

Advances in Group Theory and Applications
© 2023 AGTA - www.advgrouptheory.com/journal
17 (2023), pp. 99–128 ISSN: 2499-1287
DOI: 10.32037/agta-2023-018

On a Generalization of a Theorem of P. Hall

Tsunenobu Asai — Naoki Chigira — Takashi Niwasaki
Yugen Takegahara

(*Received Nov. 12, 2022; Accepted Aug. 22, 2023 — Comm. by A. Ballester-Bolinches*)

Dedicated to the memory of Masafumi Murai

Abstract

Let A be a finite group, and suppose that for any prime p dividing $|A/A'|$, A' the commutator subgroup of A, the type $\lambda = (\lambda_1, \lambda_2, \dots)$ of a Sylow p-subgroup of A/A' satisfies $\lambda_2 \leqslant 2$ and $\lambda_3 \leqslant 1$. For any finite group G on which A acts, the number of complements of G in the semidirect product AG of G by A is a multiple of $\gcd(|A/A'|, |G|)$. This fact is a generalization of a theorem of P. Hall.

Mathematics Subject Classification (2020): 20D99, 20J99

Keywords: semidirect product; Frobenius theorem

1 Introduction

We are interested in generalizing [11, Theorem 1.6].

Hall's theorem *Let G be any finite group, and let θ be any automorphism of G whose order divides n. Then the number of elements x of G for which the product*

$$x \cdot x^{\theta} \cdot x^{\theta^2} \cdot \ldots \cdot x^{\theta^{n-1}} = 1$$

is a multiple of $\gcd(n, |G|)$, *where* x^θ *indicates the effect of* θ *on* x.

If θ is the identical automorphism of G in Hall's theorem, the assertion is a well-known theorem of Frobenius [8].

Frobenius theorem *For a finite group* G, *the number of elements* x *of* G *which satisfy the equation* $x^n = 1$ *is a multiple of* $\gcd(n, |G|)$.

For a finite group A and for a finite group G on which A acts (cf. [17, Chapter 1, Definition 8.1]), let AG denote the semidirect product of G by A, and let $\mathscr{I}(A, G)$ denote the set of complements of G in AG, that is,

$$\mathscr{I}(A, G) = \{ B \leqslant AG \mid BG = AG \text{ and } B \cap G = \{1\} \},$$

which corresponds to the set of crossed homomorphisms from A to G (see Section 3).

Given a finite group A, we consider the condition

$$\mathrm{I}(A): \qquad \begin{array}{l} |\mathscr{I}(A, G)| \equiv 0 \mod \gcd(|A/A'|, |G|) \\ \text{for any finite group } G \text{ on which } A \text{ acts,} \end{array}$$

where A' denotes the commutator subgroup of A.

Let $\langle a \rangle$ be a cyclic group of order n generated by an element a. Under the hypothesis of Hall's theorem, suppose that $\langle a \rangle$ acts on G by $x^a = x^{\theta^{-1}}$ for all $x \in G$. Then by [4, Lemma 3.1], we have

$$\begin{aligned} |\mathscr{I}(\langle a \rangle, G)| &= |\{ x \in G \mid (ax)^n = 1 \}| \\ &= |\{ x \in G \mid x \cdot x^\theta \cdot x^{\theta^2} \dots x^{\theta^{n-1}} = 1 \}|. \end{aligned}$$

Hence Hall's theorem means that $\mathrm{I}(\langle a \rangle)$ holds.

Let p be a prime. Given a finite abelian p-group C, we consider the condition

$$\mathrm{I}(C)_p: \qquad \begin{array}{l} |\mathscr{I}(C, H)| \equiv 0 \mod \gcd(|C|, |H|) \\ \text{for any finite } p\text{-group } H \text{ on which } C \text{ acts.} \end{array}$$

The next propositions about $\mathrm{I}(A)$ and $\mathrm{I}(C)_p$ are crucial.

Proposition 1.1 *Let* A *be a finite group. If* $\mathrm{I}(C)_p$ *holds whenever* p *divides* $|A/A'|$ *and* C *is isomorphic to a Sylow* p*-subgroup of* A/A', *then* $\mathrm{I}(A)$ *holds.*

Proposition 1.2 *Let* C *be a finite abelian* p*-group, and let* N *be an elementary abelian* p*-group. If* $I(C)_p$ *holds, then* $I(C \times N)_p$ *holds.*

The latter is shown in [3] in terms of the number of crossed homomorphisms. By Hall's theorem and Proposition 1.2, if C is the direct product of a cyclic p-group and an elementary abelian p-group, then $I(C)_p$ holds (cf. [3, Proposition 1.1(iii)]).

The purpose of this paper is to establish the following theorem, which is already known if $p > 2$ (cf. [4, Main Theorem]).

Theorem 1.3 *If* C *is the direct product of a cyclic* p*-group of order greater than or equal to* p^2 *and a cyclic group of order* p^2*, then* $I(C)_p$ *holds.*

In Section 3, we provide preliminary lemmas coming from the facts relative to the number of crossed homomorphisms, and then prove Propositions 1.1 and 1.2 from the viewpoint of the number of complements. The proof of Theorem 1.3 is given in Section 4. The difficulty in proving Theorem 1.3 arises from the exceptional p-groups, namely, the cyclic, dihedral, generalized quaternion, and semidihedral groups. After considering some cases which are left behind, the condition $I(C)_p$ is reduced to the case where C acts on a non-exceptional finite p-group H possessing an exceptional maximal subgroup. The phase of this reduction requires known theorems relative to the exceptional p-groups, namely, [2, Theorem 7.3] (see Theorem 2.3) and [15, Theorem 2.8] (see Theorem 2.2); the latter was proved by Murai on the basis of [14, Theorem A(i)] (see Theorem 2.1). To complete the proof of Theorem 1.3, we provide Theorem 2.8 which is concerned with non-exceptional finite p-groups possessing exceptional maximal subgroups, and apply it to Lemma 4.6. The proof of Theorem 2.8 bears some resemblance to that of [14, Lemma 1.7] (see Appendix).

A sequence $\lambda = (\lambda_1, \lambda_2, \dots)$ of nonnegative integers in weakly decreasing order which contains only finitely many non-zero terms is called the type of a finite abelian p-group P if P is isomorphic to the direct product of cyclic p-groups $\mathbb{Z}/p^{\lambda_1}\mathbb{Z}$, $\mathbb{Z}/p^{\lambda_2}\mathbb{Z}, \dots$. The following theorem, which is a generalization of [3, Proposition 1.1(iii)], follows from Hall's theorem, Proposition 1.2, and Theorem 1.3.

Theorem 1.4 *If* C *is a finite abelian* p*-group of type* $\lambda = (\lambda_1, \lambda_2, \dots)$ *such that* $\lambda_2 \leqslant 2$ *and* $\lambda_3 \leqslant 1$*, then* $I(C)_p$ *holds.*

Combining Theorem 1.4 with Proposition 1.1, we obtain the following generalization of Hall's theorem in the sequel.

Theorem 1.5 *Let A be a finite group. If the type $\lambda = (\lambda_1, \lambda_2, \dots)$ of a Sylow p-subgroup of A/A' satisfies $\lambda_2 \leqslant 2$ and $\lambda_3 \leqslant 1$ for any prime p dividing $|A/A'|$, then $I(A)$ holds.*

For a finite group A, the condition $I(A)$ involves the condition

$$H(A): \qquad |\mathrm{Hom}(A, G)| \equiv 0 \mod \gcd(|A/A'|, |G|) \text{ for any finite group } G,$$

where $|\mathrm{Hom}(A, G)|$ denotes the number of homomorphisms from A to G.

As a generalization of Frobenius theorem, Yoshida [19] proves the following result.

Yoshida's theorem *If A is a finite abelian group, then $H(A)$ holds.*

The following corollary of Theorem 1.5 generalizes of [4, Theorem D] and is also a generalization of [18, Corollary 1.8] which is a result under the additional assumption that $\lambda_3 = 0$ and G is the symmetric group S_n on n letters.

Theorem 1.6 *Let A be a finite group, and suppose that for any prime p dividing $|A/A'|$, the type $\lambda = (\lambda_1, \lambda_2, \dots)$ of a Sylow p-subgroup of A/A' satisfies $\lambda_2 \leqslant 2$ and $\lambda_3 \leqslant 1$. Then $H(A)$ holds.*

Notation Let G be a finite group. We denote by $Z(G)$ the center of G. Let H and K be subgroups of G. We denote by $|G : K|$ the index of K in G, and denote by G/K and $K\backslash G$ the left and right cosets of K in G, respectively. The normalizer and centralizer of K in G are denoted by $N_G(K)$ and $C_G(K)$, respectively. We define

$$N_H(K) := N_G(K) \cap H \quad \text{and} \quad C_H(K) := C_G(K) \cap H.$$

The commutator subgroup of H and K is denoted by $[H, K]$. If $x, y \in G$, we define $x^y := y^{-1}xy$, $[x, y] := x^{-1}y^{-1}xy$, and $C_H(x) := C_H(\langle x \rangle)$. For any elements $x_1, x_2, \dots, x_n$ of G, $\langle x_1, x_2, \dots, x_n \rangle$ denotes the subgroup generated by $x_1, x_2, \dots, x_n$. Given a finite p-group P, we denote by $\Omega_1(P)$ the subgroup of P generated by the elements of order p. For a finite set X, $|X|$ denotes the cardinality $\sharp X$ of X.

2 Finite p-groups with exceptional maximal subgroups

A finite p-group is called *exceptional* if it is one of the following groups: for $p > 2$, a cyclic group; while for $p = 2$, a cyclic, dihedral, generalized quaternion, or semidihedral group (cf. [15]). Thus a non-cyclic exceptional group of order 2^n is isomorphic to the dihedral group D_{2^n}, the generalized quaternion group Q_{2^n}, or the semidihedral group SD_{2^n}, which are defined by

$$\begin{aligned} D_{2^n} &= \langle x, y \mid x^{2^{n-1}} = y^2 = 1,\ y^{-1}xy = x^{-1} \rangle && (n \geqslant 2), \\ Q_{2^n} &= \langle x, y \mid x^{2^{n-2}} = y^2,\ y^{-1}xy = x^{-1} \rangle && (n \geqslant 3), \\ SD_{2^n} &= \langle x, y \mid x^{2^{n-1}} = y^2 = 1,\ y^{-1}xy = x^{-1+2^{n-2}} \rangle && (n \geqslant 4). \end{aligned}$$

A group isomorphic to Q_8 is called a quaternion group.

For a finite group G and for a positive integer m, we denote by $a_m(G)$ the number of elements x of G which satisfy the equation $x^m = 1$.

An important fact about exceptional groups is [14, Theorem A(i)]:

Theorem 2.1 *Let H be a finite group of order p^n, and let e be a positive integer less than n. Then $a_{p^e}(H)$ is not a multiple of p^{e+1} if and only if H is either a cyclic group, or a non-abelian exceptional group and $1 \leqslant e \leqslant n-2$.*

Using Theorem 2.1, Murai developed [4, Theorems 7.1 and 7.2] to [15, Theorem 2.8]:

Theorem 2.2 *Let C be a cyclic group of order p^u, and let H be a finite p-group on which C acts. Suppose that $|H| \geqslant p^{u+1}$ and $|\mathscr{I}(C, H)|$ is not a multiple of p^{u+1}. Then H is exceptional.*

In Section 4, we can make use of Theorem 2.2 and [2, Theorem 7.3]:

Theorem 2.3 *Let C be the direct product of two cyclic p-groups, and let H be an exceptional p-group on which C acts. Then $|\mathscr{I}(C, H)|$ is a multiple of $\gcd(|C|, |H|)$.*

The purpose of this section is to show Theorem 2.8 which is a key result to establish Theorem 1.3. There is a connection between Theorem 2.8 and an essential part (see Lemma A.2) of Theorem 2.1 which asserts a property of non-exceptional finite p-groups possessing exceptional maximal subgroups (we give an alternative proof of Theorem 2.1 in Appendix).

Example 2.4 We define a finite group H_{16} of order 16 by the relations

$$a^2 = b^2 = c^2 = (ab)^4 = 1, \quad cac = bab, \quad \text{and} \quad cbc = aba$$

with generators a, b, and c, which appears in the statement of Theorem 2.8. Observe that $\langle a, b \rangle \simeq D_8$ (cf. [17, Chapter 2, Theorem 6.8]) and $H_{16} = \langle a, b \rangle \rtimes \langle c \rangle$, the internal semidirect product of $\langle a, b \rangle$ by $\langle c \rangle$ (cf. [17, Chapter 1, Definition 8.6]). Moreover, $cab = abc = bca$, $(ca)^2 = (ab)^2 = (bc)^2 = (abc)^2$, and

$$H_{16} = \{\, 1, a, b, c, ab, ba, bc, cb, ca, ac, \\ bab, cbc, aca, abc, bac, (abc)^2 \,\}.$$

Thus $a_2(H_{16}) = 8$ and $a_4(H_{16}) = 16$. Moreover,

$$\mathscr{I}(\langle c \rangle, \langle a, b \rangle) = \{\langle c \rangle, \langle aca \rangle\}.$$

We have $[H_{16}, H_{16}] = \langle (ab)^2 \rangle$ and $Z(H_{16}) = \langle abc \rangle$. The maximal subgroups of H_{16} are as follows:

abelian	dihedral	quaternion
$\langle ca, b \rangle$, $\langle ab, c \rangle$, $\langle bc, a \rangle$	$\langle c, a \rangle$, $\langle a, b \rangle$, $\langle b, c \rangle$	$\langle ca, ab \rangle$

We define a finite group $M(p^n)$ of order p^n to be

$$M(p^n) = \langle x, y \mid x^{p^{n-1}} = y^p = 1,\ y^{-1}xy = x^{1+p^{n-2}} \rangle,$$

where $n \geqslant 4$ if $p = 2$, and $n \geqslant 3$ otherwise. Obviously,

$$[M(p^n), M(p^n)] = \langle x^{p^{n-2}} \rangle \quad \text{and} \quad Z(M(p^n)) = \langle x^p \rangle.$$

The following well-known theorem is necessary for the argument in this paper (see, e.g., [9, Chapter 5, Theorem 4.4] or [17, Chapter 4, Theorem 4.1]).

Theorem 2.5 *Let P be a non-cyclic finite group of order p^n, and assume that $P \not\simeq M(p^n)$. If P possesses a cyclic maximal subgroup, then P is isomorphic to a non-cyclic exceptional p-group or the direct product of a cyclic group of order p^{n-1} and a cyclic group of order p.*

Let $P = D_{2^n}$ ($n \geqslant 3$), Q_{2^n}, or SD_{2^n}. Then $[P, P]$ coincides with the Frattini subgroup of P and is cyclic. The center $Z(P)$ is generated by $x^{2^{n-2}}$ and is of order 2 (see, e.g., [9, Chapter 5, Theorem 4.3] or [17, Chapter 4, (4.2)]).

Lemma 2.6 *Let i be a nonnegative integer less than 2^{n-1}.*

1) *In D_{2^n}, $(x^i y)^2 = 1$.*

2) *In Q_{2^n}, $x^{2^{n-1}} = y^4 = 1$, $y^{-1} = x^{2^{n-2}} y$, and $(x^i y)^2 = x^{2^{n-2}}$.*

3) *In SD_{2^n}, $(x^i y)^2 = 1$ if i is even, and $(x^i y)^2 = x^{2^{n-2}}$ otherwise.*

Proof — The proof is straightforward. □

The following lemma is well-known and is shown in [7].

Lemma 2.7 *Let i be a nonnegative integer less than p^{n-1}, and let m be a positive integer. In $M(p^n)$, $(x^i y)^{p^m} = 1$ if and only if $x^{ip^m} = 1$.*

Proof — For any nonnegative integer j, we have $y^{x^j} = yz^j$ with $z = [y, x]$, whence

$$(x^i y)^j = x^{ij} y^{x^{i(j-1)}} y^{x^{i(j-2)}} \dots y^{x^i} y = x^{ij} y^j z^{ij(j-1)/2}$$

(see, e.g., [9, Chapter 2, Lemma 2.2] or [17, Chapter 4, (3.7)]). If $p > 2$, then the assertion is an immediate consequence of this fact. Suppose that $p = 2$ and $n \geqslant 4$. Then $(x^i y)^{2^m} = 1$ if and only if

$$x^{2^m i} = x^{2^{n+m-3}(2^m - 1)i}.$$

Hence the assertion holds in the case where $m \geqslant 2$ or i is even. Assume now that $m = 1$ and i is odd. Then, since $n \geqslant 4$, we have $x^{2i} \neq 1$ and $(x^i y)^2 = x^{(2+2^{n-2})i} \neq 1$, completing the proof. □

We now prove a key result to establish Theorem 1.3.

Theorem 2.8 *Let H be a non-exceptional group of order p^n with $n \geqslant 4$, and suppose that H possesses an exceptional maximal subgroup. If $H \not\simeq H_{16}$, then there exists an element y of H of order p which satisfies the following conditions:*

(Y1) *The group $\Omega_1(Z(H))\langle y \rangle$ is a characteristic subgroup of H, and is an elementary abelian group of order p^2;*

(Y2) *No exceptional maximal subgroup of* H *contains* y.

The classification of finite p-groups with cyclic subgroups of index p^2 is known (cf. [12, 13, 16]); it does not immediately bring Theorem 2.8, however. We provide the following lemmas to make an exception of H_{16}, and then prove Theorem 2.8 without using the classification.

Lemma 2.9 *Let* H *be a non-exceptional group of order* 16*, and suppose that* H *possesses a subgroup* Q *which is isomorphic to* Q_8*. Then* $H \simeq H_{16}$ *or* $H = Q \times \langle y \rangle$ *for some involution* y*.*

Proof — Since H is neither cyclic nor generalized quaternion, there is an involution, say y, of H that is not contained in Q (cf. [17, Chapter 4, (4.4)]). Hence $H = Q \rtimes \langle y \rangle$. There are exactly two conjugacy classes of involutions in the group $\operatorname{Aut} Q$ of automorphisms of Q, because $\operatorname{Aut} Q$ is isomorphic to the symmetric group S_4 on 4 letters. Since $H \not\simeq SD_{16}$ by the hypothesis, we conclude that $H \simeq H_{16}$ or $H = Q \times \langle y \rangle$, completing the proof. □

Lemma 2.10 *Let* H *be a non-exceptional group of order* 2^{n+1} *with* $n \geqslant 3$*, and suppose that* H *possesses a non-cyclic exceptional maximal subgroup* P*. Let* T *be a cyclic maximal subgroup of* P*, and suppose that* $C_H(T) = T \times \langle c \rangle$*, where* c *is an involution of* H*. If* $H \not\simeq H_{16}$ *and if* $P \not\simeq Q_8$*, then* $C_H(T)$ *possesses all the cyclic subgroups of* H *of order* 2^{n-1}*.*

Proof — Since P is not abelian, it follows that $c \notin P$. Thus we have $H = \langle c \rangle P$. Suppose that $P \not\simeq Q_8$. Then T is a unique cyclic maximal subgroup of P (cf. [17, Chapter 4, (4.2)]). Let R be a cyclic subgroup of H of order 2^{n-1}, and assume that $R \not\leqslant C_H(T)$. Then $R \not\leqslant P$, so $R = \langle ca \rangle$ for some $a \in P$, which yields $ca \notin C_H(T)$. We also have $a \notin T$, because $c \in C_H(T)$. Moreover, $a^2 \in \Omega_1(T)$ and $a^4 = 1$ by Lemma 2.6. Suppose that x is a generator of T. Then a and x generate the normal subgroup P of H, so $cac = x^i a$ with $0 \leqslant i < 2^{n-1}$. Observe now that

$$(ca)^4 = (x^i a^2)^2 = x^{2i} \quad \text{and} \quad a = cx^i ac = x^i cac = x^{2i} a.$$

Thus $(ca)^4 = x^{2i} = 1$. Since ca is of order 2^{n-1} with $n \geqslant 3$, it follows that $n = 3$ and $P = D_8$. Hence $a^2 = 1$, $i = 2$, and $axa = x^3$. Set $b = xa$. Then $a^2 = b^2 = c^2 = (ab)^4 = 1$, $cac = x^2 a = bab$, and $cbc = cxac = xcac = x^3 a = ax = aba$, which force H_{16} to be isomorphic to H. Consequently, if $H \not\simeq H_{16}$ and if $P \not\simeq Q_8$, then $C_H(T)$

possesses all the cyclic subgroups of H of order 2^{n-1}. This completes the proof. □

Proof of Theorem 2.8 — We first assume that H possesses a cyclic maximal subgroup P. If $H = M(p^n)$, then, since

$$\Omega_1(H) = \langle x^{p^{n-2}} \rangle \times \langle y \rangle = \Omega_1(Z(H))\langle y \rangle$$

and the Frattini subgroup of H is $\langle x^p \rangle$ (cf. [17, Chapter 4, (4.2)]), the assertion follows from Lemma 2.7. Assume that $H \ncong M(p^n)$. Then by Theorem 2.5, $H = P \times \langle y \rangle$ for some element y of H of order p. Hence the assertion holds.

By the above paragraph, we may assume that $p = 2$ and H possesses no cyclic maximal subgroup. Let P be a non-cyclic exceptional maximal subgroup of H. Let T be a cyclic subgroup of P of order 2^{n-2}, and let x be a generator of T. Then $Z(P) = \Omega_1(T) = \langle x^{2^{n-3}} \rangle$, which is of order 2. We have $|C_H(T) : T| \leqslant 2$, because P is not abelian. Thus $C_H(T) = T$ or $|C_H(T) : T| = 2$. We find an involution y of H satisfying (Y1) and (Y2) in either case.

Case 1 Assume that $C_H(T) = T$. Then $\Omega_1(Z(H)) = \Omega_1(T)$. By Lemma 2.9, P is not quaternion. Hence T is a unique cyclic maximal subgroup of P and is a normal subgroup of H. By the assumption, H/T is isomorphic to a subgroup of $\operatorname{Aut} T$ of order 4. This, in combination with [9, Chapter 5, Lemma 4.1], yields $n > 4$. If H/T is cyclic, then there exists an element z of H such that $z^{-2}xz^2 = x^{1+2^{n-3}}$ and $P = T\langle z^2 \rangle$, contradicting the assumption that P is exceptional. Thus, H/T is isomorphic to the four group. Moreover, by [9, Chapter 5, Lemma 4.1], there exist some elements h and y of H satisfying

$$h^{-1}xh = x^{-1+2^{n-3}} \qquad \text{and} \qquad y^{-1}xy = x^{1+2^{n-3}}.$$

Since $T\langle y \rangle \simeq M(2^{n-1})$ by Theorem 2.5, we may assume that y is an involution. Obviously, $H = \langle x, h, y \rangle$. If $[h, y] = x^i$, then $h^{-1}yh = x^iy$, which implies that $(x^iy)^2 = 1$. Combining this fact with Lemma 2.7, we have $[h, y] \in \langle x^{2^{n-3}} \rangle$. Thus $[H, H] = \langle x^2 \rangle$. In addition, we have

$$T\langle y \rangle = C_H(\langle x^2 \rangle).$$

Therefore, $T\langle y \rangle$ is a characteristic subgroup of H, and so is $\Omega_1(T\langle y \rangle)$

(cf. [9, Chapter 5, Lemma 4.8]). By Lemma 2.7,

$$\Omega_1(T\langle y\rangle) = \Omega_1(T)\langle y\rangle = \Omega_1(Z(H))\langle y\rangle.$$

Hence y satisfies (Y1). We have $H = P\langle y\rangle$, because $T\langle y\rangle$ is not exceptional. If $s \in H$, then

$$s^{-1}ysy \in \Omega_1(Z(H))\langle y\rangle \cap \langle x^2\rangle = \langle x^{2^{n-3}}\rangle = \Omega_1(Z(H)).$$

Combining this fact with Lemma 2.6, we have

$$(sy)^4 = (s^2(s^{-1}ysy))^2 = s^4 = 1$$

for any $s \in P - T$. Thus every exceptional maximal subgroup of H possesses a cyclic subgroup of $T\langle y\rangle$ of order 2^{n-2}, which implies that y satisfies (Y2).

Case 2 Assume that $|C_H(T) : T| = 2$. Then $C_H(T)$ is an abelian maximal subgroup of H. By the assumption, $C_H(T)$ is not cyclic. Hence there exists an involution, say y, of H such that $C_H(T) = T \times \langle y\rangle$. If $H \ncong H_{16}$ and if $P \simeq Q_8$, then the assertion of the theorem follows from Lemma 2.9. Assume that $H \ncong H_{16}$ and $P \ncong Q_8$. By Lemma 2.10, T and $\langle xy\rangle$ are the cyclic subgroups of H of order 2^{n-2}. In particular, $C_H(T)$ is generated by the elements of H of order 2^{n-2}. Thus $C_H(T)$ is a characteristic subgroup of H, and so is $\Omega_1(C_H(T))$. Moreover, we have

$$\Omega_1(C_H(T)) = \Omega_1(T \times \langle y\rangle) = \Omega_1(Z(H))\langle y\rangle,$$

because $Z(H) \leqslant C_H(T)$. Hence y satisfies (Y1). By the preceding argument, every exceptional maximal subgroup of H possesses a cyclic subgroup of $T \times \langle y\rangle$ of order 2^{n-2}, which implies that y satisfies (Y2). This completes the proof. □

3 Preliminary lemmas and proofs of Propositions 1.1 and 1.2

Let A be a finite group, and let G be a finite group on which A acts. Given $g \in G$ and $a \in A$, we denote by g^a the effect of a on g. The

semidirect product AG of G by A is defined to be the group consisting of all ordered pairs $ag := (a, g)$ for $a \in A$ and $g \in G$ with multiplication given by $(ag)(bh) = abg^b h$ for all $a, b \in A$ and $g, h \in G$. Obviously, A and G are embedded in AG.

A map φ from A to G is called a crossed homomorphism if

$$\varphi(a_1 a_2) = \varphi(a_1)^{a_2} \varphi(a_2)$$

for all $a_1, a_2 \in A$. Let $Z^1(A, G)$ denote the set of crossed homomorphisms from A to G, and view $Z^1(A, G)$ as a right G-set with the action given by

$$\varphi^g(a) = (g^a)^{-1} \varphi(a) g$$

for all $\varphi \in Z^1(A, G)$, $g \in G$, and $a \in A$ (cf. [17, Chapter 2, §8, Exercise 3]). For each $\varphi \in Z^1(A, G)$, we define a complement $\widetilde{A}_\varphi$ of G in AG to be

$$\widetilde{A}_\varphi = \{ a\varphi(a) \mid a \in A \}.$$

Obviously, there exists a one to one correspondence

$$f : Z^1(A, G) \to \mathscr{I}(A, G), \quad \varphi \mapsto \widetilde{A}_\varphi,$$

so that $|Z^1(A, G)| = |\mathscr{I}(A, G)|$. If $\varphi \in Z^1(A, G)$ and $g \in G$, then

$$f(\varphi)^g = \{ (a\varphi(a))^g \mid a \in A \} = \{ a\varphi^g(a) \mid a \in A \} = f(\varphi^g).$$

Let H be a subgroup of G. Given $\varphi \in Z^1(A, G)$, we set

$$\mathscr{X}_H(\varphi) = \{ \psi \in Z^1(A, G) \mid \psi(a)H = \varphi(a)H \text{ for all } a \in A \}$$

and

$$\widetilde{H}_\varphi = \{ h \in H \mid \varphi^h \in \mathscr{X}_H(\varphi) \}.$$

By [1, Lemma 2.1], there are crossed homomorphisms, say $\varphi_1, \varphi_2, \ldots$, such that

$$Z^1(A, G) = \coprod_{i \geqslant 1} \coprod_{\widetilde{H}_{\varphi_i} h \in \widetilde{H}_{\varphi_i} \backslash H} \mathscr{X}_H({\varphi_i}^h) \qquad \text{(disjoint union)}. \tag{3.1}$$

We quote part of [1, Lemma 2.2] which was inspired by [6, §3 and §4].

Lemma 3.1 *Let A be a finite group, and let G be a finite group on which A*

acts. Let H *be a subgroup of* G*, and suppose that* $\varphi \in Z^1(A, G)$*. Then*

$$\widetilde{H}_\varphi = \bigcap_{a \in A} \{ a\varphi(a)h\varphi(a)^{-1}a^{-1} \mid h \in H \}$$

and

$$\sum_{\widetilde{H}_\varphi h \in \widetilde{H}_\varphi \backslash H} |\mathscr{X}_H(\varphi^h)| = |H : \widetilde{H}_\varphi| \cdot |Z^1(\widetilde{A}_\varphi, \widetilde{H}_\varphi)|,$$

where $\widetilde{A}_\varphi$ *acts on* $\widetilde{H}_\varphi$ *by conjugation.*

The following lemma, which is crucial to the proof of Proposition 1.1, is a consequence of Eq. (3.1) and Lemma 3.1 relative to the number of complements.

Lemma 3.2 *Under the notation of* Lemma 3.1*, assume also that* $|\mathscr{I}(D, F)|$ *is a multiple of* $|F|$ *for any* $D \in \mathscr{I}(A, G)$ *and for any* D*-invariant subgroup* F *of* H*. Then* $|\mathscr{I}(A, G)|$ *is a multiple of* $|H|$*.*

Proof — Recall that $|Z^1(A, G)| = |\mathscr{I}(A, G)|$. Given $\varphi \in Z^1(A, G)$, by assumption, $|Z^1(\widetilde{A}_\varphi, \widetilde{H}_\varphi)|(= |\mathscr{I}(\widetilde{A}_\varphi, \widetilde{H}_\varphi)|)$ is a multiple of $|\widetilde{H}_\varphi|$. Hence it follows from Eq. (3.1) and Lemma 3.1 that $|Z^1(A, G)|$ is a multiple of $|H|$. This completes the proof. □

Definition 3.3 Let C be a finite group and N a normal subgroup. Let H be a finite group on which C acts. Set $G = CH$ and $M = NH$. For each $K \in \mathscr{I}(N, H)$ and for each subgroup W of $H \cap Z(G)$, we define

$$\mathscr{D}_{G,W}(M, KW) := \{ D \in \mathscr{I}(C, H) \mid (D \cap M)W = KW \}.$$

Set $\mathscr{D}_G(M, K) = \mathscr{D}_{G,\{1\}}(M, K)$ for brevity's sake.

The next lemmas are fundamental to enumerating the number of complements.

Lemma 3.4 *Under the notation of* Definition 3.3*, suppose* $K \in \mathscr{I}(N, H)$ *and* $D \in \mathscr{D}_G(M, K)$*. Then* K *is a normal subgroup of* D*, and*

$$|\mathscr{D}_G(M, K)| = |\mathscr{I}(D/K, C_H(K))|,$$

where the action of D/K *on* $C_H(K)$ *is given by*

$$h^{xK} = x^{-1}hx$$

for all $x \in D$ *and* $h \in C_H(K)$. *Moreover,*

$$\sum_{N_G(K)g \in N_G(K)\backslash G} |\mathscr{D}_G(M, K^g)| = |H/C_H(K)| \cdot |\mathscr{I}(D/K, C_H(K))|,$$

where $K^g = \{x^g \mid x \in K\}$.

Proof — The first assertion is equivalent to [1, Lemma 4.1]. We prove the second one. Since

$$|\mathscr{D}_G(M, K^g)| = |\mathscr{D}_G(M, K)| = |\mathscr{I}(D/K, C_H(K))|$$

for any $g \in G$, it follows that

$$\sum_{N_G(K)g \in N_G(K)\backslash G} |\mathscr{D}_G(M, K^g)| = |G/N_G(K)| \cdot |\mathscr{I}(D/K, C_H(K))|.$$

Moreover, $|G/N_G(K)| = |DH/DC_H(K)| = |H/C_H(K)|$. This completes the proof. □

Lemma 3.5 *Let* C *be a finite group and* N *a normal subgroup. Assume that for any finite group* H *on which* C/N *acts,* $|\mathscr{I}(C/N, H)|$ *is a multiple of* $\gcd(|C/N|, |H|)$. *If* C *acts on a finite group* H, *then* $|\mathscr{I}(C, H)|$ *is a multiple of* $\gcd(|C/N|, |H|)$.

Proof — Let H be a finite group on which C acts. Then $\mathscr{I}(C, H)$ is a disjoint union of the sets $\mathscr{D}_G(M, K)$ for all $K \in \mathscr{I}(N, H)$, and G acts on $\mathscr{I}(N, H)$ by conjugation. Also, if $K \in \mathscr{I}(N, H)$ and if $D \in \mathscr{D}_G(M, K)$, then D/K is isomorphic to C/N, and hence $|\mathscr{I}(D/K, C_H(K))|$ is a multiple of $\gcd(|D/K|, |C_H(K)|)$. The assertion now follows from Lemma 3.4. This completes the proof. □

By virtue of the preceding lemmas, we are successful in proving Proposition 1.1.

Proof of Proposition 1.1 — Let p be a prime dividing $|A/A'|$, and let B be a normal subgroup of A such that A/B is isomorphic to a Sylow p-subgroup of A/A'. Assume that $I(A/B)_p$ holds. Let H be a finite group on which A/B acts. Using Sylow's theorem, we choose a subgroup K of H of order $\gcd(|A/B|, |H|)$. Suppose now that $D \in \mathscr{I}(A/B, H)$. If F is a D-invariant subgroup of K, then by the

assumption, $|\mathscr{I}(D,F)|$ is a multiple of $|F|$. This, combined with Lemma 3.2, shows that $|\mathscr{I}(A/B,H)|$ is a multiple of $|K|$. By the assumption, $|K| = \gcd(|A/B|, |H|)$. Hence it follows from Lemma 3.5 that for any finite group G on which A acts, $|\mathscr{I}(A,G)|$ is a multiple of $\gcd(|A/B|, |G|)$. Consequently, if $I(C)_p$ holds in the case where p divides $|A/A'|$ and C is isomorphic to a Sylow p-subgroup of A/A', then $I(A)$ holds. This completes the proof. □

The following lemmas are useful for enumerating the number of complements.

Lemma 3.6 *Keep the notation of* Definition 3.3, *and assume further that*

$$C = \langle x_1 \rangle \times \langle x_2 \rangle \times \ldots \times \langle x_{\ell-1} \rangle \times N \quad \textit{and} \quad N = \langle x_\ell \rangle$$

with $x_1, x_2, \ldots, x_{\ell-1} \in C$ *and* $x_\ell \in N$. *Let*

$$K \in \mathscr{I}(N,H) \quad \textit{and} \quad D \in \mathscr{D}_G(M,K).$$

Then there exists a unique sequence $(h_1, h_2, \ldots, h_\ell)$ *of elements of* H *such that*

$$D = \langle x_1 h_1 \rangle \times \langle x_2 h_2 \rangle \times \ldots \times \langle x_{\ell-1} h_{\ell-1} \rangle \times \langle x_\ell h_\ell \rangle$$

and $|\langle x_k h_k \rangle| = |\langle x_k \rangle|$ *for all integer* k *with* $1 \leqslant k \leqslant \ell$. *In particular,* $K = \langle x_\ell h_\ell \rangle$.

Proof — The lemma is a consequence of [4, Lemma 3.1]. □

Lemma 3.7 *Let* C *be a finite abelian* p*-group, and* N *a cyclic* p*-group. Let* H *be a finite* p*-group on which* $C \times N$ *acts, and let* $K \in \mathscr{I}(N,H)$. *Set* $G = (C \times N)H$ *and* $M = NH$, *and let* $W \leqslant H \cap Z(G)$. *If* $w^{|N|} = 1$ *for any* $w \in W$, *then*

$$|\mathscr{D}_{G,W}(M, KW)| = |W| \cdot |\mathscr{D}_G(M,K)|.$$

Proof — Let x be a generator of K. Then we have

$$\mathscr{D}_{G,W}(M, KW) = \bigcup_{w \in W} \mathscr{D}_G(M, \langle xw \rangle),$$

and $\langle xw_1 \rangle = \langle xw_2 \rangle$ with $w_1, w_2 \in W$ if and only if $w_1 = w_2 \in W$. Moreover, it follows from Lemma 3.6 that for any $w \in W$, there exists a one-to-one correspondence between $\mathscr{D}_G(M,K)$ and $\mathscr{D}_G(M, \langle xw \rangle)$. This completes the proof. □

We are now in a position to prove Proposition 1.2.

Proof of Proposition 1.2 — We may assume that N is a cyclic group of order p. Let H be a finite p-group on which $C \times N$ acts. Set $M = NH$ and $G = (C \times N)H$. Assume that $I(C)_p$ holds. Let $\mathscr{D}_1$ be the set of all $D \in \mathscr{I}(C \times N, H)$ with $H \neq C_H(D \cap M)$, and let $\mathscr{D}_2$ be the set of all $D \in \mathscr{I}(C \times N, H)$ with $H = C_H(D \cap M)$. Then $\mathscr{I}(C \times N, H)$ is a disjoint union of $\mathscr{D}_1$ and $\mathscr{D}_2$. Since G acts on $\mathscr{D}_1$ by conjugation, it follows from Lemma 3.4 that

$$|\mathscr{D}_1| \equiv 0 \mod \gcd(p\,|C|, |H|).$$

Let z be an element of $H \cap Z(G)$ of order p. Then $\mathscr{D}_2$ is a disjoint union of the sets $\mathscr{D}_{G,\langle z\rangle}(M, K\langle z\rangle)$ for all $K \in \mathscr{I}(N, H)$ with $H = C_H(K)$. By Lemmas 3.4 and 3.7,

$$|\mathscr{D}_{G,\langle z\rangle}(M, K\langle z\rangle)| \equiv 0 \mod p\gcd(|C|, |H|)$$

for all $K \in \mathscr{I}(N, H)$ with $H = C_H(K)$, and thus

$$|\mathscr{D}_2| \equiv 0 \mod p\gcd(|C|, |H|).$$

Hence $|\mathscr{I}(C \times N, H)|$ is a multiple of $\gcd(|C \times N|, |H|)$. This completes the proof. □

4 The proof of Theorem 1.3

This section is devoted to the proof of Theorem 1.3. We walk along the line of the proof of [4, Main Theorem]. The following proposition, which is shown in the proof of [5, Proposition 3.3], plays an important role in the proof of Theorem 1.3.

Proposition 4.1 *Let C be a cyclic p-group. Then $I(C)_p$ holds. In particular, if H is a finite p-group on which C acts and if $|H|$ divides $|C|$, then $|\mathscr{I}(C, H)| = |H|$.*

Let C be the direct product of a cyclic group of order p^u with $u \geqslant 2$ and a cyclic group N of order p^2. Let H be a finite p-group on which C acts. Set $G = CH$, $M = NH$, and $Z = H \cap Z(G)$. We aim to show that

$$|\mathscr{I}(C, H)| \equiv 0 \mod \gcd(p^{u+2}, |H|). \tag{4.1}$$

Let W be the subgroup of Z generated by the elements of order at most p^2, and $\mathscr{K}_W$ the set of subgroups KW of G with $K \in \mathscr{I}(N, H)$ such that $\mathscr{D}_{G,W}(M, KW) \neq \emptyset$. Obviously, $D \cap M \in \mathscr{I}(N, H)$ for any D in $\mathscr{I}(C, H)$. Also, $\mathscr{I}(C, H)$ is a disjoint union of the sets $\mathscr{D}_{G,W}(M, KW)$ for every $K \in \mathscr{I}(N, H)$ with $KW \in \mathscr{K}_W$. Let $\mathscr{K}(p^u)$ be the set of all $K \in \mathscr{I}(N, H)$ with $|C_H(K)| \leqslant p^u$, and let $\mathscr{K}_W(p^u)$ be the set of subgroups $KW \in \mathscr{K}_W$ with $K \in \mathscr{K}(p^u)$. Then we have

$$\coprod_{KW \in \mathscr{K}_W(p^u)} \mathscr{D}_{G,W}(M, KW) = \coprod_{K \in \mathscr{K}(p^u)} \mathscr{D}_G(M, K). \tag{4.2}$$

Lemma 4.2

$$\sum_{KW \in \mathscr{K}_W(p^u)} |\mathscr{D}_{G,W}(M, KW)| \equiv 0 \mod |H|.$$

Proof — By Lemma 3.4 and Proposition 4.1, we have

$$\sum_{N_G(K)g \in N_G(K)\backslash G} |\mathscr{D}_G(M, K^g)| \equiv 0 \mod |H|$$

for any $K \in \mathscr{K}(p^u)$. Observe that G acts on $\mathscr{K}(p^u)$ by conjugation. Hence the assertion is a consequence of Eq. (4.2). This completes the proof. □

Since $\exp W \leqslant p^2$, it follows from Lemmas 3.4 and 3.7 and Proposition 4.1 that

$$|\mathscr{D}_{G,W}(M, KW)| = |W| \cdot |\mathscr{D}_G(M, K)| \equiv 0 \bmod |W|\, p^u \tag{4.3}$$

for any $K \in \mathscr{I}(N, H)$ with $KW \notin \mathscr{K}_W(p^u)$.

Lemma 4.3 *If* $|W| \geqslant p^2$, *then* Eq. (4.1) *holds.*

Proof — The assertion is an immediate consequence of Lemma 4.2 and Eq. (4.3). □

From now on we assume that Z is a cyclic group of order p. Obviously, $W = Z$. We denote by $\mathscr{L}$ the set of subgroups KZ of G with $K \in \mathscr{I}(N, H)$ such that

i) $KZ \geqslant [H, KZ]$, or equivalently, $Z \geqslant [H, K]$,

ii) $C_H(KZ)$ is an exceptional p-group of order greater than p^u, and

iii) $\mathscr{D}_{G,Z}(M, KZ) \neq \emptyset$.

Let $\mathscr{E}(H)$ be the set of exceptional subgroups of H. We set

$$\mathscr{L}_0 = \mathscr{K}_Z - \mathscr{K}_Z(p^u),$$

$$\mathscr{L}_1 = \{\, KZ \in \mathscr{L}_0 \mid K \in \mathscr{I}(N, H) \text{ and } C_H(KZ) \notin \mathscr{E}(H) \,\},$$

and

$$\mathscr{L}_2 = \{\, KZ \in \mathscr{L}_0 \mid K \in \mathscr{I}(N, H),\ C_H(KZ) \in \mathscr{E}(H),\ \text{and } KZ \not\geqslant [H, KZ] \,\}.$$

Observe that $\mathscr{K}_Z = \mathscr{K}_Z(p^u) \amalg \mathscr{L}_1 \amalg \mathscr{L}_2 \amalg \mathscr{L}$. We have the following.

Lemma 4.4 *For any $K \in \mathscr{I}(N, H)$ with $KZ \in \mathscr{L}_1$,*

$$|\mathscr{D}_{G,Z}(M, KZ)| \equiv 0 \mod p^{u+2}.$$

Moreover,

$$\sum_{KZ \in \mathscr{L}_2} |\mathscr{D}_{G,Z}(M, KZ)| \equiv 0 \mod p^{u+2}.$$

Proof — Let $K \in \mathscr{I}(N, H)$, and suppose that $KZ \notin \mathscr{K}_Z(p^u)$. Assume that $C_H(KZ)$ is not exceptional. Since $C_H(K) = C_H(KZ)$, we have

$$|\mathscr{D}_G(M, K)| \equiv 0 \mod p^{u+1}$$

by Theorem 2.2 and Lemma 3.4. Therefore the first assertion follows from Lemma 3.7. Assume next that $C_H(KZ)$ is exceptional and that $KZ \not\geqslant [H, KZ]$. Then $H \neq N_H(KZ)$, whence $|G : N_G(KZ)| \geqslant p$. Moreover, we have

$$|\mathscr{D}_{G,Z}(M, K^g Z)| = |\mathscr{D}_{G,Z}(M, KZ)|$$

for all $g \in G$. Hence it follows from Eq. (4.3) that

$$\begin{aligned} \sum_{N_G(KZ)g \in N_G(KZ)\backslash G} |\mathscr{D}_{G,Z}(M, K^g Z)| &= |G : N_G(KZ)| \cdot |\mathscr{D}_{G,Z}(M, KZ)| \\ &\equiv 0 \mod p^{u+2}. \end{aligned}$$

Since G acts on $\mathscr{L}_2$ by conjugation, the second assertion is an immediate consequence of this fact. The lemma is proved. □

By Lemmas 4.2 and 4.4, Eq. (4.1) is equivalent to the congruence

$$\sum_{KZ\in\mathscr{L}} |\mathscr{D}_{G,Z}(M, KZ)| \equiv 0 \mod \gcd(p^{u+2}, |H|). \tag{4.4}$$

By Theorem 2.3, Eq. (4.1) holds if H is exceptional. We assume that H is not exceptional.

Lemma 4.5 *Let* $K \in \mathscr{I}(N, H)$. *If* $KZ \in \mathscr{L}$, *then* $|H : C_H(K)| = p$.

Proof — Suppose $KZ \in \mathscr{L}$. Clearly, $C_H(K) = C_H(KZ)$. Thus, $C_H(K)$ is exceptional, whereas H is not. In particular, $H \neq C_H(K)$. Let x be a generator of K, and take an element y of $H - C_H(K)$. Since $|Z| = p$ and $Z \geqslant [H, K]$, it follows that $Z = [H, K] = \langle [y, x] \rangle$. We now define a map φ from H to Z by setting $\varphi(h) = [h, x]$ for all $h \in H$. Observe that

$$[h_1h_2, x] = [h_1, x]^{h_2}[h_2, x] = [h_1, x][h_2, x] \in Z$$

for all $h_1, h_2 \in H$. Thus φ is a homomorphism. Also, $C_H(K) = \ker\varphi$ and $Z = \operatorname{Im}\varphi$. Consequently, we have $|H : C_H(K)| = p$, completing the proof. □

By Lemma 4.5, Eq. (4.1) holds if H possesses no exceptional maximal subgroup. From now on we assume that Z is a cyclic group of order p and H is a non-exceptional finite p-group of order greater than p^{u+1} possessing an exceptional maximal subgroup.

When $H \ncong H_{16}$, Eq. (4.4) is proved on the basis of the following lemma.

Lemma 4.6 *Suppose that* $H \ncong H_{16}$. *There exists an element* y *of* H *of order* p *such that* $Z\langle y \rangle$ *is a normal subgroup of* G *and* H *is the semidirect product* $C_H(K) \rtimes \langle y \rangle$ *for any* $K \in \mathscr{I}(N, H)$ *with* $KZ \in \mathscr{L}$.

Proof — Let $K \in \mathscr{I}(N, H)$, and suppose that $KZ \in \mathscr{L}$. Then by Lemma 4.5, $C_H(K)$ is an exceptional maximal subgroup of H. Using Theorem 2.8, we can choose an element y of H of order p satisfying the conditions (Y1) and (Y2). We have $Z \leqslant C_H(K)$ and $y \notin C_H(K)$. Thus

$$\Omega_1(Z(H))\langle y \rangle = Z\langle y \rangle \quad \text{and} \quad H = C_H(K) \rtimes \langle y \rangle.$$

Also, $Z\langle y \rangle$ is a normal subgroup of G. This completes the proof. □

For each element y of H of order p, we set

$$\mathscr{L}_y = \{\, KZ \in \mathscr{L} \mid K \in \mathscr{I}(N, H),\ H = C_H(K)\langle y \rangle, \text{ and } Z\langle y \rangle \geqslant [C_G(K),\, Z\langle y \rangle] \,\}.$$

Lemma 4.7 *Let y be an element of H of order p, and let $x \in M$. If $\langle x \rangle \in \mathscr{I}(N, H)$ and if $\langle x \rangle Z \in \mathscr{L}_y$, then $\langle xy \rangle \in \mathscr{I}(N, H)$, $\langle xy \rangle Z \in \mathscr{L}_y$, and there exists a one to one correspondence between $\mathscr{D}_{G,Z}(M, \langle x \rangle Z)$ and $\mathscr{D}_{G,Z}(M, \langle xy \rangle Z)$. Moreover,*

$$\sum_{KZ \in \mathscr{L}_y} |\mathscr{D}_{G,Z}(M, KZ)| \equiv 0 \mod p^{u+2}.$$

Proof — The assertions of the lemma are proved via the following seven steps.

Step 1 Assume that $\langle x \rangle Z \in \mathscr{L}_y$. Then $Z\langle y \rangle$ is $\langle x \rangle$-invariant, and also $|Z\langle y \rangle| \leqslant p^2$ because $|Z| = p$. By Lemma 4.5, $y \notin C_H(x)$, so we have that $|Z\langle y \rangle| = p^2$. This, combined with Proposition 4.1, shows that $|\mathscr{I}(\langle x \rangle, Z\langle y \rangle)| = p^2$. Hence $\langle xy \rangle \in \mathscr{I}(N, H)$.

Step 2 We set $L = C_G(x)$ and $P = Z\langle y \rangle$. Since $\langle x \rangle Z \in \mathscr{L}_y \subset \mathscr{L}$, it follows that $Z = [H, \langle x \rangle] = \langle [y, x] \rangle$ and $P \geqslant [L, P]$. By using Three Subgroup Lemma (see, e.g., [9, Chapter 2, Theorem 2.3] or [17, Chapter 4, Theorem 1.9]), we have

$$[[H, \langle x \rangle], L] = [[\langle x \rangle, L], H] = \{1\},$$

so $[[L, H], \langle x \rangle] = \{1\}$. Thus $L \geqslant [L, H]$, which yields $Z = L \cap P \geqslant [L, P]$. In particular, $Z = [L, \langle y \rangle]$. For any $s \in L$,

$$[sy^m, xy] = [s, y][y, x]^m \in Z \quad \text{with} \quad m = 0, 1, \ldots, p-1$$

(cf. [4, p. 557, (F6)]). Hence we have $Z \geqslant [C_H(x)\langle y \rangle, \langle xy \rangle] = [H, \langle xy \rangle]$ (see, e.g., [9, Chapter 2, Lemma 2.2] or [17, Chapter 4, (3.7)]).

Step 3 Let $s \in L$ and let $m(s)$ be the integer such that $0 \leqslant m(s) < p$ and

$$[sy^{m(s)}, xy] = [s, y][y, x]^{m(s)} = 1, \text{ or equivalently, } sy^{m(s)} \in C_G(xy).$$

Set $h = y^{m(s)}$. For any nonnegative integer k, $h^{s^k} = hz^k$ with $z = [h, s]$,

whence

$$(sh)^k = s^k h^{s^{k-1}} h^{s^{k-2}} \dots h^s h = s^k h^k z^{k(k-1)/2}.$$

This fact implies that, if the order of s is greater than p, then the order of $sy^{m(s)}$ coincides with that of s except for the case where s is of order 4 and $s^2 = z$ (if s is of order 4 and $s^2 = z$, then $(sh)^2 = s^2 z = 1$).

Step 4 Since $sy^{m(s)} \in C_H(xy)$ for each $s \in C_H(x)$, it follows that

$$C_H(x)\langle y \rangle \leqslant C_H(xy)\langle y \rangle \leqslant H = C_H(x)\langle y \rangle.$$

Thus, $H = C_H(xy)\langle y \rangle$. Note that $y \notin C_H(xy)$, so $|H : C_H(xy)| = p$. In particular, $|C_H(xy)| = |C_H(x)| > p^u \geqslant p^2$. We claim that $C_H(xy)$ is exceptional. If $C_H(x) = \langle s \rangle$ for some element s of $C_H(x)$, then

$$C_H(xy) = \langle sy^{m(s)} \rangle$$

by Step 3. Assume that $C_H(x)$ is a non-cyclic 2-group, and choose a set $\{s, t\}$ of generators of $C_H(x)$. Then by Steps 2 and 3, $[s, y], [t, y] \in Z$ and $sy^{m(s)}, ty^{m(t)} \in C_H(xy)$. For any $g \in L$, $[g, y] = 1$ if and only if $m(g) = 0$. Hence $[s, y]^{m(t)}[t, y]^{m(s)} = 1$. By using [17, Chapter 4, (1.1)], we have

$$[sy^{m(s)}, ty^{m(t)}] = [s, y]^{m(t)}[s, t]^{y^{m(s)+m(t)}}[y, t]^{m(s)} = [s, t]^{y^{m(s)+m(t)}},$$

which implies that $[sy^{m(s)}, ty^{m(t)}] = 1$ if and only if $[s, t] = 1$. Moreover, since $C_H(x)$ is not abelian, neither is $C_H(xy)$. Thus $C_H(xy)$ is a non-abelian 2-group of order greater than 2^2. If $|C_H(x)| = 2^3$, then $C_H(xy)$ is dihedral or quaternion. Assume that $|C_H(x)| > 2^3$ and that $\langle s \rangle$ is a cyclic maximal subgroup of $C_H(x)$. By Step 3, $\langle sy^{m(s)} \rangle$ is a cyclic maximal subgroup of $C_H(xy)$. In addition, we have

$$C_H(xy) = \langle sy^{m(s)}, ty^{m(t)} \rangle \quad \text{and} \quad |C_H(xy) : [C_H(xy), C_H(xy)]| = 2^2,$$

because $[sy^{m(s)}, ty^{m(t)}] = [s, t]^{y^{m(s)+m(t)}} (\neq 1)$. This fact, combined with Theorem 2.5, shows that $C_H(xy)$ is non-abelian exceptional, as claimed.

Step 5 By the hypothesis, $\mathscr{D}_{G,Z}(M, \langle x \rangle Z) \neq \emptyset$. Suppose that d is an element of L such that $\langle d \rangle \times \langle x \rangle \in \mathscr{D}_{G,Z}(M, \langle x \rangle Z)$. Then P is $\langle d \rangle$-in-

variant. By Proposition 4.1, we have $|\mathscr{I}(\langle d \rangle, P)| = p^2$. Thus

$$\langle dy^{m(d)} \rangle \times \langle xy \rangle \in \mathscr{D}_{G,Z}(M, \langle xy \rangle Z),$$

which, combined with the facts given in Steps 1, 2, and 4, shows that $\langle xy \rangle Z \in \mathscr{L}$. We have $Z \geqslant [LP, P]$, because $Z \geqslant [L, P]$ by Step 2 and P is abelian. Observe that $L = \langle d, x \rangle C_H(x)$, which yields $G = LP$. Hence $Z \geqslant [C_G(xy), P]$. Moreover, $H = C_H(xy)\langle y \rangle$ by Step 4. Consequently, we have $\langle xy \rangle Z \in \mathscr{L}_y$.

Step 6 Suppose that $C = \langle c \rangle \times N$ with $c \in C$. If $D \in \mathscr{D}_{G,Z}(M, \langle x \rangle Z)$, then by Lemma 3.6, there exists a unique pair (h, z) of $h \in H$ and $z \in Z$ such that $D = \langle ch \rangle \times \langle xz \rangle$. We define a map

$$\psi_y : \mathscr{D}_{G,Z}(M, \langle x \rangle Z) \to \mathscr{D}_{G,Z}(M, \langle xy \rangle Z)$$

by

$$\psi_y(\langle ch \rangle \times \langle xz \rangle) = \langle chy^{m(ch)} \rangle \times \langle xyz \rangle$$

for all $\langle ch \rangle \times \langle xz \rangle \in \mathscr{D}_{G,Z}(M, \langle x \rangle Z)$ with $h \in H$ and $z \in Z$. Observe that $\langle xy \rangle Z \in \mathscr{L}_{y^{-1}}$. Thus the map

$$\psi_{y^{-1}} : \mathscr{D}_{G,Z}(M, \langle xy \rangle Z) \to \mathscr{D}_{G,Z}(M, \langle x \rangle Z)$$

also exists. Clearly, the composition maps $\psi_{y^{-1}} \circ \psi_y$ and $\psi_y \circ \psi_{y^{-1}}$ are the identity maps on $\mathscr{D}_{G,Z}(M, \langle x \rangle Z)$ and $\mathscr{D}_{G,Z}(M, \langle xy \rangle Z)$, respectively. Hence it turns out that ψ_y is a one to one correspondence. This completes the proof of the first statement.

Step 7 We prove the second statement. Let r be a generator of N. If $K \in \mathscr{I}(N, H)$ with $KZ \in \mathscr{L}_y$, then by Lemma 3.6, there exists a unique element h of H such that $K = \langle rh \rangle$. Thus the permutations π_i on $\mathscr{L}_y$ for $i = 0, 1, \ldots, p-1$ given by

$$\pi_i : \langle rh \rangle Z \mapsto \langle rhy^i \rangle Z$$

for all $\langle rh \rangle Z \in \mathscr{L}_y$ with $h \in H$ form a permutation group

$$\{\pi_i \mid i = 0, 1, \ldots, p-1\}$$

on $\mathscr{L}_y$ of order p. Moreover, if $\langle rh \rangle Z \in \mathscr{L}_y$ with $h \in H$, then

by Eq. (4.3),

$$\sum_{i=0}^{p-1} |\mathscr{D}_{G,Z}(M, \langle rhy^i \rangle Z)| = p\,|\mathscr{D}_{G,Z}(M, \langle rh \rangle Z)| \equiv 0 \mod p^{u+2}.$$

Hence the second statement holds. This completes the proof of the lemma. □

The previous lemmas prove Eq. (4.4) except for the case $H \simeq H_{16}$ (see the end of this section). Using Lemma 4.7, we prove Eq. (4.4) in the case where $H = H_{16}$.

Lemma 4.8 *Under the preceding assumptions, if* $p = 2$ *and* $H = H_{16}$, *then*

$$\sum_{KZ \in \mathscr{L}} |\mathscr{D}_{G,Z}(M, KZ)| \equiv 0 \mod 16.$$

Proof — Keep the notation of Example 2.4. Since $Z(H) = \langle abc \rangle$, it follows that $Z = \langle (abc)^2 \rangle$ and $Z = [H, H]$. Let $\langle x \rangle \in \mathscr{I}(N, H)$ with $x \in M$, and suppose that $\langle x \rangle Z \in \mathscr{L}$. Let

$$D := \langle d \rangle \times \langle x \rangle \in \mathscr{D}_{G,Z}(M, \langle x \rangle Z)$$

with $d \in C_G(x)$. By Lemma 4.5, $C_H(x)$ is a D-invariant exceptional subgroup of H of order 8. In particular, $C_H(x)$ is dihedral or quaternion. In either case, $C_H(x)$ possesses a D-invariant cyclic maximal subgroup T, so that $C_H(T)$ is D-invariant. There exists an element y of $C_H(T)$ chosen from among the generators a, b, and c of H such that $H = C_H(x)\langle y \rangle$. Moreover, $\Omega_1(C_H(T)) = Z\langle y \rangle$, which is D-invariant. Since $Z = [H, H]$, it follows that $Z\langle y \rangle$ is a normal subgroup of G. Thus $\langle x \rangle Z \in \mathscr{L}_y$.

By the preceding paragraph, we have $\mathscr{L} = \mathscr{L}_a \cup \mathscr{L}_b \cup \mathscr{L}_c$. Let $\mathscr{H}$ be the set of all $\langle x \rangle Z \in \mathscr{L}$ with $x \in M$ such that $|\mathscr{D}_{G,Z}(M, \langle x \rangle Z)| = 8$. By Lemma 4.4,

$$\sum_{KZ \in \mathscr{L}} |\mathscr{D}_{G,Z}(M, KZ)| \equiv \sum_{KZ \in \mathscr{H}} |\mathscr{D}_{G,Z}(M, KZ)| \mod 16. \tag{4.5}$$

Moreover, it follows from Lemma 4.7 that

$$\sum_{KZ \in \mathscr{L}_y \cap \mathscr{H}} |\mathscr{D}_{G,Z}(M, KZ)| \equiv \sum_{KZ \in \mathscr{L}_y} |\mathscr{D}_{G,Z}(M, KZ)| \equiv 0 \mod 16, \tag{4.6}$$

where $y = a$, b, or c. By Eqs. (4.5) and (4.6), it suffices to verify that $\mathscr{H}$ is a disjoint union of $\mathscr{L}_a \cap \mathscr{H}$, $\mathscr{L}_b \cap \mathscr{H}$, and $\mathscr{L}_c \cap \mathscr{H}$. Suppose that

$$\langle x \rangle Z \in \mathscr{L}_a \cap \mathscr{L}_b$$

with $x \in M$. Then we have $C_H(x) = \langle ca, ab \rangle$. Let

$$\langle d \rangle \times \langle x \rangle \in \mathscr{D}_{G,Z}(M, \langle x \rangle Z)$$

with $d \in C_G(x)$. Since $Z\langle a \rangle$ and $Z\langle b \rangle$ are $\langle d \rangle$-invariant, it follows that $\langle a, b \rangle$ is $\langle d \rangle$-invariant. Hence $\langle ab \rangle$ is $\langle d \rangle$-invariant, and so is $\Omega_1(C_H(ab))$. This implies that $Z\langle c \rangle$ is $\langle d \rangle$-invariant, because

$$C_H(ab) = \langle ab, c \rangle \quad \text{and} \quad \Omega_1(\langle ab, c \rangle) = Z\langle c \rangle.$$

Thus $\langle bc \rangle$ and $\langle ca \rangle$ are $\langle d \rangle$-invariant. By Proposition 4.1, we have

$$|\mathscr{I}(\langle d \rangle, \langle ca \rangle)| = |\mathscr{I}(\langle d \rangle, \langle ab \rangle)| = |\mathscr{I}(\langle d \rangle, \langle bc \rangle)| = 4,$$

which yields $|\mathscr{I}(\langle d \rangle, C_H(x))| = 8$. This, combined with Lemmas 3.4 and 3.7, shows that $|\mathscr{D}_{G,Z}(M, \langle x \rangle Z)| = 16$. Hence $\mathscr{L}_a \cap \mathscr{L}_b \cap \mathscr{H} = \emptyset$. Likewise, $\mathscr{L}_b \cap \mathscr{L}_c \cap \mathscr{H} = \emptyset$ and $\mathscr{L}_c \cap \mathscr{L}_a \cap \mathscr{H} = \emptyset$. Consequently, $\mathscr{H}$ is a disjoint union of $\mathscr{L}_a \cap \mathscr{H}$, $\mathscr{L}_b \cap \mathscr{H}$, and $\mathscr{L}_c \cap \mathscr{H}$. This completes the proof. □

Proof of Theorem 1.3 — The assertion of Theorem 1.3 is equivalent to Eq. (4.1). By the preceding argument, it suffices to verify that Eq. (4.4) holds under the current assumption that Z is a cyclic group of order p and H is a non-exceptional finite p-group of order greater than p^{u+1} possessing an exceptional maximal subgroup. If $H \not\cong H_{16}$, then by Lemma 4.6, $\mathscr{L} = \mathscr{L}_y$ for some element y of H of order p, and hence Eq. (4.4) follows from Lemma 4.7. Hence it follows from Lemma 4.8 that Eq. (4.4) holds in any case. This completes the proof. □

Remark 4.9 The proof of Theorem 1.3 depends heavily on Theorems 2.2, 2.3, and 2.8 which assert crucial results in case $p = 2$. For the arguments in this section, there is no difference between the cases where $p > 2$ and where $p = 2$ except for Step 4 in the proof of Lemma 4.7, and Lemma 4.8.

Appendix

Let H be a finite group of order p^n. For each nonnegative integer e, let $c_{p^e}(H)$ be the number of cyclic subgroups of H of order p^e. By Frobenius theorem, we have

$$\begin{aligned} p^e c_{p^{e+1}}(H) &\equiv -(p^{e+1}-p^e)c_{p^{e+1}}(H) \\ &= -(a_{p^{e+1}}(H) - a_{p^e}(H)) \equiv a_{p^e}(H) \mod p^{e+1} \end{aligned} \tag{A.1}$$

for $0 \leqslant e \leqslant n-1$. Therefore Theorem 2.1 is equivalent to the core of [14, Theorem A(ii)]:

Theorem A.1 *Let H be a finite group of order p^n, and let e be a positive integer less than n. Then $c_{p^{e+1}}(H)$ is not a multiple of p if and only if H is either a cyclic group, or a non-abelian exceptional group and $1 \leqslant e \leqslant n-2$.*

Actually, Murai proved [14, Theorem A(ii)], and the equivalence between [14, Theorem A(i)] and [14, Theorem A(ii)]. The essential part of Theorem A.1 appears in [14, Lemma 1.7] whose proof has been adapted to the proof of Theorem 2.8. We directly prove Theorem 2.1. The proof of the following lemma parallels that of Theorem 2.8, while H_{16} is not set aside in the argument.

Lemma A.2 *Let H be a non-exceptional group of order p^n with $n \geqslant 2$, and suppose that H possesses an exceptional maximal subgroup. Then for each positive integer e less than n, $a_{p^e}(H)$ is a multiple of p^{e+1}.*

Proof — The lemma holds if $H \simeq M(p^n)$. By Theorem 2.5, we may assume that $p = 2$ and H possesses no cyclic maximal subgroup, so that $a_{2^{n-1}}(H) = a_{2^{n-2}}(H) = 2^n$. Suppose that $n \geqslant 4$ and $e \leqslant n-3$. We keep the notation of the second paragraph in the proof of Theorem 2.8. Recall that $C_H(T) = T$ or $|C_H(T) : T| = 2$.

Case 1 Assume that $C_H(T) = T$. In this case, we keep the notation of Case 1 in the proof of Theorem 2.8, together with the assumption that y is an involution. Since $n > 4$, $T\langle h \rangle \simeq SD_{2^{n-1}}$ by Theorem 2.5. Hence we may assume that h is an involution. Let $s \in T\langle h \rangle - T$, and suppose that $s = x^i h$ with $0 \leqslant i < 2^{n-2}$. By Lemma 2.6, we have that $s^2 = 1$ if i is even, and that $s^2 = x^{2^{n-3}}$ otherwise. Recall that $[h, y] \in \langle x^{2^{n-3}} \rangle$. Moreover, we have

$$(sy)^2 = x^i(hy)x^i(hy) = x^i(hy)x^i(yh)(hy)^2 = (hy)^2 = [h, y].$$

Since $T\langle y\rangle \simeq M(2^{n-1})$, Lemma 2.7 yields that $a_{2^e}(T\langle y\rangle) = 2^{e+1}$. Thus

$$a_{2^e}(H) = \begin{cases} 2^{e+1} + 2^{n-1} & \text{if } e \geqslant 2, \\ 4 + 2^{n-3} \quad \text{or} \quad 4 + 2^{n-3} + 2^{n-2} & \text{if } e = 1. \end{cases}$$

Consequently, $a_{2^e}(H)$ is a multiple of 2^{e+1}.

Case 2 Assume that $|C_H(T) : T| = 2$. In this case, we keep the notation of Case 2 in the proof of Theorem 2.8. Obviously, $H = P\langle y\rangle$. We have $P = T\langle z\rangle$ for some $z \in P - T$. Hence

$$H = \langle x, y, z\rangle \quad \text{and} \quad C_H(T) = T \times \langle y\rangle.$$

Let $s \in P - T$. By Lemma 2.6, we have $s^2 \in \langle x^{2^{n-3}}\rangle$. Suppose $s = x^i z$ with $0 \leqslant i < 2^{n-2}$. Since $\Omega_1(C_H(T))$ is a characteristic subgroup of H, it follows that

$$\begin{aligned} s^{-2}(sy)^2 &= s^{-1}ysy = z^{-1}(x^{-i}yx^i)(zy) \\ &= z^{-1}yzy \in \Omega_1(C_H(T)) \cap P = \langle x^{2^{n-3}}\rangle. \end{aligned}$$

Thus $(sy)^4 = 1$. Moreover,

$$(sy)^2 = 1 \text{ if and only if } s^2 = yz^{-1}yz (\in \langle x^{2^{n-3}}\rangle).$$

Obviously, $a_{2^e}(T \times \langle y\rangle) = 2^{e+1}$. Combining these facts with Lemma 2.6, we conclude that

$$a_{2^e}(H) = \begin{cases} 2^{e+1} + 2^{n-1} & \text{if } e \geqslant 2, \\ 4 + 2^{n-2} \text{ or } 4 + 2^{n-1} & \text{if } e = 1 \text{ and if } P \simeq D_{2^{n-1}}, \\ 4 \text{ or } 4 + 2^{n-2} & \text{if } e = 1 \text{ and if } P \simeq Q_{2^{n-1}}, \\ 4 + 2^{n-2} & \text{if } e = 1 \text{ and if } P \simeq SD_{2^{n-1}},\ n \geqslant 5. \end{cases}$$

Hence $a_{2^e}(H)$ is a multiple of 2^{e+1}. This completes the proof. □

Example A.3 Under the notation of Example 2.4 and Case 2 in the proof of Lemma A.2, if $H = H_{16}$ and $x = ca$, then we may consider $y = b \in H_{16}$ and $z = c$ or $ab \in H_{16}$. If $z = c$, then P is dihedral and $(yz)^2 = (bc)^2 = (ca)^2 = x^2$. If $z = ab$, then P is quaternion and $yz^{-1}yz = b(ab)^{-1}b(ab) = (ab)^2 = x^2$. In either case, we reach the fact that $a_2(H_{16}) = 8$.

Remark A.4 Assume that $n \geqslant 4$. Referring to [16, Theorem 2], we set

$$\begin{aligned}
G_2(n) &= \langle x, y, z \mid x^{2^{n-3}} = y^2,\ z^2 = 1,\ [x,y] = x^{-2},\ [x,z] = [y,z] = 1 \rangle \\
&\simeq Q_{2^{n-1}} \times C_2, \\
G_3(n) &= \langle x, y, z \mid x^{2^{n-2}} = y^2 = z^2 = 1,\ [x,y] = x^{-2},\ [x,z] = [y,z] = 1 \rangle \\
&\simeq D_{2^{n-1}} \times C_2, \\
G_4(n) &= \langle x, y, z \mid x^{2^{n-2}} = y^2 = z^2 = 1,\ [x,y] = [x,z] = 1,\ [y,z] = x^{2^{n-3}} \rangle, \\
G_{11}(n) &= \langle x, y, z \mid x^{2^{n-2}} = y^2 = z^2 = 1,\ [x,y] = x^{-2+2^{n-3}},\ [x,z] = [y,z] = 1 \rangle \\
&\simeq SD_{2^{n-1}} \times C_2 \quad (n \geqslant 5), \\
G_{12}(n) &= \langle x, y, z \mid x^{2^{n-2}} = y^2 = z^2 = 1,\ [x,y] = 1,\ [x,z] = x^{-2},\ [y,z] = x^{2^{n-3}} \rangle \\
&\simeq D_{2^{n-1}} \rtimes C_2 \simeq Q_{2^{n-1}} \rtimes C_2 \simeq SD_{2^{n-1}} \rtimes C_2 \quad (n \geqslant 5), \\
G_{15}(n) &= \langle x, y, z \mid x^{2^{n-2}} = y^2 = z^2 = 1, [x,y] = x^{2^{n-3}}, [x,z] = x^{-2+2^{n-3}}, [y,z] = 1 \rangle \\
&\simeq D_{2^{n-1}} \rtimes C_2 \simeq SD_{2^{n-1}} \rtimes C_2 \simeq M(2^{n-1}) \rtimes C_2 \quad (n \geqslant 5), \\
G_{16}(n) &= \langle x, y, z \mid x^{2^{n-2}} = y^2 = z^2 = 1,\ [x,y] = [y,z] = x^{2^{n-3}},\ [x,z] = x^{-2+2^{n-3}} \rangle \\
&\simeq Q_{2^{n-1}} \rtimes C_2 \simeq SD_{2^{n-1}} \rtimes C_2 \simeq M(2^{n-1}) \rtimes C_2 \quad (n \geqslant 5).
\end{aligned}$$

There is an isomorphism $f : H_{16} \to G_4(4)$ given by

$$abc \mapsto x, \quad a \mapsto y, \quad c \mapsto z.$$

Let H be a non-exceptional group of order 2^n which possesses a non-cyclic exceptional maximal subgroup. Let P be a non-cyclic exceptional maximal subgroup of H, and let T be a cyclic maximal subgroup of P. Then by the proofs of Theorem 2.8 and Lemma A.2, $[H, H]$ coincides with the Frattini subgroup of H and is a maximal subgroup of T. Combining this fact with [16, Theorem 2], we have

$$H \simeq G_2(n),\ G_3(n),\ G_{11}(n),\ G_{12}(n),\ G_{15}(n),\ G_{16}(n)$$

or $H \simeq H_{16} \simeq G_4(4)$. The maximal subgroups of $G_4(n)$ with $n \geqslant 5$ are as follows:

abelian	$M(2^{n-1})$	$G_4(n-1)$
$\langle x, y \rangle$, $\langle x, z \rangle$, $\langle x, yz \rangle$	$\langle xy, z \rangle$, $\langle zx, y \rangle$, $\langle zx, x^{2^{n-4}}yz \rangle$	$\langle x^2, y, z \rangle$

In $G_4(4)$, $\langle zx, y \rangle = \langle zx, x^{2^{n-4}}yz \rangle \simeq D_8$, $\langle x^2, y, z \rangle \simeq D_8$, and $\langle zx, xy \rangle \simeq Q_8$.

In the following lemma, Eq.(A.3) is a consequence of Hall's enumeration principle [10, Theorem 1.4] and is used for the proof of Theorem A.1 in [14].

Lemma A.5 *Let H be a finite group of order p^n, and let $\mathscr{M}$ be the set of maximal subgroups of H. For each integer e with $0 \leqslant e \leqslant n-2$,*

$$a_{p^e}(H) \equiv \sum_{P \in \mathscr{M}} a_{p^e}(P) \mod p^{e+1} \tag{A.2}$$

and

$$c_{p^{e+1}}(H) \equiv \sum_{P \in \mathscr{M}} c_{p^{e+1}}(P) \mod p. \tag{A.3}$$

Proof — By Eq.(A.1), we have $p^e c_{p^{e+1}}(P) \equiv a_{p^e}(P) \bmod p^{e+1}$ for any $P \in \mathscr{M}$ and $p^e c_{p^{e+1}}(H) \equiv a_{p^e}(H) \bmod p^{e+1}$. Hence Eq. (A.2) is equivalent to Eq. (A.3). We give a concise proof of Eq. (A.3). Let $\mathscr{C}_{e+1}$ denote the set of cyclic subgroups of H of order p^{e+1}. For every K in $\mathscr{C}_{e+1}$, set $\mathscr{M}_{\geqslant K} = \{ P \in \mathscr{M} \mid P \geqslant K \}$ and $R_K = \cap_{P \in \mathscr{M}_{\geqslant K}} P$. We have

$$\mathscr{M}_{\geqslant K} = \{ P \in \mathscr{M} \mid P \geqslant R_K \}.$$

Since R_K possesses the Frattini subgroup of H, it follows that

$$|\mathscr{M}_{\geqslant K}| = \left(p^{|H:R_K|} - 1\right)/(p-1).$$

Consequently, we have

$$\sum_{P \in \mathscr{M}} c_{p^{e+1}}(P) = \sum_{K \in \mathscr{C}_{e+1}} |\mathscr{M}_{\geqslant K}| \equiv c_{p^{e+1}}(H) \mod p,$$

completing the proof. □

Proof of Theorem 2.1 — By Lemma 2.6, we get $a_2(D_{2^n}) = 2 + 2^{n-1}$, $a_2(Q_{2^n}) = 2$, $a_2(SD_{2^n}) = 2 + 2^{n-2}$, and

$$a_{2^e}(D_{2^n}) = a_{2^e}(Q_{2^n}) = a_{2^e}(SD_{2^n}) = 2^e + 2^{n-1}$$

for $2 \leqslant e \leqslant n-1$. The "if" part is a consequence of these facts. We prove the "only if" part. Assume that $a_{p^e}(H)$ is not a multiple of p^{e+1}. If $e = n-1$, then H must be cyclic. We assume that $e \leqslant n-2$. By Lemma A.5, there exists a maximal subgroup, say P, of H such

that $a_{p^e}(P)$ is not a multiple of p^{e+1}. Assume that H is a minimal counter-example. Then H is not exceptional; P is exceptional, however. Hence it follows from Lemma A.2 that $a_{p^e}(H)$ is a multiple of p^{e+1}. This is a contradiction. We have thus proved the theorem. □

REFERENCES

[1] T. Asai – N. Chigira – T. Niwasaki – Y. Takegahara: "On a theorem of P. Hall", *J. Group Theory* 16 (2013), 69–80.

[2] T. Asai – T. Niwasaki – Y. Takegahara: "Crossed homomorphisms from rank 2 abelian to exceptional p-groups", *J. Algebra* 270 (2003), 212–237.

[3] T. Asai – Y. Takegahara: "On the number of crossed homomorphisms", *Hokkaido Math. J.* 28 (1999), 535–543.

[4] T. Asai – Y. Takegahara: "$|\mathrm{Hom}(A, G)|$, IV", *J. Algebra* 246 (2001), 543–563.

[5] T. Asai – T. Yoshida: "$|\mathrm{Hom}(A, G)|$, II", *J. Algebra* 160 (1993), 273–285.

[6] R. Brauer: "On a theorem of Frobenius", *Amer. Math. Monthly* 76 (1969), 12–15.

[7] M. Farrokhi D.G. – Y. Takegahara: "A formula of subgroup normality degrees with applications to the finite p-groups with cyclic subgroups of index p^2", *J. Algebra Appl.* 19 (2020), 2050073, 27pp.

[8] G. Frobenius: "Verallgemeinerung des Sylowschen Satzes", *Sitzungsberichte der Königlich Preußischen Akademie der Wissenschaften zu Berlin* (1895), 981–993; in :"Gesammelte Abhandlungen", Band II, *Springer*, Berlin (1968), 664–676.

[9] D. Gorenstein: "Finite Groups", 2nd Ed., *Chelsea*, New York (1980).

[10] P. Hall: "A contribution to the theory of groups of prime-power order", *Proc. London Math. Soc.* 36 (1933), 29–95.

[11] P. Hall: "On a theorem of Frobenius", *Proc. London Math. Soc.* 40 (1936), 468–501.

[12] G.A. Miller: "Determination of all the groups of order p^m which contain the abelian group of type $(m-2,1)$, p being any prime", *Trans. Amer. Math. Soc.* 2 (1901), 259–272.

[13] G.A. Miller: "On the groups of order p^m which contain operators of order p^{m-2}", *Trans. Amer. Math. Soc.* 3 (1902), 383–387.

[14] M. Murai: "On the number of p-subgroups of a finite group", *J. Math. Kyoto Univ.* 42 (2002), 161–174.

[15] M. Murai – Y. Takegahara: "Hall's relations in finite groups", *J. Algebra* 271 (2004), 312–326.

[16] Y. Ninomiya: "Finite p-groups with cyclic subgroups of index p^2", *Math. J. Okayama Univ.* 36 (1994), 1–21.

[17] M. Suzuki: "Group Theory I, II", *Springer*, New York (1982, 1986).

[18] Y. Takegahara: "The number of subgroups of a finite group (II)", *Comm. Algebra* 47 (2019), 1964–1972.

[19] T. Yoshida: "$|\mathrm{Hom}(A,G)|$", *J. Algebra* 156 (1993), 125–156.

Tsunenobu Asai
Department of Mathematics
Kindai University
Higashi-Osaka (Japan)
e-mail: asai@math.kindai.ac.jp

Naoki Chigira
Department of Mathematics
Kumamoto University
Kumamoto (Japan)
e-mail: chigira@kumamoto-u.ac.jp

Takashi Niwasaki
Department of Mathematics
Ehime University
Matsuyama (Japan)
e-mail: niwasaki.takashi.mb@ehime-u.ac.jp

Yugen Takegahara (*corresponding author*)
Muroran Institute of Technology
Muroran (Japan)
e-mail: yugen@mmm.muroran-it.ac.jp