formula for $q, r > 2$.

Now assume that $r > q = 2$. If $r \mid (p+1)$, then N contains, up to conjugacy, two irreducible subgroups of order $2r$, one being cyclic, the other non-cyclic; this yields the summand $2\Delta_{p+1}^r$. Now suppose $r \mid (p-1)$. We deal with reducible subgroups as before. The main difference is that this time $\mathbb{Z}_{2r}^*$ is cyclic, so there are only 2 elements of order dividing 2; in total, we obtain $(3r+5)/2$ classes of reducible subgroups if $r \mid (p-1)$. It remains to count subgroups of I that are not reducible: a short argument shows that, up to conjugacy, there is a unique such subgroup, namely, $\langle s, \mathrm{diag}(a, a^{-1})\rangle$ where $a \in \mathbb{Z}_p^*$ has order r and s is the permutation matrix of the transposition $(1, 2)$. This gives an additional summand Δ_{p-1}^r.
d) If $q = 2$, then $\mathrm{diag}(1, 1, -1)$, $\mathrm{diag}(1, -1, -1)$, and $\mathrm{diag}(-1, -1, -1)$ generate the three classes of subgroups of order 2; now let $q > 2$. Up to conjugacy, every diagonalisable subgroup of order q is generated by an element of type $\mathrm{diag}(a, 1, 1)$, $\mathrm{diag}(a, a^k, 1)$, or $\mathrm{diag}(a, a^k, a^\ell)$, respectively, where $a \in \mathbb{Z}_p^*$ has order q and $k, \ell \in \mathbb{Z}_q^*$. By a), there are $(q+3)/2$ classes of groups with generators of the first two types; for the last type, let $\sigma \in \mathbb{Z}_q^*$ be a primitive element and note that $\langle \mathrm{diag}(a, a^{(\sigma^k)}, a^{(\sigma^\ell)})\rangle$ and $\langle \mathrm{diag}(a, a^{(\sigma^x)}, a^{(\sigma^y)})\rangle$ with $k, \ell, x, y \in \mathbb{Z}_{q-1}$ are conjugate if and only if $\{x, y\} \in \{\{-\ell, k-\ell\}, \{-k, \ell-k\}, \{k, \ell\}\}$. To get the number of classes for this type, we use the Cauchy-Frobenius Lemma (Holt et al., 2005, Lemma 2.17) to count the G-orbits in the set of parameters $(k, \ell) \in \mathbb{Z}_{q-1}^2$, where

$$G = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} -1 & -1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ -1 & -1 \end{pmatrix} \right\} \cong \mathrm{Sym}_3.$$

The number of orbits is determined as $(q^2 + q + 4\Delta_{q-1}^3)/6$. In total, this gives $(q^2 + 4q + 9 + 4\Delta_{q-1}^3)/6$ classes of diagonal subgroups of order q. Non-diagonalisable groups arise from irreducible subgroups in $\mathrm{GL}_2(p)$ or $\mathrm{GL}_3(p)$. In the former case, a) yields Δ_{p+1}^q groups. In the latter case, Lemma 3.1 shows that there is a (unique) class if and only if $q \mid (p^3-1)$ but $q \nmid (p^2-1)$. In total, there are $\Delta_{(p+1)(p^2+p+1)}^q(1 - \Delta_{p-1}^q)$ non-diagonalisable groups □.

3.2. *Counting split extensions*

A group G splits over a normal subgroup $N \trianglelefteq G$ if there exists a subgroup $U \leqslant G$ with $G = UN$ and $U \cap N = 1$; in this case we write $G = U \ltimes N$. If $|N|$ and $|G/N|$ are coprime, then the Schur-Zassenhaus Theorem (Robinson, 1982, (9.1.2)) implies that G splits over N. Conversely, if U and N are groups and $\varphi \colon U \to \mathrm{Aut}(N)$ is a homomorphism, then the group $G = U \ltimes_\varphi N$ with underlying set $\{(u, n) : u \in U, n \in N\}$ and multiplication $(u, n)(v, m) = (uv, n^{\varphi(v)}m)$ splits over $\{(1, n) : n \in N\} \cong N$ with complement $\{(u, 1) : u \in U\} \cong U$. For some special cases, we will have to determine all split extensions of U by N up to isomorphism; the results of this section will be useful for that.

Let U and N be groups. The direct product $\mathrm{Aut}(U) \times \mathrm{Aut}(N)$ acts on $\varphi \in \mathrm{Hom}(U, \mathrm{Aut}(N))$ via

$$\varphi^{(\alpha,\beta)} = \overline{\beta^{-1}} \circ \varphi \circ \alpha,$$

where $\overline{\beta} \in \mathrm{Aut}(N)$ is the conjugation by β in $\mathrm{Aut}(N)$, so $\varphi^{(\alpha,\beta)}(u) = \beta \circ \varphi(\alpha(u)) \circ \beta^{-1}$ for all $u \in U$. The stabiliser of $\varphi \in \mathrm{Hom}(U, \mathrm{Aut}(N))$ under this action is the group of *compatible pairs*

$$\mathrm{CP}(\varphi) = \{(\alpha, \beta) \in \mathrm{Aut}(U) \times \mathrm{Aut}(N) : \varphi(\alpha(u)) = \beta^{-1} \circ \varphi(u) \circ \beta \quad (\forall u \in U)\}.$$

If N is a abelian, then $\mathrm{CP}(\varphi)$ acts on the group of 2-cocycles $Z^2_\varphi(U, N)$ via $\gamma^{(\alpha,\beta)} = \beta^{-1} \circ \gamma \circ (\alpha, \alpha)$, inducing an action on the cohomology group $H^2_\varphi(U, N)$, see Holt et al. (2005, p. 55). Every extension of U by N is isomorphic to a group $E(\varphi, \gamma)$ with underlying set $U \times N$ and multiplication $(u, n)(v, m) = (uv, n^{\varphi(u)} m\gamma(u, v))$ for some $\varphi \in \mathrm{Hom}(U, \mathrm{Aut}(N))$ and $\gamma \in Z^2_\varphi(U, N)$, see Holt et al. (2005, Section 2.7.3). Two such extensions of U by N are *strongly isomorphic* if every isomorphism maps the normal subgroup N to itself. This holds, for example, if U and N are solvable of coprime orders, because in any extension N is a unique Hall subgroup, see Robinson (1982, (9.1.7)), or if N maps onto the Fitting subgroup in each extension. We call N a *strong U-group* if every pair of isomorphic extensions of U by N is also strongly isomorphic.

Proposition 3.3. *Let U be a group and let N be a strong U-group that is abelian. Let $\mathcal{X}$ be a set of representatives of the $\mathrm{Aut}(U) \times \mathrm{Aut}(N)$ orbits in $\mathrm{Hom}(U, \mathrm{Aut}(N))$, and for each $\varphi \in \mathcal{X}$ let o_φ be the number of $\mathrm{CP}(\varphi)$-orbits in $H^2_\varphi(U, N)$. There are $\sum_{\varphi \in \mathcal{X}} o_\varphi$ isomorphism types of extensions of U by N.*

Proof. Suppose $\tau : E(\varphi, \gamma) \to E(\psi, \delta)$ is an isomorphism. Since N is a strong U-group, there exist $(\alpha, \beta) \in \mathrm{Aut}(U) \times \mathrm{Aut}(N)$ and a map $\varepsilon : U \to N$ such that each $\tau((u, n)) = (\alpha(u), \beta(n)\varepsilon(u))$. Comparing the images of $(1, n^{\varphi(u)}) = (u^{-1}, 1)(1, n)(u, 1)$ under τ shows that $\beta(n^{\varphi(u)}) = \beta(n)^{\psi(\alpha(u))}$ for all $u \in U$ and $n \in N$, so φ and ψ are in the same $\mathrm{Aut}(U) \times \mathrm{Aut}(N)$ orbit. This shows that extensions using different $\varphi, \psi \in \mathcal{O}$ are non-isomorphic. Now consider $\varphi \in \mathrm{Hom}(U, \mathrm{Aut}(N))$ with representative $\psi \in \mathcal{X}$, that is, there is $(\alpha, \beta) \in \mathrm{Aut}(U) \times \mathrm{Aut}(N)$ such that $\beta(n^{\varphi(u)}) = \beta(n)^{\psi(\alpha(u))}$ for all $u \in U$ and $n \in N$; a direct computation shows that for every $\gamma \in Z^2_\varphi(U, N)$ the group $E(\varphi, \gamma)$ is isomorphic to $E(\psi, \gamma^{(\alpha^{-1},\beta^{-1})})$ via $(u, n) \mapsto (\alpha(u), \beta(n))$. The claim of the theorem now follows from Besche and Eick (1999, Section 4.2.1), which shows that for a fixed $\varphi \in \mathcal{O}$ there are o_φ isomorphism types of extensions $E(\varphi, \gamma)$ with $\gamma \in Z^2_\varphi(U, N)$. □

A special case is considered in Dietrich and Eick (2005, Lemma 5 and Theorem 14):

Lemma 3.4. *Let U and N be groups such that N and the Sylow p-subgroup $P \leqslant U$ are cyclic of order p. If N and P are isomorphic as $N_U(P)$-modules, then there is a unique isomorphism type of non-split extensions of U by N; otherwise every extension is a split extension.*

We conclude this section by discussing the number of group extensions of solvable groups of coprime order; this requires the following definition:

Definition 3.5. For solvable groups U and N of coprime order we define the following. Let $\mathcal{S}$ be a set of representatives for the conjugacy classes of subgroups in $\mathrm{Aut}(N)$, let $\mathcal{K}$ be a set of representatives for the $\mathrm{Aut}(U)$-classes of normal subgroups in U, and set

$$\mathcal{X} = \{(S, K) : S \in \mathcal{S}, K \in \mathcal{K} \text{ with } S \cong U/K\}.$$

For $(S, K) \in \mathcal{X}$ let $A_K, A_S \leqslant \mathrm{Aut}(U/K)$ be defined as follows: A_K is the subgroup induced by the action of $\mathrm{Stab}_{\mathrm{Aut}(U)}(K)$ on U/K; the group A_S is defined as the preimage under a fixed isomorphism $U/K \to S$ of the subgroup of $\mathrm{Aut}(S)$ induced by the action of $N_{\mathrm{Aut}(N)}(S)$. Finally, we set

$$\mathrm{ind}_K = [\mathrm{Aut}(U/K) : A_K] \quad \text{and} \quad \mathrm{DC}(S, K) = A_K \setminus \mathrm{Aut}(U/K)/A_S.$$

Proposition 3.6. *Let N and U be solvable of coprime orders. Let $\sigma(U,N)$ be the number of isomorphism types of extensions of U by N. We have $\sigma(U,N)=\sum_{(S,K)\in\mathcal{X}}|\mathrm{DC}(S,K)|$, and the following hold:*

a) *If N and $\mathrm{Aut}(N)$ are cyclic, then $\sigma(U,N)=\sum_{\ell\mid\pi}\sum_{K\in\mathcal{K}_\ell}\mathrm{ind}_K$, where $\pi=\gcd(|U|,|\mathrm{Aut}(N)|)$ and $\mathcal{K}_\ell$ is a set of representatives of the $\mathrm{Aut}(U)$-classes in $\{K\trianglelefteq U : U/K\cong C_\ell\}$.*

b) *If q is a prime and $U\cong C_{q^k}$, then $\sigma(U,N)=|\mathcal{T}|$, where $\mathcal{T}$ is a set of conjugacy class representatives of cyclic subgroups of order dividing q^k in $\mathrm{Aut}(N)$.*

Proof. The assumptions imply that N is a strong U-group and that every extension splits; in particular, each $H^2_\varphi(U,N)=1$ is trivial. Proposition 3.3 (or Taunt, 1955) shows that $\sigma(U,N)$ is the number of $\mathrm{Aut}(U)\times\mathrm{Aut}(N)$-orbits in $\mathrm{Hom}(U,\mathrm{Aut}(N))$. These orbits correspond to the union of $A_K\times N_{\mathrm{Aut}(N)}(S)$-orbits in the set of isomorphisms $U/K\to S$ for every $(S,K)\in\mathcal{X}$. The latter corresponds to $\mathrm{DC}(S,K)$.

a) For each $\ell\mid\pi$ there is a unique subgroup $S\leqslant\mathrm{Aut}(N)$ of order ℓ. Since $\mathrm{Aut}(N)$ is abelian, $N_{\mathrm{Aut}(N)}(S)=\mathrm{Aut}(N)$ acts trivially on S by conjugation, so $A_S=1$. This implies that $|\mathrm{DC}(S,K)|=\mathrm{ind}_K$ for each K.
b) For each $\ell=0,\dots,k$ there is a unique $K\trianglelefteq U$ with $|K|=p^\ell$ and $U/K\cong C_{p^{k-\ell}}$. Each such K satisfies $A_K=\mathrm{Aut}(U/K)$, hence $|\mathrm{DC}(S,K)|=1$ in all cases. □

3.3. *Group enumeration*

In the subsequent sections we enumerate the isomorphism types of groups of order p^2q, p^3q, p^2q^2, and p^2qr, where p,q,r are distinct primes. We freely use the following results in our discussion. Burnside's Theorem (Robinson, 1982, (8.5.4)) shows that groups of order p^aq^b are solvable, and such groups have a nontrivial Fitting subgroup (which is the largest nilpotent normal subgroup). A group is nilpotent if and only if it is the direct product of its Sylow subgroups. Up to isomorphism, the groups of order p, p^2, and p^3 are the abelian groups C_p, C_{p^2}, C_{p^3}, C_p^2, C_p^3, $C_{p^2}\times C_p$, and two extraspecial groups p_+^{1+2} and p_-^{1+2}; if $p=2$, then $p_+^{1+2}=D_8$ and $p_-^{1+2}=Q_8$. We often make case distinctions on the structure of the Fitting subgroup and on whether there exists a normal Sylow subgroup. Recall that if G has a normal Sylow subgroup N, then $G=U\ltimes N$ for some $U\leqslant G$ by the Schur-Zassenhaus Theorem (Robinson, 1982, (9.1.2)); in particular, the complement U is unique up to conjugacy. The following lemma will be useful.

Lemma 3.7. *If G is a solvable group with abelian Fitting subgroup F, then G/F acts faithfully on F via conjugation; in particular, G/F embeds into $\mathrm{Aut}(F)$ and so $|G/F|$ divides $|\mathrm{Aut}(F)|$.*

Proof. The assumptions imply that F is nontrivial and G acts via conjugation on F with kernel $C_G(F)$. Since G is solvable and F is abelian, (Robinson, 1982, (5.4.4)) shows that $F=C_G(F)$. The claim follows. □

3.4. *The groups of order p^2q*

The groups of order p^2q have been considered by Hölder (1893), by Cole and Glover (1893), by Lin (1974), by Laue (1982) and in various other places. The results by Hölder, Lin and Laue agree with ours, although Lin's results have some harmless typos; we have not considered Cole and Glover (1893). We also refer to Blackburn et al. (2007, Proposition 21.17) for an alternative description and proof of the following result.

Proof of Theorem 2.1a). Let G be a group of order p^2q. Since G is solvable, the Fitting subgroup satisfies $1<F\leqslant G$. If $F=G$, then G is nilpotent, so isomorphic to $C_{p^2}\times C_q$ or $C_p^2\times C_q$. Now let $F<G$. The case $|F|=p$ and $|G/F|=pq$ contradicts Lemma 3.7, thus $|F|\in\{q,pq,p^2\}$ and F contains a Sylow subgroup of G. The latter is characteristic in F, so normal in G. Thus, if $F<G$, then G has a normal Sylow p- or Sylow q-subgroup, but not both. We make a case distinction and use Proposition 3.6.

If G has a normal Sylow p-subgroup, then $G = U \ltimes N$ where $|N| = p^2$ and $U \cong C_q$ acts faithfully on N. If $N \cong C_p^2$, then $\mathrm{Aut}(N) \cong \mathrm{GL}_2(p)$ and the number of conjugacy classes of subgroups of $\mathrm{Aut}(N)$ of order q is determined by Proposition 3.2a). If $N \cong C_{p^2}$, then $\mathrm{Aut}(N) \cong C_{p(p-1)}$ is cyclic and there are Δ^q_{p-1} subgroups of order q in $\mathrm{Aut}(N)$. This gives $\frac{q+3}{2}\Delta^q_{p-1} + \Delta^q_{p+1} + \Delta^q_{p-1}$ groups if $q > 2$, and 3 groups if $q = 2$.

If G has a normal Sylow q-subgroup, then $G = U \ltimes N$ where $|U| = p^2$ and $N \cong C_q$. To apply Proposition 3.6a) for counting non-abelian extensions, we have to consider the $\mathrm{Aut}(U)$-classes of proper normal subgroups K in U with U/K cyclic. If U is cyclic, then it has two proper normal subgroups K with cyclic quotients; the case $K = 1$ arises if and only if $p^2 \mid (q-1)$ and the case $K = C_p$ arises if and only if $p \mid (q-1)$; in both cases $\mathrm{ind}_K = 1$, and together we get $\Delta^p_{q-1} + \Delta^{p^2}_{q-1}$ groups. If U is non-cyclic, then there is a unique $\mathrm{Aut}(U)$-class of proper normal subgroups K with cyclic quotients, namely $K \cong C_p$ with $\mathrm{ind}_K = 1$; this case arises if $p \mid (q-1)$, and so we get Δ^p_{q-1} groups. □

3.5. The groups of order p^3q

Western (1899) and Laue (1982) determined these groups. Western's summary misses one group for $q \equiv 1 \bmod p$, but this group is mentioned in Western (1899, Section 13); there are further minor issues in Western (1899, Section 32). There are disagreements between our results and Laue (1982, pp. 224-6) for the case $p = 2$ and the case $q = 3$; we have not tried to track the origin of these in Laue's work.

Proof of Theorem 2.1b). We follow the strategy of the proof of Theorem 2.1a). Every group G of order p^3q is solvable and there are five nilpotent groups of order p^3q; we now consider non-nilpotent groups.

Case 1: *Non-nilpotent with normal Sylow p-subgroup.* Suppose $G = U \ltimes N$ with $|N| = p^3$ and $|U| = q$. Proposition 3.6b) shows that the isomorphism types of these groups correspond to the conjugacy classes of subgroups of order q in $\mathrm{Aut}(N)$. We first consider the special case $p = 2$: a direct computation shows that the only options are $N = C_2^3$ with $q \in \{3, 7\}$ (one class each) and $N = Q_8$ with $q = 3$ (one class). We now consider $p > 2$ and discuss the different subgroups N.

If N is cyclic, then $\mathrm{Aut}(N) \cong C_{p^2(p-1)}$ and there are $c_1 = \Delta^q_{p-1}$ groups. If $N \cong C_{p^2} \times C_p$, then a short argument shows that $|\mathrm{Aut}(N)| = p^3(p-1)^2$; since $p > 2$, the Sylow Theorem (Robinson, 1982, p. 40) implies that $\mathrm{Aut}(N)$ has a normal Sylow p-subgroup. Up to conjugacy, this Sylow p-subgroup has a unique complement C_{p-1}^2, thus $\mathrm{Aut}(N)$ has $c_2 = (q+1)\Delta^q_{p-1}$ conjugacy classes of subgroups of order q. If N is extraspecial of exponent p, then there is an epimorphism $\mathrm{Aut}(N) \to \mathrm{GL}_2(p)$ with kernel C_p^2, see Winter (1972, Theorem 1), and so the conjugacy classes of subgroups C_q in $\mathrm{Aut}(N)$ correspond to conjugacy classes of subgroups C_q in $\mathrm{GL}_2(p)$. Proposition 3.2a) shows that the number of such subgroups is $c_3 = 2$ if $q = 2$, and $c_3 = \frac{1}{2}(q+3)\Delta^q_{p-1} + \Delta^q_{p+1}$ if $q > 2$. If N is extraspecial of exponent p^2, then Winter (1972, Theorem 1) shows that $\mathrm{Aut}(N)$ has a normal Sylow p-subgroup and a complement isomorphic to C_{p-1}; this yields $c_4 = \Delta^q_{p-1}$ groups. Lastly, suppose $N \cong C_p^3$ is elementary abelian, so $\mathrm{Aut}(N) \cong \mathrm{GL}_3(p)$, and Proposition 3.2d) yields $c_5 = 3$ groups if $q = 2$; if $q > 2$, then the number of groups we have to add is

$$c_5 = \tfrac{1}{6}(q^2 + 4q + 9 + 4\Delta^3_{q-1})\Delta^q_{p-1} + \Delta^q_{(p+1)(p^2+p+1)}(1 - \Delta^q_{p-1}).$$

Case 2: *Non-nilpotent with normal Sylow q-subgroup.* Suppose $G = U \ltimes N$ with $|N| = q$ and $|U| = p^3$. Using Proposition 3.6, we have to find the $\mathrm{Aut}(U)$-orbits of proper normal subgroups $K \trianglelefteq U$ with U/K cyclic of order dividing $q - 1$, and then for each such K determine ind_K. We make a case distinction on U.

If U is cyclic, then the possibilities are $K \in \{1, C_p, C_{p^2}\}$ with each $\mathrm{ind}_K = 1$; the number of groups is

$$c_6 = \Delta^p_{q-1} + \Delta^{p^2}_{q-1} + \Delta^{p^3}_{q-1}.$$

If $U \cong C_{p^2} \times C_p$, then there are two Aut(U)-orbits of normal subgroups K with $U/K \cong C_p$ and one Aut(U)-orbit of $K \trianglelefteq U$ with $U/K \cong C_{p^2}$; in each case, $\mathrm{ind}_K = 1$, so the number of groups is

$$c_7 = 2\Delta^p_{q-1} + \Delta^{p^2}_{q-1}.$$

If U is extraspecial of exponent p (or $U \cong Q_8$), then there is a unique Aut(U)-orbit of normal subgroups K with $U/K \cong C_p$; in this case, $\mathrm{ind}_K = 1$, and we have $c_8 = \Delta^p_{q-1}$ groups. If U is extraspecial of exponent p^2 (or $U \cong D_8$), then there are two Aut(U)-orbits of normal subgroups K with $U/K \cong C_p$; one has $\mathrm{ind}_K = 1$ and the other has $\mathrm{ind}_K = p-1$, which yields $c_9 = p\Delta^p_{q-1}$ groups. Lastly, if $U \cong C_p^3$, then there is one Aut(U)-orbit of $K \trianglelefteq U$ with $U/K \cong C_p$; here $\mathrm{ind}_k = 1$, and we have $c_{10} = \Delta^p_{q-1}$ groups.

Case 3: *Non-nilpotent with no normal Sylow subgroups.* The Fitting subgroup F satisfies $1 < F < G$ and, as in the proof of Theorem 2.1, we require that F does not contain a Sylow subgroup of G. This forces $|F| = p$ or $|F| = p^2$, and Lemma 3.7 yields $F \cong C_p^2$ as the only option. In this case G/F has order pq and embeds into $\mathrm{Aut}(F) \cong \mathrm{GL}_2(p)$, so $q \mid (p^2-1)$. If G/F has a normal subgroup of order p, then its preimage in G would be a normal Sylow subgroup, which is not possible. This shows that $G/F \cong C_p \ltimes C_q$ and $p \mid (q-1)$. Since we also have $q \mid (p^2-1)$, we deduce $(p,q) = (2,3)$; this case is treated separately.

In summary, the cases $(p,q) \in \{(2,3),(2,7)\}$ are dealt with by a direct computation. For the other cases, it remains to compute $5 + \sum_{i=6}^{10} c_i$ for $p = 2$ and $5 + \sum_{i=1}^{10} c_i$ for $p > 2$; this yields the claimed formulas. □

3.6. *The groups of order p^2q^2*

The groups of order p^2q^2 have been determined by Lin (1974), Le Vavasseur (1902) and Laue (1982). Lin's work has only minor mistakes and is essentially correct; it agrees with our work and Laue (1982, pp. 214-43). Lin seems unaware of Le Vavasseur (1902); we have not compared our results with those in Le Vavasseur (1902).

Proof of Theorem 2.1c). We assume $p > q$. Every group G of order p^2q^2 is solvable and there are four nilpotent groups of order p^2q^2. The case $(p,q) = (3,2)$ is dealt with by a direct calculation; if $(p,q) \neq (3,2)$, then the Sylow Theorem (Robinson, 1982, p. 40) implies that G has a normal Sylow p-subgroup. Below we assume that $G = U \ltimes N$ is non-nilpotent with $|N| = p^2$ and $|U| = q^2$. We use Proposition 3.6 below.

First, let N be cyclic, so $\mathrm{Aut}(N) \cong C_{p(p-1)}$. If U is cyclic as well, then Aut(N) has at most subgroup of order q and one subgroup of order q^2, respectively; this yields $c_1 = \Delta^{q^2}_{p-1} + \Delta^q_{p-1}$ groups. If U is not cyclic, then there is one Aut(U)-orbit of $K \trianglelefteq U$ with U/K nontrivial cyclic; this yields $c_2 = \Delta^q_{p-1}$ groups.

Now let N be non-cyclic and identify $\mathrm{Aut}(N) = \mathrm{GL}_2(p)$. For both possibilities of U, the Aut(U)-orbits of proper subgroups of U are $\mathcal{K} = \{1, C_q\}$. If $K \cong C_q$, then $U/K \cong C_q$ and $A_K = \mathrm{Aut}(U/K)$; it remains to count the number c_3 of conjugacy classes of subgroups of order q in $\mathrm{GL}_2(p)$; Proposition 3.2a) yields $c_3 = 2$ if $q = 2$ and $c_3 = \frac{q+3}{2}\Delta^q_{p-1} + \Delta^q_{p+1}$ otherwise. Note that c_3 has to be counted twice, for $U \cong C_{q^2}$ and for $U \cong C_q^2$. If $K = 1$, then $A_K = \mathrm{Aut}(U/K)$ and it remains to count the number c_4 of conjugacy classes of subgroups of order q^2 in $\mathrm{GL}_2(p)$; this time we obtain $c_4 = 1 + 4\Delta^4_{p-1} + \Delta^4_{p+1}$ if $q = 2$ and $c_4 = \Delta^q_{p-1} + \frac{q^2+q+2}{2}\Delta^{q^2}_{p-1} + \Delta^{q^2}_{p+1}$ otherwise. The number of groups of order p^2q^2 now is $4 + c_1 + c_2 + 2c_3 + c_4$. We use $\Delta^4_{p-1} = 1 - \Delta^4_{p+1}$ to rewrite the formula for $q = 2$. □

3.7. *The groups of order p^2qr*

The groups of order p^2qr have been considered by Glenn (1906) and Laue (1982). Glenn's work has several problems: some groups are missing, there are duplicates, and some invariants are not correct. Laue (1982, p. 244-62) also does not agree with Glenn (1906); we have not compared our results with those of Laue.

Proof of Theorem 2.1d). Every non-solvable group has a non-abelian simple composition factor, which implies that the only non-solvable group of order p^2qr is the alternating group A_5 of order 60, see Dietrich and Eick (2005, Theorem 2). There are $c_0 = 2$ nilpotent groups of order p^2qr, and we now consider solvable non-nilpotent groups G of order p^2qr. We make a case distinction on the Fitting subgroup $F \leqslant G$. By assumption, $1 < F < G$, and Lemma 3.7 implies that G/F embeds into $\mathrm{Aut}(F)$. We organise our case distinction by the number of prime factors of $|F|$; as before, we freely use Proposition 3.6.
Case 1: *$|F|$ is a prime.* If $|F| = p$, then $\mathrm{Aut}(F) = C_{p-1}$ and $G/F \cong C_{prq}$. This implies that G has a normal (nilpotent) Sylow p-subgroup, a contradiction to $|F| = p$. If $|F| = q$, then $|G/F| = p^2r$ divides $q-1$, contradicting $r > q$. If $|F| = r$, then $G \cong C_{p^2q} \ltimes F$, and there are $c_1 = \Delta_{r-1}^{p^2q}$ such groups; note that $c_1 = \Delta_{r-1}^{p^2}$ for $q = 2$.
Case 2: *$|F|$ is the product of two primes.* If $F \cong C_{p^2}$, then $G \cong C_{qr} \ltimes F$ and $qr \mid (p-1)$; this gives $c_2 = \Delta_{p-1}^{qr}$ groups, with $c_2 = w_{p-1}^{r}$ if $q = 2$. If $F \cong C_p^2$, then G splits over F and G/F can be considered as a subgroup of $\mathrm{GL}_2(p)$ of order qr. Using Proposition 3.2c), the number of groups arising in this case is

$$c_3 = \begin{cases} \frac{3r+7}{2}\Delta_{p-1}^{r} + 2\Delta_{p+1}^{r} & (\text{if } q = 2) \\ \frac{qr+q+r+5}{2}\Delta_{p-1}^{qr} + \Delta_{p^2-1}^{qr}(1-\Delta_{p-1}^{qr}) & (\text{otherwise.}) \end{cases}$$

If $F \cong C_{pq}$, then $G/F \cong C_{pr}$ embeds into $\mathrm{Aut}(F) = C_{p-1} \times C_{q-1}$; since $r > q$, we have $r \mid (p-1)$ and $p \mid (q-1)$, but $r \leqslant p-1 \leqslant q-2$ also contradicts $r > q$.

If $F \cong C_{pr}$, then $G/F \cong C_{pq}$, which forces $p \mid (r-1)$. Note that G splits over the (normal) Sylow r-subgroup of F, so $G \cong \bar{G} \ltimes C_r$ where $\bar{G}$ has Fitting subgroup $\bar{F} \cong C_p$ with $\bar{G}/\bar{F} \cong C_{pq}$. There are two cases to consider. First, suppose that the Sylow q-subgroup of G/F acts non-trivially on the Sylow p-subgroup of F. Then $q \mid (p-1)$ and $G \cong G/F \ltimes_\varphi F$ follows from Lemma 3.4 applied to $\bar{F}$ and $\bar{G}/\bar{F}$. As in Proposition 3.6, the number of such groups is given by the number of subgroups of order pq in $\mathrm{Aut}(F)$. As the image of the Sylow p-subgroup of G/F under φ is uniquely determined, the number of groups is determined by the number of subgroups of order q in $\mathrm{Aut}(F) \cong C_{p-1} \times C_{r-1}$ that act non-trivially on the Sylow p-subgroup of F; this number is $1 + (q-1)\Delta_{r-1}^{q}$. Second, suppose that the Sylow q-subgroup of G/F acts trivially on the Sylow p-subgroup of F; then $q \mid (r-1)$ and the action of G/F on F is uniquely determined. By Lemma 3.4, there are two isomorphism types of extensions in this case. In summary, if $F \cong C_{pr}$, then the number of groups is

$$c_4 = \begin{cases} 4\Delta_{r-1}^{p} & (\text{if } q = 2) \\ \Delta_{r-1}^{p}(\Delta_{p-1}^{q}(1 + (q-1)\Delta_{r-1}^{q}) + 2\Delta_{r-1}^{q}) & (\text{otherwise.}) \end{cases}$$

If $F \cong C_{qr}$, then $G = U \ltimes_\varphi F$ with $|U| = p^2$. We have to count the number of subgroups of order p^2 in $\mathrm{Aut}(F) \cong C_{q-1} \times C_{r-1}$. The number of subgroups C_p^2 is $c_5' = \Delta_{q-1}^{p}\Delta_{r-1}^{p}$, and it remains determine the number of subgroups C_{p^2}. This number depends on $\gcd(q-1, p^2) = p^a$ and $\gcd(r-1, p^2) = p^b$. If $a, b \leqslant 1$, then there is no subgroup C_{p^2}. If $(a,b) \in \{(2,0),(0,2)\}$, then there is one subgroup each; if $(a,b) \in \{(2,1),(1,2)\}$, then there are p subgroups each; if $(a,b) = (2,2)$, then there are $p(p+1)$ subgroups. Together, the number of cyclic subgroups C_{p^2} is

$$c_5'' = p(p+1)\Delta_{q-1}^{p^2}\Delta_{r-1}^{p^2} + \sum_{(u,v)\in\{(q,r),(r,q)\}} \left(\Delta_{u-1}^{p^2}(1-\Delta_{v-1}^{p}) + p\Delta_{u-1}^{p^2}\Delta_{v-1}^{p}(1-\Delta_{v-1}^{p^2})\right).$$

In summary, if $F \cong C_{qr}$, then we get $c_5 = c_5' + c_5''$ groups, which can be written as $c_5 = \Delta_{r-1}^{p^2}$ for $q = 2$, and if $q > 2$, then

$$c_5 = (p^2-p)\Delta_{q-1}^{p^2}\Delta_{r-1}^{p^2} + (p-1)(\Delta_{q-1}^{p^2}\Delta_{r-1}^{p} + \Delta_{r-1}^{p^2}\Delta_{q-1}^{p}) + \Delta_{q-1}^{p^2} + \Delta_{r-1}^{p^2} + \Delta_{q-1}^{p}\Delta_{r-1}^{p}.$$

Case 3: *$|F|$ is the product of three primes.* If $F \cong C_{pqr}$, then $G = U \ltimes_\varphi N$ with $N \cong C_{qr}$ and $|U| = p^2$, and $\ker\varphi \cong C_p$. The group U is either cyclic or elementary abelian, but in both cases there is a unique $\mathrm{Aut}(U)$-orbit of normal subgroups $K \trianglelefteq U$ with $K \cong C_p$, and we have $A_K = \mathrm{Aut}(U/K)$; it remains to count the number of subgroups C_p in $\mathrm{Aut}(N) \cong C_{q-1} \times C_{r-1}$. If $F \cong C_{pqr}$, then the number of groups is

$$c_6 = \begin{cases} 2\Delta_{r-1}^{p} & (\text{if } q=2) \\ 2(\Delta_{q-1}^{p} + \Delta_{r-1}^{p} + (p-1)\Delta_{q-1}^{p}\Delta_{r-1}^{p}) & (\text{otherwise.}) \end{cases}$$

If $|F| = p^2q$, then $G = U \ltimes_\varphi F$ with $F = N \times M$ with $|N| = p^2$, $M \cong C_q$, and $U \cong C_r$. We have to count the number of conjugacy class representatives of subgroups of order r in $\mathrm{Aut}(F) \cong \mathrm{Aut}(N) \times C_{q-1}$. Since $r > q$, we need to count the number of conjugacy classes of subgroups of order r in $\mathrm{Aut}(N)$. If N is cyclic, then $\mathrm{Aut}(N) \cong C_{p(p-1)}$ and we get Δ_{p-1}^{r} groups; if $N \cong C_p^2$, then $\mathrm{Aut}(N) \cong \mathrm{GL}_2(p)$ and Proposition 3.2a) applies. In summary, if $|F| = p^2q$, then the number of groups is

$$c_7 = \tfrac{r+5}{2}\Delta_{p-1}^{r} + \Delta_{p+1}^{r}.$$

The case $|F| = p^2r$ is dual to the previous one, with the exception that now the bigger prime $r > q$ divides $|F|$. We have $G = U \ltimes_\varphi F$ and there are two possibilities for F. If $F \cong C_{p^2r}$, then $\mathrm{Aut}(F)$ is isomorphic to $C_{p(p-1)} \times C_{r-1}$ and we count the desired subgroups as

$$c_8' = \Delta_{p-1}^{q} + \Delta_{r-1}^{q} + (q-1)\Delta_{p-1}^{q}\Delta_{r-1}^{q}.$$

The final case $F \cong C_p^2 \times C_r$ is more complicated and required a slightly different approach. All groups in this case have the form $G = U \ltimes_\varphi N$ with $N \cong C_p^2$ and $|U| = qr$ such that φ has kernel of order $r \mid |K|$, where U/K is cyclic. There are two possibilities for U, either $U \cong C_{qr}$ or $U \cong C_q \ltimes C_r$ with $q \mid (r-1)$. If U is cyclic, then $K \cong C_r$ (since G is non-nilpotent); now we count the conjugacy classes of subgroups of order q in $\mathrm{Aut}(N)$, which by Proposition 3.2 is determined as $c_8'' = 2$ if $q = 2$ and $c_8'' = \frac{q+3}{2}\Delta_{p-1}^{q} + \Delta_{p+1}^{q}$ otherwise. If U is non-abelian, then $|K| \in \{r, qr\}$. If $K \cong C_{qr}$, then φ is trivial hence there are $c_8''' = \Delta_{r-1}^{q}$ groups. It remains to consider $K \cong C_r$. Studying $\mathrm{Aut}(U)$ via the proof of Proposition 3.3, one can deduce that $A_K = 1$. Thus, if $\mathcal{S}$ is a set of conjugacy class representatives of subgroups of order q in $\mathrm{GL}_2(p)$, then the number of groups arising in this case is

$$\Delta_{r-1}^{q} \sum\nolimits_{S \in \mathcal{S}} |\mathrm{Aut}(U/K)/A_S|.$$

Here A_S can be determined via Proposition 3.2a), and since $\mathrm{Aut}(U/K) \cong C_{q-1}$, it follows that there are $c_8'''' = 2$ groups if $q = 2$, and if $q > 2$, then

$$c_8'''' = \Delta_{r-1}^{q}\left(\tfrac{(q-1)(q+2)}{2}\Delta_{p-1}^{q} + \tfrac{q-1}{2}\Delta_{p+1}^{q}\right).$$

In summary, this case adds $c_8 = c_8' + c_8'' + c_8''' + c_8''''$ groups, which is $c_8 = 8$ if $q = 2$, and if $q > 2$ then

$$c_8 = \tfrac{(q-1)(q+4)}{2}\Delta_{p-1}^{q}\Delta_{r-1}^{q} + \tfrac{q-1}{2}\Delta_{p+1}^{q}\Delta_{r-1}^{q} + \tfrac{q+5}{2}\Delta_{p-1}^{q} + 2\Delta_{r-1}^{q} + \Delta_{p+1}^{q}.$$

Now $c_0 + c_1 + \ldots + c_8$ yields the formula for $p^2qr \neq 60$ given in the theorem. □

4. Construction and identification

For $n \in \mathcal{O}$ let $\mathcal{G}_n$ be the list of all (isomorphism types of) groups of order n.

4.1. Construction by ID

The proof Theorem 2.1 determines the size $\mathcal{N}(n)$ of $\mathcal{G}_n$ by making various case distinctions on the structure of the groups G of order n. Distinguishing features are to consider whether G is nilpotent or non-nilpotent, whether G has a normal Sylow subgroup, or whether the Fitting subgroup of G has a specific structure. For each of these properties, the counting formulas developed in the proof of Theorem 2.1 tell us exactly how many isomorphism types of these groups exist. This allows us to partition $\mathcal{G}_n$ into various *clusters* such that the groups within one cluster are split extensions that essentially only differ by having different action homomorphisms; it then remains to sort the different actions in a canonical way; this is explained in the proof of Theorem 2.1 and makes use of the canonical generators and matrices defined in Notation 2.3. The formulas for the numbers of groups in each cluster (see the right columns in the tables) are the key ingredient that allows us to directly construct the i-th group in $\mathcal{G}_n$ *without* constructing the whole list of group. A similar approach is used for the construction functionality provided by the SmallGroups library and by the algorithms in Dietrich and Low (2021); please cf. Footnote 1. Here we exemplify this approach by discussing the groups of order p^2q; extensive details for all order types are given in the MPhil thesis Pan (2021) of the third author.

Example 4.1. Let $n = p^2q$ with $q > 2$. The proof of Theorem 2.1 partitions the groups in $\mathcal{G}_n$ in five clusters as given in Table 1. The groups in Cluster 1 are nilpotent and can be sorted by their exponents. Clusters 3 and 4 each contain at most one group, and so does Cluster 2 if $q \nmid (p-1)$. Cluster 5 contains at most two groups, and they can be distinguished by the order of the action group (the Sylow p-subgroup acting on the Sylow q-subgroup). If $q \mid (p-1)$, then Cluster 2 contains $(q+3)/2$ isomorphism types of groups and these are parametrised by the conjugacy classes of diagonalisable subgroups of $\mathrm{GL}_2(p)$ of order q, see the proof of Proposition 3.2a). The latter proof also explains how to list these classes canonically: if $\sigma_p \in \mathbb{Z}_p^*$ and $\sigma_q \in \mathbb{Z}_q^*$ are the canonical generators and $a = \sigma_p^{(p-1)/q}$, then the subgroups we have to consider can be sorted as $\langle \mathrm{diag}(a,1)\rangle$ and $\langle M(p,q,\sigma_q^k))\rangle$ with $k \in \{0,\dots,(q-1)/2\}$, where each $M(p,q,\sigma_q^k) = \mathrm{diag}(a, a^{\sigma_q^k})$. For example, if $n = 29^2.7$, then Clusters 1–5 have 2, 5, 1, 0, 0 groups, respectively, so the group with ID $(29^2.7, 6)$ is $G = C_7 \ltimes C_{29}^2$ where a generator $u \in C_7$ acts on generators $v, w \in C_{29}^2$ via $M(29,7,\sigma_7^2) = \mathrm{diag}(a, a^{(\sigma_7^2)})$; here $\sigma_{29} = 2$ and $\sigma_7 = 3$, so $a = \sigma_{29}^4 = 16$ and $a^{(\sigma_7^2)} = 24$. Thus, G can be defined via the presentation $\langle u, v, w \mid u^7, v^{29}, w^{29}, w^v/w, v^u/v^{16}, w^u/w^{24}\rangle$.

4.2. Identification of groups

The identification of groups of order $n \in \mathcal{O}$ reverses the construction process: given a group G of order n, we first determine to which cluster the group belongs by computing the Fitting and Sylow subgroups. Then we determine the actions that arise. Lastly, it remains to decide to which canonical action (namely, the one used in the construction-by-ID) this action is equivalent to. We exemplify this process with another example and refer to Pan (2021) for more information; the main idea is to exploit the known structure of the relevant action groups described in the proof of Proposition 3.2.

Example 4.2. Consider the group $G = \langle u, v, w \mid u^7, v^{29}, w^{29}, w^v/w, v^u/v^{24}, w^u/v^{11}w^7\rangle$. We determine $n = |G| = 29^2.7$ and compute a Sylow 29-subgroup N and a Sylow 7-subgroup U. We find $N \trianglelefteq G$, so G is a split extension of U by N. Since $N \cong C_{29}^2$, we know that G is a group in Cluster 2 as given in Table 1. We choose generators $u \in U$ and $v, w \in N$ and observe that $v^u = v^{24}$ and $w^u = v^{11}w^7$. (Here this can be determined directly from the presentation, but if G is given as a matrix or permutation group, then we would have likely chosen different generators.) Thus, u acts on v, w via $\left(\begin{smallmatrix} 24 & 0 \\ 11 & 7 \end{smallmatrix}\right) \in \mathrm{GL}_2(29)$. This matrix has eigenvalues $\{24, 7\}$, so it is conjugate to $\mathrm{diag}(24,7) = \mathrm{diag}(a^2, a^3)$ with $a = 16$ as in Example 4.1. We have $\mathrm{diag}(a^2,a^3)^4 = \mathrm{diag}(a, a^{(3^5)}) = M(29,7,\sigma_7^5)$, but the parameter 5 is greater than $(q-1)/2 = 3$; since $3^{-5} = 3$ in $\mathbb{Z}_7^*$, the proof of Proposition 3.2a) shows that

$\langle M(29, 7, \sigma_7^5)\rangle$ is conjugate to $\langle M(29, 7, \sigma_7)\rangle$. This determines the parameter $k = 1$, and therefore G has ID $(29^2.7, 5)$.

4.3. Implementation and performance

A GAP implementation of our algorithms is available in Pan (2021). Using this implementation we checked that our determination coincides (up to permuting the ordering of the lists of groups) with that in the SmallGroups library, that obtained by the GrpConst package, see Besche et al. (2002), and that obtained by the Cubefree package, see Dietrich and Eick (2005) and Dietrich and Wilson (2020), for a large range of orders.

We now comment on the performance of our algorithms; all computations have been carried out with GAP 4.11.0 on a computer with Intel(R) Core(TM) i5-7500 CPU@3.40GHz and 16GB RAM.[2] At the time of writing, the SmallGroups library contains the following orders discussed in this paper: p^2q for all primes $p \neq q$, and $q^n p$ for primes $p \neq q$ with q^n dividing one of $\{2^8, 3^6, 5^5, 7^4\}$, and all relevant orders up to 2000.

- There are 20514 groups of order p^2q at most 10^5. SmallGroups required 196 seconds to construct these groups, while our code took 16 seconds. Our code identified the groups constructed with SmallGroups in 78 seconds, whereas SmallGroups required 778 seconds to identify our groups. Up to order 10^6, there are 159800 groups and our code required 120 seconds for the construction; SmallGroups took 15181 seconds. The reason for the increased runtime of SmallGroups is because for some order types the construction of groups involves some computations (akin to the ones described below), whereas our code directly writes down the group presentations.
- There are 74562 groups of order p^2q, p^3q, p^2q^2 or p^2qr at most 50000 available in the SmallGroups library. Our code required 47 seconds to construct these groups, whereas SmallGroups required 27359 seconds. Moreover, SmallGroups took 43356 seconds to identify our groups, while our code required 259 seconds to identify the groups constructed with SmallGroups.
- Our code is also practical for larger primes; e.g. the construction of the 37371, 6566, and 21348 groups of order $9341^3.467$, $127691^2.113^2$, and $415631^2.467.89$ took 32, 5, and 17 seconds, respectively.[3] For such large primes we cannot compare our result with those of `GrpConst` or `Cubefree`, because the latter computations do not terminate in reasonable time (within a few hours). This is partly because these packages use general purpose algorithms which invoke computations with group homomorphisms and matrix groups. Our code avoids these bottlenecks by directly writing down polycyclic presentations of the (solvable) groups; the main bottleneck in our code seems to be GAP's pc-group arithmetic for large primes.

We plan to extend the functionality of our implementation to other order types. For example, we will soon include construction and identification functionality for groups of order p^4q, that is, our work makes most of the enumeration results of Eick and Moede (2018) constructive.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

Besche, H.U., Eick, B., 1999. Construction of finite groups. J. Symb. Comput. 27, 387–404.

[2] All our runtimes have been determined by using the option USE_NC:=true in our code: this avoids that GAP tests consistency of polycyclic presentations, which becomes a major bottleneck when large primes are involved.

[3] The performance of our code is even better (5, 1, and 3 seconds, respectively) if groups are returned as GAP objects `pcp-group` (instead of `pc-group`) by setting USE_PCP:=true.

Besche, H.U., Eick, B., O'Brien, E. SmallGroups – a library of groups of small order. Version 1.4.2. A GAP 4 package available at gap-system.org/Packages/smallgrp.html.

Besche, H.U., Eick, B., O'Brien, E.A., 2002. A millenium project: constructing small groups. Int. J. Algebra Comput. 12, 623–644.

Blackburn, S., Neumann, P., Venkataraman, G., 2007. Enumeration of Finite Groups. Cambridge University Press.

Bosma, W., Cannon, J., Playoust, C., 1997. The magma algebra system I: the user language. J. Symb. Comput. 24, 235–265.

Cole, F.N., Glover, J.W., 1893. On groups whose orders are products of three prime factors. Am. J. Math. 15, 191–220.

Conway, J., Dietrich, H., O'Brien, E., 2008. Counting groups: gnus, moas and other exotica. Math. Intell. 30, 6–15.

Dietrich, H., Eick, B., 2005. Groups of cube-free order. J. Algebra 292, 122–137.

Dietrich, H., Low, D., 2021. Generation of finite groups with cyclic Sylow subgroups. J. Group Theory 24, 161–175.

Dietrich, H., Wilson, J.B., 2020. Isomorphism testing of groups of cube-free order. J. Algebra 545, 174–197.

Eick, B., 2017. Enumeration of groups whose order factorises in at most 4. arXiv:1702.02616.

Eick, B., Horn, M., Hulpke, A., 2017. Constructing groups of 'small' order: recent results and open problems. In: Algorithmic and Experimental Methods in Algebra, Geometry, and Number Theory. Springer, Cham, pp. 199–211.

Eick, B., Moede, T., 2018. The enumeration of groups of order p^nq for $n \leqslant 5$. J. Algebra 507, 571–591.

GAP – Groups, Algorithms and programming, Version 4.11.0. Available at gap-system.org.

Girnat, B., 2003. Klassifikation der Gruppen bis zur Ordnung p^5. Staatsexamensarbeit. TU, Braunschweig. See arXiv:1806.07462 for an alternative presentation of the results, 2018.

Glenn, O.E., 1906. Determination of the abstract groups of order p^2qr; p, q, r being distinct primes. Trans. Am. Math. Soc. 7, 137–151.

Holt, D.F., Eick, B., O'Brien, E.A., 2005. Handbook of Computational Group Theory. Discrete Mathematics and Its Applications. Chapman & Hall/CRC, FL.

Hölder, O., 1893. Die Gruppen der Ordnungen p^3, pq^2, pqr, p^4. Math. Ann. 43, 301–412.

Hölder, O., 1895. Die Gruppen mit quadratfreier Ordnungzahl. Nachr Ges. Wiss. Göttingen, Math.-Phys. Kl, pp. 211–229.

Laue, R., 1982. Zur Konstruktion und Klassifikation endlicher auflösbarer Gruppen. Bayreuth. Math. Schr. 9. ii+304 pp.

Le Vavasseur, R., 1899. Les groupes d'ordre p^2q^2, p étant un nombre premier plus grand que le nombre premier q. C. R. Acad. Sci. Paris 128, 1152–1153.

Le Vavasseur, R., 1902. Les groupes d'ordre p^2q^2, p étant un nombre premier plus grand que le nombre premier q. Ann. Éc. Norm. 19, 335–355.

Lin, H.-L., 1974. On groups of order p^2q, p^2q^2. Tamkang J. Math. 5, 167–190.

Pan, X., 2021. Groups of small order type. MPhil thesis. Monash University. Thesis and GAP code accompanying this paper are available at github.com/xpan-eileen/sotgrps_gap_pkg.

Robinson, D.J.S., 1982. A Course in the Theory of Groups. Springer-Verlag.

Short, M.W., 1992. The Primitive Soluble Permutation Groups of Degree Less than 256. Lecture Notes in Mathematics, vol. 1519. Springer-Verlag, Berlin.

Slattery, M.C., 2007. Generation of groups of square-free order. J. Symb. Comput. 42, 668–677.

Taunt, D., 1955. Remarks on the isomorphism problem in theories of construction of finite groups. Proc. Camb. Philos. Soc. 51, 16–24.

Western, A., 1899. Groups of order p^3q. Proc. Lond. Math. Soc. 30, 209–263.

Winter, D.L., 1972. The automorphism group of an extraspecial p-group. Rocky Mt. J. Math. 2, 159–168.