CLASSIFICATION OF FINITE GROUPS WITH BIRDCAGE-SHAPED HASSE DIAGRAMS

Shigeru TAKAMURA

Takamura, S.
Osaka J. Math.
58 (2021), 885–897

CLASSIFICATION OF FINITE GROUPS WITH BIRDCAGE-SHAPED HASSE DIAGRAMS

Shigeru TAKAMURA

(Received May 13, 2020, revised July 15, 2020)

Abstract

The subgroup posets of finite groups are illustrated by graphs (*Hasse diagrams*). The properties of these graphs have been studied by many researchers — initiated by K. Brown and D. Quillen for p-subgroups. We consider the opposite direction, that is, a realization problem: *Given a graph, when does a finite group with its Hasse diagram being the graph exist?, and if any, classify all such finite groups.* The Hasse diagram of a group is not arbitrary — it has the top and the bottom vertices, and they are connected by paths of edges. We divide such graphs into two types "branched" and "unbranched", where unbranched graphs are birdcage-shaped, and finite groups with their Hasse diagrams being such graphs are called *birdcage groups*. We completely classify the unbranched case: *A birdcage group is either a cyclic group of prime power order or a semidirect product of two cyclic groups of prime orders* (*the orders are possibly equal*). In the former, the Hasse diagram is a straight line (a birdcage with a single bar) and in the latter, a birdcage with all bars being of length 2.

1. Introduction

Notation. id is the identity element of a group and $\mathbb{Z}_n$ is the cyclic group of order n.

For a finite group, the inclusion relations between its subgroups are geometrically illustrated by a *Hasse diagram* — a graph whose vertices consist of the subgroups of the finite group, and two vertices are connected by an edge if there is an inclusion relation between them and *no* subgroup lies between them. For the identity group, this graph is degenerated, consisting only of a single vertex. *In what follows, the finite group is assumed to be not the identity group.* Then this graph has two special vertices: the *top vertex* (corresponding to the finite group itself) and the *bottom vertex* (corresponding to the identity subgroup); they are connected by paths of edges. This graph is said to be *unbranched* (or *birdcage-shaped*) if there is no branch at any "intermediate" vertex between the top and the bottom vertices (while there *may* be branches at the top and the bottom vertices). Otherwise it is said to be *branched*. Compare Figure 1 (1), (2) with (3).

In an unbranched graph, a path connecting the top and the bottom vertices is called a *bar* (the numbers of bars in Figure 1 (1), (2) are six and one). The *length* of a bar is the number of its edges, and the *height* of an unbranched graph is the maximum of lengths of its bars (the heights of Figure 1 (1), (2) are five and four). We will show the following (Proposition 5.2): *If an unbranched graph is the Hasse diagram of a finite group, then the number of its*

2020 Mathematics Subject Classification. Primary 05C25; Secondary 20E34.

bars is not *arbitrary, but* 1, 2, *or* $p + 1$ *for some prime* p: *in the case of* "2 or $p + 1$", *the height of the unbranched graph is* always 2 (*in fact the lengths of all bars are* 2), *while in the case of* "1", *the length of the single bar may be arbitrarily large*.

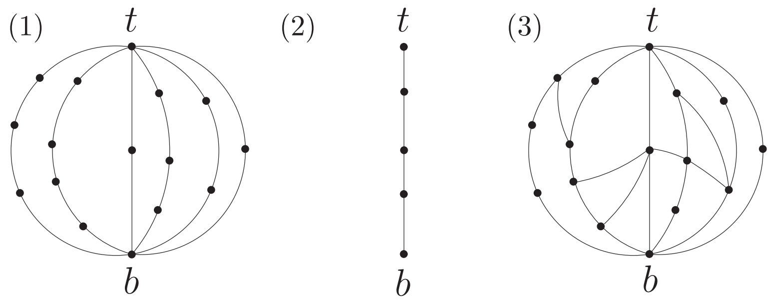

Fig. 1. Black circles are vertices; t and b are the top and the bottom ones. (1), (2) are unbranched (or birdcage-shaped) graphs, though (1) has branches at t and b. (3) is a branched graph.

Throughout this paper, we adopt the following:

Convention 1.1. (i) The Hasse diagram of the subgroup poset of a finite group is simply called the *Hasse diagram of the finite group*.

(ii) Two terms "Hasse diagram" and "its underlying graph" are interchangeably used, though the latter does not carry the information about the subgroups corresponding to vertices.

The properties of the Hasse diagrams of finite groups have been investigated by many researchers, pioneered by K. Brown [2] and D. Quillen [4] for p-subgroups (see [7] for details on this subject). In this paper we conversely start with (special) graphs and study the realization problem: when they are realized as the Hasse diagrams of some finite groups. The motivation behind this is that we are concerned with classifying finite groups in terms of graphs — Hasse diagrams — as well as characterizing the graphs that are the Hasse diagrams of some finite groups:

(P1) *What kinds of graphs could be the Hasse diagrams of some finite groups?*

(P2) *Classify all finite groups with their Hasse diagrams being equal to a given graph.*

In this paper we completely classify the finite groups whose Hasse diagrams are unbranched graphs — such finite groups are called *birdcage groups*, as their Hasse diagrams are "birdcage-shaped". For example, a direct product group $\mathbb{Z}_p \times \mathbb{Z}_q$ for any primes p and q is a birdcage group, whose Hasse diagram, depending on whether $p \neq q$ or $p = q$, is illustrated in (1) or (2) of Figure 2. An example of a nonabelian birdcage group is a *nontrivial* semidirect product $\mathbb{Z}_p \rtimes \mathbb{Z}_q$ of two cyclic groups of prime orders, where "nontrivial" means that $\mathbb{Z}_p \rtimes \mathbb{Z}_q$ is *not* a direct product. Its Hasse diagram is illustrated in (3) of Figure 2. The symmetric group $\mathfrak{S}_3$ of degree 3 is a nonabelian birdcage group, as $\mathfrak{S}_3 = \mathbb{Z}_3 \rtimes \mathbb{Z}_2$, where $\mathbb{Z}_3$ is generated by the cyclic permutation $(1\,2\,3)$ and $\mathbb{Z}_2$ is generated by a transposition $(1\,2)$.

An example of a *non*-birdcage group is $\mathbb{Z}_p \times \mathbb{Z}_q \times \mathbb{Z}_r$ where p, q, r are (not necessarily distinct) primes. In the case that p, q, r are distinct, its Hasse diagram is illustrated in Figure 3, and indeed not birdcage-shaped — branched at six vertices $\mathbb{Z}_p \times \mathbb{Z}_q$, $\mathbb{Z}_p \times \mathbb{Z}_r$, $\mathbb{Z}_q \times \mathbb{Z}_r$, $\mathbb{Z}_p$,

$\mathbb{Z}_q, \mathbb{Z}_r$.

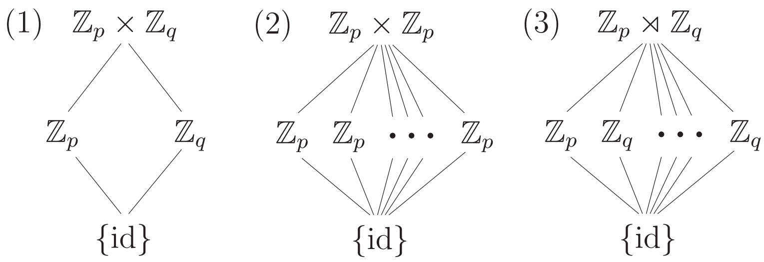

Fig. 2. In (2), the second row consists of $(p + 1)$ $\mathbb{Z}_p$'s, and the number of bars is $p + 1$. In (3), the second row consists of one $\mathbb{Z}_p$ and p $\mathbb{Z}_q$'s, and the number of bars is $p + 1$. See Proposition 5.2.

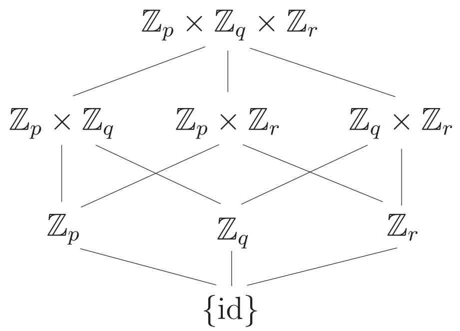

Fig. 3. The Hasse diagram of $\mathbb{Z}_p \times \mathbb{Z}_q \times \mathbb{Z}_r$ for distinct primes p, q, r.

Our main result is as follows (see §5 for the proof):

Classification Theorem *A birdcage group is either a cyclic group $\mathbb{Z}_{p^n}$ of prime power order or a semidirect product group $\mathbb{Z}_p \rtimes \mathbb{Z}_q$ of two cyclic groups of prime orders* (*possibly $p = q$, in which case this is a direct product group $\mathbb{Z}_p \times \mathbb{Z}_q$*). *Here*:

(a) *In the former case, its Hasse diagram is a straight line* (*a birdcage-shaped graph with a single bar*) *consisting of n edges*: *Explicitly* $\{\mathrm{id}\} - \mathbb{Z}_p - \mathbb{Z}_{p^2} - \cdots - \mathbb{Z}_{p^n}$.

(b) *In the latter case, its Hasse diagram is a birdcage-shaped graph with all bars being of length* 2 (*in contrast, in the former case, the length n of the straight line may be arbitrarily large*).

Consequently except for the two types (a) and (b), the other birdcage-shaped graphs cannot be the Hasse diagrams of finite groups.

Remark 1.2. Properties of $\mathbb{Z}_p \rtimes \mathbb{Z}_q$ are summarized in §6: To define a *nontrivial* semidirect product $\mathbb{Z}_p \rtimes \mathbb{Z}_q$ (which is not $\mathbb{Z}_p \times \mathbb{Z}_q$), the primes p and q are *not* arbitrary, but q must divide $p - 1$ (Lemma 6.2 (3)), and moreover in this case a nontrivial semidirect product of $\mathbb{Z}_p$ and $\mathbb{Z}_q$ is unique (Proposition 6.5).

Iterated birdcage groups Birdcage groups are generalized to "iterated" birdcage groups, which are obtained by iterated application of group extensions to birdcage groups (e.g. the alternating group $\mathfrak{A}_4$ of degree 4 and the quaternion group Q_8 of order 8). Their Hasse diagrams are no longer birdcage-shaped, but branched — "modified birdcage-shaped": as we iterate group extensions, the Hasse diagrams generally become more and more complicated and branched (cf. iterated torus knots in knot theory). This will be discussed in our subsequent paper, in light of *algebro-geometric* group theory we formulate there — which is based on "birational viewpoint", e.g. "blow down" corresponding to the quotient of a group by a normal subgroup, and "blow up" to a group extension. *The dynamic changes of Hasse diagrams after blow up and down is of fundamental importance, in addition to the static classification of Hasse diagrams.*

2. Preparation

Let G be a group. A set of subgroups $\{K_\lambda\}_{\lambda\in\Lambda}$ of G is called a *concise system* if $K_\lambda \not\subset K_\mu$ for any distinct $\lambda, \mu \in \Lambda$; then for the subgroup $H := \langle K_\lambda \rangle_{\lambda\in\Lambda}$ of G generated by K_λ ($\lambda \in \Lambda$), we say that $\{K_\lambda\}_{\lambda\in\Lambda}$ is a *genesis* of H (genesis < *gene*rating subgroup-*sys*tem). Note that $\{H\}$ itself is a genesis of H.

We will show that a group G whose subgroup poset is 'aligned', such as $\{\mathrm{id}\} \subset H_1 \subset H_2 \subset \cdots \subset H_n \subset \cdots \subset G$, has only one genesis — the trivial one $\{G\}$. We begin with formulation:

Definition 2.1. A group G is *straight* if its subgroup poset $\{H_\alpha\}_{\alpha\in A}$ is *aligned*, i.e. A is a totally ordered set such that $H_\alpha \subset H_\beta$ if $\alpha \leq \beta$.

Lemma 2.2. *If G is a straight group, then $\{G\}$ is a unique genesis of G.*

Proof. Let $\{H_\alpha\}_{\alpha\in A}$ be the subgroup poset of G, where A is a totally ordered set such that $H_\alpha \subset H_\beta$ if $\alpha \leq \beta$. A genesis of G is then of the form $\{H_\alpha\}_{\alpha\in B}$, where $B \subset A$ (so, B is also totally ordered). It suffices to show that B consists of a single element (in which case the genesis is necessarily $\{G\}$). If B contains at least two elements, then the straightness of G implies that for any distinct $\alpha, \beta \in B$ such that $\alpha \leq \beta$, we have $H_\alpha \subset H_\beta$. This however contradicts the conciseness of $\{H_\alpha\}_{\alpha\in B}$. □

Example 2.3. Any cyclic group $\mathbb{Z}_{p^n}$ of prime power order is straight: its subgroup poset is aligned as $\{\mathrm{id}\} \subset \mathbb{Z}_p \subset \mathbb{Z}_{p^2} \subset \cdots \subset \mathbb{Z}_{p^n}$. Note that $\mathbb{Z}_{p^n}$ has only one genesis $\{\mathbb{Z}_{p^n}\}$ by Lemma 2.2.

Example 2.3 indicates that any subgroup of a straight group is also straight. This is indeed true, because the subgroup poset of any subgroup of a straight group is necessarily aligned. Conversely if any subgroup of a group G is straight, then in particular G is straight. The following thus holds:

Lemma 2.4. *A group G is straight if and only if any subgroup of G is straight.*

Before proceeding, we clarify the difference between "largest subgroup" and "maximal subgroup":

Definition 2.5. Let G be a (not necessarily finite) group.

(1) A proper subgroup L of G is called a *largest* subgroup of G if $H \subset L$ for any proper subgroup H of G. Note that a largest subgroup if exists is *unique*: Say L' is another

largest subgroup of G, then $L' \subset L$ and $L \subset L'$, so $L' = L$.

(2) A proper subgroup M of G is called a *maximal* subgroup of G if there exists *no* proper subgroup H of G such that $M \subsetneq H$. Note that even if a maximal subgroup exists, it is generally not unique.

Note that if a group G has a largest subgroup, then G cannot have more than one maximal subgroup — the largest subgroup is the unique maximal subgroup. If G is infinite, then G may have *no* maximal subgroup (in which case G has no largest subgroup). In contrast if G is finite, then G *does* have (finitely many) maximal subgroups, and the following hold:

(i) If G has only one maximal subgroup M, then M is a largest subgroup of G, and vice versa.

(ii) If G has more than one maximal subgroups, then G has *no* largest subgroup.

For an infinite group G, (i) may fail (while (ii) holds): Even if G has only one maximal subgroup, G may have *no* largest subgroup.

Example 2.6. We identify a cyclic group $\mathbb{Z}_{p^n}$ of prime power order with the multiplicative group of p^nth roots of unity. From the sequence of inclusions $\mathbb{Z}_p \hookrightarrow \mathbb{Z}_{p^2} \hookrightarrow \cdots \hookrightarrow \mathbb{Z}_{p^n} \hookrightarrow \cdots$, the direct limit group $H := \varinjlim_n \mathbb{Z}_{p^n}$ is constructed. Set $G := H \times \mathbb{Z}_2$ (the direct product group of H and $\mathbb{Z}_2 = \{\pm 1\}$). Then G has only one maximal subgroup $H \times \{1\}$, but has no largest subgroup (see Figure 4): note that $\{1\} \times \mathbb{Z}_2 \subset \mathbb{Z}_p \times \mathbb{Z}_2 \subset \mathbb{Z}_{p^2} \times \mathbb{Z}_2 \subset \cdots \subset \mathbb{Z}_{p^n} \times \mathbb{Z}_2 \subset \cdots$ does *not* attain a largest subgroup, as it is an infinite increasing "unbounded" sequence. Note also that the subgroup poset of G is *not* aligned, so G is not a straight group.

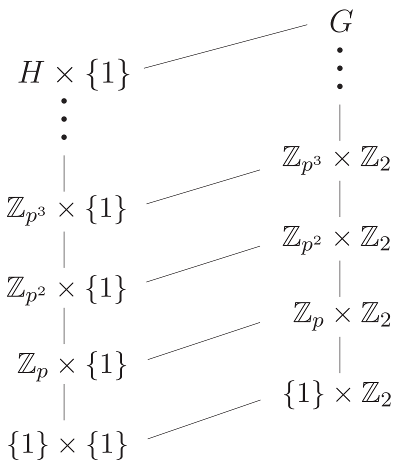

Fig. 4. The subgroup poset of $G := H \times \mathbb{Z}_2$, where $H := \varinjlim_n \mathbb{Z}_{p^n}$.

If a straight group G is *finite*, then its subgroup poset is "finitely" aligned, such as $\{\mathrm{id}\} \subsetneq H_1 \subsetneq H_2 \subsetneq \cdots \subsetneq H_n \subsetneq G$. Then H_n is a largest subgroup of G (or equivalently, a unique maximal subgroup of G). This implies that G is cyclic — in fact the following holds:

Lemma 2.7. *If a (not necessarily finite) group G has a largest subgroup, then G is cyclic.*

Proof. Let L be the largest subgroup of G. Take any element $g \in G \setminus L$ and consider the cyclic subgroup K of G generated by g. Of course $K \not\subset L$. As the largest subgroup L is the unique maximal subgroup of G, this implies that K coincides with G. Hence G is a cyclic group generated by g. □

There is an infinite *straight* group that is not cyclic and has no largest subgroup.

Example 2.8. Let p be a prime and consider the direct limit $G := \varinjlim_n \mathbb{Z}_{p^n}$ of the sequence of inclusions $\mathbb{Z}_p \hookrightarrow \mathbb{Z}_{p^2} \hookrightarrow \cdots \hookrightarrow \mathbb{Z}_{p^n} \hookrightarrow \cdots$. Then G is straight but not cyclic and has no largest subgroup.

In Lemma 2.7, the cyclic group G is actually finite: otherwise G is $\mathbb{Z}$, which has *no* largest subgroup, contradicting the assumption. The following thus holds:

Lemma 2.9. *If a group G has a largest subgroup, then G is a finite cyclic group* (consequently the largest subgroup is a unique maximal subgroup of G).

We can say more:

Corollary 2.10. *If a group G has a largest subgroup, then G is a cyclic group of prime power order, that is, $\mathbb{Z}_{p^n}$ for some prime power p^n.*

Proof. By Lemma 2.9, G is a finite cyclic group, say, generated by $g \in G$. If the order m of g is divisible by (at least) two primes, say p and q, then G contains two maximal subgroups $\mathbb{Z}_{m/p} := \langle g^p \rangle$ and $\mathbb{Z}_{m/q} := \langle g^q \rangle$, which contradicts the uniqueness of a maximal subgroup of G — the unique maximal subgroup is the largest subgroup of G. Hence the order of g is a power p^n of a single prime, that is, $G = \mathbb{Z}_{p^n}$. □

Corollary 2.11. *A finite group G is straight if and only if G is a cyclic group $\mathbb{Z}_{p^n}$ of prime power order.*

Proof. $\Longrightarrow$: A finite straight group has a largest subgroup (or equivalently has only one maximal subgroup), thus the assertion follows from Corollary 2.10. $\Longleftarrow$: See Example 2.3. □

Proposition 2.12. *For a finite group G, the following are equivalent:*

(a) *G is straight.*
(b) *G has only one maximal subgroup* (*or equivalently G has a largest subgroup*).
(c) *G is a cyclic group $\mathbb{Z}_{p^n}$ of prime power order.*

Proof. (a) $\Longrightarrow$ (b): Trivial. (b) $\Longrightarrow$ (c): Corollary 2.10. (c) $\Longleftrightarrow$ (a): Corollary 2.11. □

3. Birdcage groups

The Hasse diagram of a finite group is of special shape — it has the top vertex (corresponding to the finite group itself) and the bottom vertex (corresponding to the identity subgroup), and these two vertices are connected by paths of edges. The Hasse diagram is called *unbranched* (or *birdcage-shaped*) if there is no branch at any "intermediate" vertex between the top and the bottom vertices (while there *may* be branches at the top and the bottom vertices). Otherwise it is called *branched*.

Definition 3.1. A finite group with birdcage-shaped Hasse diagram is called a *birdcage group*.

Let Γ be a birdcage-shaped graph (not necessarily assumed to be the Hasse diagram of a finite group). Let $B_1, B_2, \ldots, B_m$ be the *bars* of Γ, where each bar connects the top and the bottom vertices (see Figure 5). The number l_i of edges of B_i ($i = 1, 2, \ldots, m$) is called the *length* of B_i, and the maximum $h := \max\{l_1, l_2, \ldots, l_m\}$ is called the *height* of Γ.

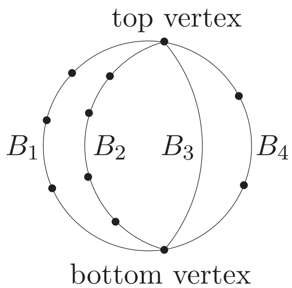

Fig.5. $l_1 = 4$, $l_2 = 5$, $l_3 = 1$, $l_4 = 3$, and $h = 5$.

As seen later, a birdcage-shaped graph is generally *not* the Hasse diagram of a finite group. In fact it must consist of either a single bar (whose length is arbitrary) or more than one bar such that the length of every bar is 2.

The following is a fundamental constraint on birdcage groups:

Lemma 3.2. *If G is a birdcage group, then every "proper" subgroup of G is a straight group* (*so a cyclic group of prime power order by* Proposition 2.12).

Proof. Otherwise, say that H is a proper nonstraight subgroup of G. Then the Hasse diagram of G branches at H. □

Note next the following:

Lemma 3.3. *If a finite group G contains a straight subgroup $\mathbb{Z}_{p^n}$ that is normal in G, then all subgroups $\mathbb{Z}_{p^i}$ ($i = 0, 1, 2, \ldots, n$) of $\mathbb{Z}_{p^n}$ are normal in G.*

Proof. As $\mathbb{Z}_{p^n}$ is normal in G, $g\mathbb{Z}_{p^n}g^{-1} = \mathbb{Z}_{p^n}$ for any $g \in G$. Thus for each i, $g\mathbb{Z}_{p^i}g^{-1}$ is a subgroup of $\mathbb{Z}_{p^n}$. Here any subgroup of $\mathbb{Z}_{p^n}$ is uniquely determined by its order, so $g\mathbb{Z}_{p^i}g^{-1} = \mathbb{Z}_{p^i}$, that is, $\mathbb{Z}_{p^i}$ is normal in G. □

Now consider a semidirect product group $G = \mathbb{Z}_{p^n} \rtimes \mathbb{Z}_{q^m}$ of two cyclic groups of prime power orders. By the definition of semidirect product, (i) G is generated by $\mathbb{Z}_{p^n}$ and $\mathbb{Z}_{q^m}$: $G = \langle \mathbb{Z}_{p^n}, \mathbb{Z}_{q^m} \rangle$, (ii) $\mathbb{Z}_{p^n}$ is normal in G, and (iii) $\mathbb{Z}_{p^n} \cap \mathbb{Z}_{q^m} = \{\mathrm{id}\}$. Note the following:

(a) If $m \geq 2$, then a subgroup $H := \langle \mathbb{Z}_{p^n}, \mathbb{Z}_q \rangle$ of G is not a straight group, in fact a semidirect product $\mathbb{Z}_{p^n} \rtimes \mathbb{Z}_q$, because $\mathbb{Z}_{p^n}$ is normal in H and $\mathbb{Z}_{p^n} \cap \mathbb{Z}_q = \{\mathrm{id}\}$ (as $\mathbb{Z}_{p^n} \cap \mathbb{Z}_{q^m} = \{\mathrm{id}\}$). As G contains a nonstraight group, G is *not* a birdcage group (Lemma 3.2).

(b) If $n \geq 2$, then a subgroup $K := \langle \mathbb{Z}_p, \mathbb{Z}_{q^m} \rangle$ of G is not a straight group, in fact a semidirect product $\mathbb{Z}_p \rtimes \mathbb{Z}_{q^m}$, because $\mathbb{Z}_p$ is normal in G by Lemma 3.3 (so normal in K) and $\mathbb{Z}_p \cap \mathbb{Z}_{q^m} = \{\mathrm{id}\}$ (as $\mathbb{Z}_{p^n} \cap \mathbb{Z}_{q^m} = \{\mathrm{id}\}$). As G contains a nonstraight group, G is *not* a birdcage group (Lemma 3.2).

We thus obtain the following:

Lemma 3.4. *Let $\mathbb{Z}_{p^n} \rtimes \mathbb{Z}_{q^m}$ be a semidirect product group of two cyclic groups of prime power orders. If $n \geq 2$ or $m \geq 2$, then $\mathbb{Z}_{p^n} \rtimes \mathbb{Z}_{q^m}$ is not a birdcage group.*

In the Hasse diagram of a finite group G, an edge connecting a maximal subgroup and G is unique. Similarly an edge connecting a minimal subgroup and $\{\mathrm{id}\}$ is unique. In particular the following holds:

Lemma 3.5. *If H is both a maximal and a minimal subgroup of a finite group G, then the Hasse diagram of G does not branch at H.*

Note that H is both a maximal and a minimal subgroup of G precisely when in the Hasse diagram of G an ascending path of edges connecting $\{\mathrm{id}\}$ and G through H is unique, given by $\{\mathrm{id}\}$ — H — G (length 2). From Lemma 3.5, the following holds:

Proposition 3.6. *In the Hasse diagram of a finite group G, if every ascending path from* $\{\mathrm{id}\}$ *to G is of length* 2*, then G is a birdcage group.*

Note next the following:

Lemma 3.7. *For any semidirect product $\mathbb{Z}_p \rtimes \mathbb{Z}_q$, where p and q are* (*not necessarily distinct*) *primes, every ascending path from* $\{\mathrm{id}\}$ *to $\mathbb{Z}_p \rtimes \mathbb{Z}_q$ in its Hasse diagram is of length* 2.

Proof. Case $p \neq q$: As the order of $\mathbb{Z}_p \rtimes \mathbb{Z}_q$ is pq, the order of any nontrivial proper subgroup of $\mathbb{Z}_p \rtimes \mathbb{Z}_q$ must be either p or q; so the nontrivial proper subgroups of $\mathbb{Z}_p \rtimes \mathbb{Z}_q$ are, up to conjugation, $\mathbb{Z}_p$ and $\mathbb{Z}_q$ (Sylow subgroups). Thus all ascending paths from $\{\mathrm{id}\}$ to $\mathbb{Z}_p \rtimes \mathbb{Z}_q$ in the Hasse diagram of $\mathbb{Z}_p \rtimes \mathbb{Z}_q$ are of length 2: $\{\mathrm{id}\}$ — $\mathbb{Z}_p$ — $\mathbb{Z}_p \rtimes \mathbb{Z}_q$ and $\{\mathrm{id}\}$ — $\mathbb{Z}_q$ — $\mathbb{Z}_p \rtimes \mathbb{Z}_q$.

Case $p = q$: Then $\mathbb{Z}_p \rtimes \mathbb{Z}_p$ is a direct product $\mathbb{Z}_p \times \mathbb{Z}_p$ (Lemma 6.2 (3)). The nontrivial proper subgroups of $\mathbb{Z}_p \times \mathbb{Z}_p$ are $\mathbb{Z}_p$'s. Thus any ascending path from $\{\mathrm{id}\}$ to $\mathbb{Z}_p \times \mathbb{Z}_p$ in the Hasse diagram of $\mathbb{Z}_p \times \mathbb{Z}_p$ is $\{\mathrm{id}\}$ — $\mathbb{Z}_p$ — $\mathbb{Z}_p \times \mathbb{Z}_p$ and of length 2. □

Lemma 3.7 ensures that $\mathbb{Z}_p \rtimes \mathbb{Z}_q$ satisfies the condition of Proposition 3.6, so it is a birdcage group and its Hasse diagram is birdcage-shaped, where each ascending path from $\{\mathrm{id}\}$ to $\mathbb{Z}_p \rtimes \mathbb{Z}_q$ is a bar of length 2. This with Lemma 3.4 yields the following:

Corollary 3.8. *A semidirect product group $\mathbb{Z}_{p^n} \rtimes \mathbb{Z}_{q^m}$ of two cyclic groups of prime power orders is a birdcage group if and only if $n = m = 1$. Here the length of every bar in the Hasse diagram of $\mathbb{Z}_p \rtimes \mathbb{Z}_q$ is* 2; *so the height of the Hasse diagram is* 2.

4. Maximal normal subgroups of birdcage groups

We prepare terminologies. Let G be a finite group.

- G is *Sylow-cyclic* (or a *Z-group*) if any Sylow subgroup of it is cyclic.

- G is *metacyclic* if its commutator group $[G, G]$ and the quotient group $G/[G, G]$ are cyclic ([5] p.247). Note: This is a classical definition. A modern (broader) definition is as follows: G is *metacyclic* if it has a normal subgroup N such that N and G/N are cyclic ([5] p.56).
- G is *solvable* if its derived series terminates in finite steps.

Then: Sylow-cyclic $\overset{\text{(i)}}{\Longrightarrow}$ metacyclic $\overset{\text{(ii)}}{\Longrightarrow}$ solvable, where for (i) see [6] p.356 Theorem 12.6.17 (2) or [3] p.146 Theorem 9.4.3, and for (ii) see Remark 4.2 below. In particular the following holds:

Lemma 4.1. *If a finite group is Sylow-cyclic, then it is solvable.*

Remark 4.2. "Metacyclic $\Longrightarrow$ solvable" is immediate from an alternative definition of solvable (finite) group ([6] p.38): A finite group G is *solvable* if it has a normal series $N_0 = \{\mathrm{id}\} \subsetneq N_1 \subsetneq \cdots \subsetneq N_l = G$ such that the factor groups N_i/N_{i-1} ($i = 1, 2, \ldots, l$) are abelian. Note that if a finite group G is metacyclic, then it has a normal series $N_0 = \{\mathrm{id}\} \subsetneq N_1 = [G, G] \subsetneq N_2 = G$ such that $N_1/N_0 = [G, G]$ and $N_2/N_1 = G/[G, G]$ are cyclic, in particular G is solvable.

For a group G, its commutator subgroup $[G, G]$ is normal in G. Here if G is solvable, then in particular $[G, G] \subsetneq G$, and $[G, G]$ is a proper normal subgroup of G. If moreover G is simple, then the simpleness of G implies that $[G, G] = 1$, that is, G is abelian. Note that an abelian simple finite group is a cyclic group of prime order. Hence: *A simple solvable finite group is a cyclic group of prime order.* If a simple finite group is Sylow-cyclic, then it is solvable (Lemma 4.1), so the following holds:

Lemma 4.3. *If a simple finite group is Sylow-cyclic, then it is a cyclic group of prime order.*

A *maximal normal* subgroup of a finite group is a normal subgroup that is maximal among all proper normal subgroups of the finite group; it is generally *not* a normal maximal subgroup. However for any birdcage group, it *is* (see (2) of Lemma 4.4 below). This fact will play a key role in our later discussion.

Lemma 4.4. *Let G be a birdcage group. Then the following hold:*

(1) *For any maximal normal subgroup N of G, the quotient G/N is a cyclic group of prime order.*
(2) *Any maximal normal subgroup of G is a maximal subgroup of G.*

Proof. (1): If N is a *maximal* normal subgroup of G, then G/N is a *simple* group. We first consider the case that G/N is a p-group. Since a simple p-group is a cyclic group of prime order p (Remark 4.5 below), the assertion holds. We next consider the case that G/N is not a p-group; then Sylow subgroups of G/N are *proper* subgroups of G/N. We show that any proper (in particular Sylow) subgroup of G/N is cyclic. Let $\pi : G \to G/N$ be the quotient homomorphism. If H is a proper subgroup of G/N, then $\pi^{-1}(H)$ is a proper subgroup of G. As G is a birdcage group, $\pi^{-1}(H)$ is a cyclic group (Lemma 3.2), say, generated by g. Then H is generated by $\pi(g)$, so H is cyclic. Hence any proper subgroup of the simple group G/N is cyclic. In particular G/N is Sylow-cyclic. Such a simple group is a cyclic group of prime order (Lemma 4.3).

(2): Let N be a maximal normal subgroup of G. If there exists a subgroup H such that $N \subsetneq H \subsetneq G$, then H/N is a nontrivial proper subgroup of G/N. This cannot occur as G/N is a cyclic group of prime order by (1). Hence N is a maximal subgroup of G. □

REMARK 4.5. *Any simple p-group is a cyclic group of prime order p.* To see this, note that any p-group has a nontrivial center ([5] Theorem 4.28 p.79), which is a nontrivial normal subgroup. In particular if a p-group is simple, then the center coincides with the p-group itself. Thus any simple p-group is abelian, which is necessarily a cyclic group of prime order p.

5. Proof of our main result

We show our main result that a birdcage group is either $\mathbb{Z}_{p^n}$ or $\mathbb{Z}_p \rtimes \mathbb{Z}_q$. Let G be a birdcage group. We separate into two cases depending on whether the number of maximal subgroups of G is one or more.

Case 1. G has only one maximal subgroup M: Then G is a cyclic group $\mathbb{Z}_{p^n}$ of prime power order (Corollary 2.10).

Case 2. G has more than one maximal subgroups: Let $M_1, M_2, \dots, M_l$ $(l \geq 2)$ be the maximal subgroups of G. Note the following properties of them:

(M.1) Any two maximal subgroups M_i and M_j intersect trivially: $M_i \cap M_j = \{\mathrm{id}\}$. Otherwise the Hasse diagram of G is branched at $M_i \cap M_j$ (where two branches towards M_i and M_j come out).

(M.2) (At least) one of $M_1, M_2, \dots, M_l$ is normal in G. In fact any maximal normal subgroup N of G is a maximal subgroup of G (Lemma 4.4 (2)), so N is one of $M_1, M_2, \dots, M_l$.

We now show that G is a semidirect product of cyclic groups of prime orders. First in (M.2), renumbering if necessary, we may assume that $N = M_1$. Set $H := M_k$, where k is any of $2, 3, \dots, l$. Then $G = \langle N, H\rangle$ (because $\langle N, H\rangle$ is strictly larger than the maximal subgroups N and H). Moreover $N \cap H = \{\mathrm{id}\}$ by (M.1) and N is normal in G. Thus $G = N \rtimes H$ (a semidirect product of N and H). Here note that as N and H are proper subgroups of a birdcage group G, they are cyclic groups of prime power orders (Lemma 3.2), say $N = \mathbb{Z}_{p^n}$ and $H = \mathbb{Z}_{q^m}$; then $G = \mathbb{Z}_{p^n} \rtimes \mathbb{Z}_{q^m}$. This is a birdcage group if and only if $n = m = 1$ (Corollary 3.8). This completes the proof of our main result.

REMARK 5.1. As shown above, in terms of the numbers of maximal subgroups in birdcage groups, the following holds: *A birdcage group contains only one maximal subgroup if and only if it is $\mathbb{Z}_{p^n}$, while it contains more than one maximal subgroup if and only if it is a semidirect product group $\mathbb{Z}_p \rtimes \mathbb{Z}_q$.*

The number of bars in the Hasse diagrams of $\mathbb{Z}_p \rtimes \mathbb{Z}_q$. We determine the Hasse diagram of $\mathbb{Z}_p \rtimes \mathbb{Z}_q$. We already know that it is birdcage-shaped with the length of every bar being 2 (Lemma 3.7). It thus suffices to determine the number of its bars. This number is equal to the number of nontrivial proper subgroups of $\mathbb{Z}_p \rtimes \mathbb{Z}_q$, which we shall determine. Consider first the direct product case: $\mathbb{Z}_p \times \mathbb{Z}_q$ $(p \neq q)$ and $\mathbb{Z}_p \times \mathbb{Z}_p$. For $\mathbb{Z}_p \times \mathbb{Z}_q$ $(\cong \mathbb{Z}_{pq})$, the number of nontrivial proper subgroups are two, consisting of $\mathbb{Z}_p$ and $\mathbb{Z}_q$. For $\mathbb{Z}_p \times \mathbb{Z}_p$, as $|\mathbb{Z}_p \times \mathbb{Z}_p| = p^2$ and $\mathbb{Z}_p \times \mathbb{Z}_p$ is noncyclic, the order of any nonidentity element is p, and any nontrivial proper subgroup of $\mathbb{Z}_p \times \mathbb{Z}_p$ is a cyclic group of order p. The number of nonidentity elements of $\mathbb{Z}_p \times \mathbb{Z}_p$ is $p^2 - 1$, while the number of nonidentity elements that generate the same cyclic subgroup of order p is $p - 1$ (the number of generators of a cyclic subgroup of order p). Thus the number of cyclic subgroups of order p in $\mathbb{Z}_p \times \mathbb{Z}_p$ is $\dfrac{p^2-1}{p-1}$, that is, $p + 1$ (which is the number of nontrivial proper subgroups of $\mathbb{Z}_p \times \mathbb{Z}_p$).

We next determine the nontrivial proper subgroups of a *nontrivial* semidirect product $G := \mathbb{Z}_p \rtimes \mathbb{Z}_q$; note that $q < p$ as q divides $p - 1$ (Lemma 6.2 (3)). Since $|G| = pq$, any nontrivial proper subgroup of G is isomorphic to $\mathbb{Z}_p$ or $\mathbb{Z}_q$ (Sylow p- or q-subgroup of G). We determine the numbers n_p and n_q of $\mathbb{Z}_p$ and $\mathbb{Z}_q$ in G. Note that $|G| = n_p(|\mathbb{Z}_p| - 1) + n_q(|\mathbb{Z}_q| - 1) + 1$, i.e. $|G| = n_p(p - 1) + n_q(q - 1) + 1$. On the other hand, by Sylow's theorem, n_p divides the factor q in $|G| = pq$, so n_p is 1 or q. Similarly n_q is 1 or p. The possible combinations of n_p and n_q are thus

$$(n_p, n_q) = (1, 1),\ (1, p),\ (q, 1),\ (q, p). \tag{5.1}$$

Here $(n_p, n_q) = (1, 1)$ does *not* occur: otherwise $|G| = (p - 1) + (q - 1) + 1 = p + q - 1$, where $pq - (p + q - 1) = (p - 1)(q - 1) > 1$ (as p and q are distinct primes), thus $pq > |G|$ (a contradiction). Similarly $(n_p, n_q) = (q, p)$ does *not* occur: otherwise $|G| = q(p - 1) + p(q - 1) + 1 = pq + (pq - p - q + 1)$, where $pq - p - q + 1 = (p - 1)(q - 1) > 1$, thus $|G| > pq$ (a contradiction). Moreover $(n_p, n_q) = (q, 1)$ does *not* occur: in fact by Sylow's theorem $n_p \equiv 1 \bmod p$, so if $n_p = q$, then $q \equiv 1 \bmod p$, which implies $q = 1$ (as $q < p$). This contradicts the assumption that q is a prime. Therefore $(n_p, n_q) = (1, p)$. We summarize the above results (together with the data for $\mathbb{Z}_{p^n}$) as follows — note that the nontrivial proper subgroups of $\mathbb{Z}_p \rtimes \mathbb{Z}_q$ are the maximal subgroups of $\mathbb{Z}_p \rtimes \mathbb{Z}_q$, as the length of any bar of the Hasse diagram of $\mathbb{Z}_p \rtimes \mathbb{Z}_q$ is 2 (Lemma 3.7):

Proposition 5.2. *For birdcage groups, their nontrivial proper subgroups, maximal subgroups, and the numbers of bars of their Hasse diagrams are as follows*:

birdcage group	*nontrivial proper subgroups*	*maximal subgroups*	#(*bars*)
(a) *Cyclic group of prime power order*			
$\mathbb{Z}_{p^n}$	$\mathbb{Z}_p, \mathbb{Z}_{p^2}, \ldots, \mathbb{Z}_{p^{n-1}}$	$\mathbb{Z}_{p^{n-1}}$	1
(b) *Direct product*			
$\mathbb{Z}_p \times \mathbb{Z}_q$ $(p \neq q)$	$\mathbb{Z}_p, \mathbb{Z}_q$	$\mathbb{Z}_p, \mathbb{Z}_q$	2
$\mathbb{Z}_p \times \mathbb{Z}_p$	$(p+1)\mathbb{Z}_p$*'s*	$(p+1)\mathbb{Z}_p$*'s*	$p+1$
(c) *Nontrivial semidirect product*			
$\mathbb{Z}_p \rtimes \mathbb{Z}_q$ $(q < p)$	$\mathbb{Z}_p$, $p\mathbb{Z}_q$*'s*	$\mathbb{Z}_p$, $p\mathbb{Z}_q$*'s*	$p+1$

REMARK 5.3. *In* (c)*, the p $\mathbb{Z}_q$'s are given by the conjugates* $g\mathbb{Z}_q g^{-1}$ $(g \in \mathbb{Z}_p)$. To see this, note that the $\mathbb{Z}_q$'s are Sylow q-subgroups of $\mathbb{Z}_p \rtimes \mathbb{Z}_q$, so they are conjugate by elements of $\mathbb{Z}_p \rtimes \mathbb{Z}_q$. Here an element of $\mathbb{Z}_p \rtimes \mathbb{Z}_q$ is of the form gh $(g \in \mathbb{Z}_p, h \in \mathbb{Z}_q)$. Then $(gh)\mathbb{Z}_q(gh)^{-1} = g(h\mathbb{Z}_q h^{-1})g^{-1} = g\mathbb{Z}_q g^{-1}$, so h is irrelevant. As the number of $\mathbb{Z}_q$'s in $\mathbb{Z}_p \rtimes \mathbb{Z}_q$ is exactly p, the p conjugates $g\mathbb{Z}_q g^{-1}$ $(g \in \mathbb{Z}_p)$ must be distinct and exhaust all $\mathbb{Z}_q$'s in $\mathbb{Z}_p \rtimes \mathbb{Z}_q$.

6. Supplement: Semidirect products of cyclic groups of prime orders

We derive properties of $\mathbb{Z}_p \rtimes \mathbb{Z}_q$. We begin with a general setup. A semidirect product $N \rtimes H$ of groups N and H is a group structure on the direct product *set* $N \times H$ associated with a homomorphism $\varphi : H \to \mathrm{Aut}(N)$: the product of two elements is given by

$$(6.1) \qquad (k,h)(k',h') = (k\varphi_h(k'), hh') \text{ for } (k,h),(k',h') \in N \times H,$$

where by convention φ_h denotes $\varphi(h)$ (an automorphism of N). In emphasizing φ, the semidirect product is denoted by $N \rtimes_\varphi H$. Consider the case that $N = \mathbb{Z}_p$ and $H = \mathbb{Z}_q$, where p and q are primes. Then $\mathbb{Z}_p \rtimes_\varphi \mathbb{Z}_q$ is associated with a homomorphism $\varphi : \mathbb{Z}_q \to \mathrm{Aut}(\mathbb{Z}_p)$. Here $\mathrm{Ker}(\varphi)$ is a subgroup of $\mathbb{Z}_q$, so $\mathrm{Ker}(\varphi)$ is either $\{\mathrm{id}\}$ or $\mathbb{Z}_q$. In the former case, φ is injective. In the latter case, φ is trivial, and $\mathbb{Z}_p \rtimes_\varphi \mathbb{Z}_q$ is the direct product group $\mathbb{Z}_p \times \mathbb{Z}_q$. We closely look at the former case. Note first that $\mathrm{Aut}(\mathbb{Z}_p) \cong \mathbb{Z}_{p-1}$. In fact letting a be a generator of $\mathbb{Z}_p$, then for $\varphi \in \mathrm{Aut}(\mathbb{Z}_p)$, $\varphi(a) = a^k$ for some positive integer k ($1 \le k \le p-1$), and the correspondence $k \in \mathbb{Z}_{p-1} \mapsto \varphi \in \mathrm{Aut}(\mathbb{Z}_p)$ gives an isomorphism $\mathrm{Aut}(\mathbb{Z}_p) \cong \mathbb{Z}_{p-1}$. Now $\varphi : \mathbb{Z}_q \to \mathrm{Aut}(\mathbb{Z}_p) \cong \mathbb{Z}_{p-1}$ is injective, so $\mathbb{Z}_q$ may be regarded as a subgroup of $\mathbb{Z}_{p-1}$. Consequently $q = |\mathbb{Z}_q|$ divides $p-1 = |\mathbb{Z}_{p-1}|$. Conversely if q divides $p-1$, then $\mathbb{Z}_{p-1}$ contains a (unique) cyclic subgroup of order q, say K, and an injective homomorphism from $\mathbb{Z}_q$ into $\mathrm{Aut}(\mathbb{Z}_p) \cong \mathbb{Z}_{p-1}$ is unique up to isomorphism of K.

REMARK 6.1. Write $p-1 = nq$, where n is a positive integer, and identify $\mathbb{Z}_{nq}$ with the cyclic group generated by an nqth root $\alpha := e^{2\pi\mathrm{i}/nq}$ of unity. Then $\alpha^n = e^{2\pi\mathrm{i}/q}$ is an element of order q in $\mathbb{Z}_{nq}$, and the elements of order q in $\mathbb{Z}_{nq}$ are exhausted by $\alpha^{kn} = e^{2\pi\mathrm{i}k/q}$ ($k = 1, 2, \dots, q-1$). Hence a cyclic subgroup of order q in $\mathbb{Z}_{nq}$ is given by $K := \langle \alpha^n \rangle$ and is unique.

Note that the condition "q divides $p-1$" is *not* satisfied if $p = q$, and in this case any semidirect product $\mathbb{Z}_p \rtimes_\varphi \mathbb{Z}_p$ is trivial, that is, $\mathbb{Z}_p \times \mathbb{Z}_p$. We formalize the above results as follows:

Lemma 6.2. *Let p and q be primes. Then the following hold:*

(1) *Any homomorphism* $\varphi : \mathbb{Z}_q \to \mathrm{Aut}(\mathbb{Z}_p) \cong \mathbb{Z}_{p-1}$ *is either trivial or injective*; *thus a semidirect product* $\mathbb{Z}_p \rtimes_\varphi \mathbb{Z}_q$ *is nontrivial precisely when* φ *is injective.*
(2) *A nontrivial* (*equivalently, injective*) *homomorphism* $\mathbb{Z}_q \to \mathrm{Aut}(\mathbb{Z}_p) \cong \mathbb{Z}_{p-1}$ *exists if and only if q divides* $p-1$; *in this case there exists a unique cyclic subgroup of order q in* $\mathrm{Aut}(\mathbb{Z}_p)$.
(3) *A* nontrivial *semidirect product* $\mathbb{Z}_p \rtimes_\varphi \mathbb{Z}_q$ *exists if and only if q divides* $p-1$. *In the case that* $p = q$, *any semidirect product* $\mathbb{Z}_p \rtimes_\varphi \mathbb{Z}_p$ *is trivial, that is,* $\mathbb{Z}_p \times \mathbb{Z}_p$.

In what follows, we assume that q divides $p-1$ so that there exists (at least one) *nontrivial* semidirect product of $\mathbb{Z}_p$ and $\mathbb{Z}_q$. We show that such a semidirect product is unique up to isomorphism. We need the following:

Lemma 6.3. *Let* $\mathbb{Z}_p \rtimes_\varphi \mathbb{Z}_q$ *be a nontrivial semidirect product; so q divides* $p-1$. *Then the nontrivial homomorphism* $\varphi : \mathbb{Z}_q \to \mathrm{Aut}(\mathbb{Z}_p)$ *is injective and its image* $\varphi(\mathbb{Z}_q)$ *is independent of* φ.

Proof. The injectivity of φ is already shown in Lemma 6.2 (1). It remains to show that $\varphi(\mathbb{Z}_q)$ is independent of the choice of an injective homomorphism φ. This follows from the fact that a cyclic subgroup of order q in $\mathrm{Aut}(\mathbb{Z}_p)$ is unique (Lemma 6.2 (2)). $\square$

We will use the following general result:

Proposition 6.4 ([1] p.23 Proposition 11)**.** *Let H be a cyclic group. If two homomorphisms $\varphi, \psi : H \to \mathrm{Aut}(N)$ are injective and $\varphi(H) = \psi(H)$, then two semidirect product groups $N \rtimes_\varphi H$ and $N \rtimes_\psi H$ are isomorphic.*

We return to our context. Let $\mathbb{Z}_p \rtimes_\varphi \mathbb{Z}_q$ and $\mathbb{Z}_p \rtimes_\psi \mathbb{Z}_q$ be *nontrivial* semidirect product groups. By Lemma 6.3, φ and ψ are injective and $\varphi(\mathbb{Z}_p) = \psi(\mathbb{Z}_p)$. Hence by Proposition 6.4, $\mathbb{Z}_p \rtimes_\varphi \mathbb{Z}_q$ and $\mathbb{Z}_p \rtimes_\psi \mathbb{Z}_q$ are isomorphic. Therefore nontrivial semidirect product groups of $\mathbb{Z}_p$ and $\mathbb{Z}_q$ are unique. We formalize these results as follows:

Proposition 6.5. *Let p and q be* (a priori *not necessarily distinct*) *primes. For a* nontrivial *semidirect product group of $\mathbb{Z}_p$ and $\mathbb{Z}_q$ to exist, q must divide $p - 1$* (*so* a posteriori *p and q are distinct*)*. Moreover in this case there exists exactly one* nontrivial *semidirect product group of $\mathbb{Z}_p$ and $\mathbb{Z}_q$ up to isomorphism.*

REMARK 6.6. If $q = 2$, then the condition "q divides $p - 1$" is satisfied precisely when p is an odd prime. If q is an odd prime, then it is subtle: p must be a prime of the form $nq + 1$. For example if $q = 3$, then $p = 7, 13, 19, \ldots$.

ACKNOWLEDGEMENTS. We would like to thank Ryota Hirakawa, Takayuki Okuda, and Kenjiro Sasaki for valuable discussions. This work was supported by Grant-in-Aid for Scientific Research(C) Grant Number JP20K03533.

References

[1] J. Alperin and R. Bell: Groups and Representations, Springer-Verlag, New York, 1995.
[2] K. Brown: *Euler characteristics of groups: the p-fractional part*, Inv. Math. **29** (1975), 1–5.
[3] M. Hall: The Theory of Groups, 2nd ed., American Mathematical Society, Chelsea, 1999.
[4] D. Quillen: *Homotopy properties of the poset of nontrivial p-subgroups of a group*, Adv. in Math. **28** (1978), 101–128.
[5] J. Rose: A Course on Group Theory, Dover, 2012.
[6] W. Scott: Group Theory, Dover, 2010.
[7] S. Smith: Subgroup Complexes, Mathematical Surveys and Monographs **179**, American Mathematical Society, Providence, RI, 2011.

Department of Mathematics, Kyoto University
Kitashirakawa Oiwake-cho, Sakyo-ku
Kyoto 606–8502
Japan
e-mail: takamura@math.kyoto-u.ac.jp