Hall's Relations in Finite Groups

Hall's Relations in Finite Groups

Masafumi Murai

Meiji-machi 2-27, Izumi Toki-shi, Gifu 509-5146, Japan

and

Yugen Takegahara

Muroran Institute of Technology, 27-1 Mizumoto, Muroran 050-8585, Japan
E-mail: yugen@mmm.muroran-it.ac.jp

Let H be a finite group, and let θ be an automorphism of H whose order divides n. Hall proved that the number of elements x of H that satisfy the relation $x \cdot x^{\theta} \cdot x^{\theta^2} \cdots x^{\theta^{n-1}} = 1$ is a multiple of $\gcd(n, |H|)$. For a prime factor p of $\gcd(n, |H|)$, if such a number is not a multiple of $\gcd(pn, |H|)$, then a Sylow p-subgroup of H is exceptional.

1. INTRODUCTION

Let n be a positive integer. For a finite group H and for an automorphism θ of H whose order divides n, let $L_n(H, \theta)$ denote the set consisting of all elements x of H such that

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

where x^{θ} denotes the effect of θ on x. The following theorem is due to Hall [8, Theorem 1.6].

Hall's Theorem. *For a finite group H and for an automorphism θ of H whose order divides n, $\sharp L_n(H, \theta)$ is a multiple of* $\gcd(n, |H|)$.

Under the hypothesis of the Hall's Theorem, consider the semidirect product of the cyclic group generated by θ and H. Then we have

$$L_n(H, \theta) = \{x \in H \mid (x\theta^{-1})^n = 1\}$$

and

$$\sharp L_n(H, \theta) = \sharp\{x \in H\theta H = \theta H \mid x^n = 1\}.$$

2000*Mathematics Subject Classification* : 20D60, 20D15, 20D45.

Hence the Hall's Theorem is obtained as a special case of the following theorem, which is also due to Hall.

Theorem 1.1. *Let G be a finite group and H a subgroup. For any $y \in G$ and for any $z \in C_G(H)$, the number of elements x in the double coset HyH of H such that $x^n = z$ is a multiple of* $\gcd(n, |H|)$.

Theorem 1.1 is proved in Section 4, though it is a special case of [8, Theorem 1].

For a finite group G, let $a_n(G)$ denote the number of elements x of G that satisfy the equation $x^n = 1$. In the Hall's Theorem, if θ is the identity mapping, then $L_n(H, \theta) = a_n(H)$ and the assertion is due to Frobenius [4, §2, II]:

Frobenius Theorem. *For a finite group G, $a_n(G)$ is a multiple of* $\gcd(n, |G|)$.

Arising out of this theorem, several interesting facts are known (see, e.g., [13]). Our purpose is to investigate the corresponding facts that arise from the Hall's Theorem.

Let p be a prime integer. In connection with the Frobenius Theorem, Kulakoff proved the following theorem [11, Satz 2].

Kulakoff's Theorem. *Suppose that $p > 2$ and that P is a finite non-cyclic group of order p^ℓ. Then, for $0 < m < \ell$, $a_{p^m}(P)$ is a multiple of p^{m+1}.*

Under the assumption $p > 2$, Asai and the second author have proved a generalization of the Kulakoff's Theorem (cf. [1, Theorem 7.1], Theorem 2.9) related to the Hall's Theorem.

We define the exceptional p-groups as follows. If $p > 2$, then the exceptional p-groups are the cyclic p-groups. The exceptional 2-groups are the cyclic, dihedral, generalized quaternion, and quasi-dihedral 2-groups (see [14, Chap. 4, Theorem 4.1]). By the definition, the four-group is exceptional, which seems to be natural for our assertions.

In this paper, we show that, for a finite p-group P and for an automorphism θ of P whose order divides p^u, if $\sharp L_{p^u}(P, \theta)$ is not a multiple of $\gcd(p^{u+1}, |P|)$, then P is an exceptional p-group of order greater than p^u (cf. Theorem 2.8). Furthermore, in Section 4, we establish the following theorem which concerns Theorem 1.1.

Theorem 1.2. *Let G be a finite group and H a subgroup. Suppose that* $\gcd(n, |H|)$ *is divisible by a prime p. For any $y \in G$ and for any $z \in C_G(H)$, if the number of elements x in the double coset HyH of H such that $x^n = z$ is not a multiple of* $\gcd(pn, |H|)$*, then a Sylow p-subgroup of H is an exceptional p-group whose order is greater than the highest power of p dividing n.*

The assertion of Theorem 1.2 with $p > 2$ is a special case of [8, Theorem 1 (iii)].

With regard to the Hall's Theorem, we get the following special case of Theorem 1.2.

Theorem 1.3. *Let H be a finite group, and let θ be an automorphism of H whose order divides n. Suppose that $\gcd(n, |H|)$ is divisible by a prime p. If $\sharp L_n(H, \theta)$ is not a multiple of $\gcd(pn, |H|)$, then a Sylow p-subgroup of H is an exceptional p-group whose order is greater than the highest power of p dividing n.*

Theorems 1.2 and 1.3 are regarded as generalizations of the following theorem which has been established by the first author [13, Corollary B].

Theorem 1.4. *Let G be a finite group. Suppose that $\gcd(n, |G|)$ is divisible by a prime p. Let P be a Sylow p-subgroup of G, and let p^u be the highest power of p dividing n. If $a_n(G)$ is not a multiple of $\gcd(pn, |G|)$, then P is a cyclic group of order greater than p^u, or else $p = 2$ and P is a non-cyclic exceptional 2-group of order greater than 2^{u+1}.*

The Kulakoff's Theorem is a special case of Theorem 1.4. It follows from [12, Theorem 6.2(Thompson)] that, for a finite 2-group P, $a_2(P)$ is not a multiple of 4 if and only if P is either cyclic or non-abelian exceptional (see also [10, pp. 52-53]). This fact, which is considered as a special case of Theorem 1.4 too, and the Kulakoff's Theorem with $m = 1$ are used for the proof of an essential result, Theorem 2.8, to Theorem 1.2 (see Section 2).

In Section 5, we have certain results (cf. Theorems 5.1 and 5.2) related to Theorem 1.3 and the Frobenius Conjecture which has been shown to be true by Iiyori and Yamaki [9]:

Theorem If the number of elements x of a finite group G that satisfy the equation $x^n = 1$ is equal to $\gcd(n, |G|)$, then such elements form a characteristic subgroup of G.

Notation Let G be a group. We denote by $Z(G)$ the center of G, and denote by $\exp G$ the exponent of G. For subgroups H and K of G, $[H, K]$ denotes the commutator subgroup of H and K. For any element x of G, $\langle x \rangle$ denotes the cyclic subgroup generated by x. If G is a finite p-group, then, for each positive integer u, the characteristic subgroup $\Omega_u(G)$ of G is defined to be the subgroup generated by the elements of order at most p^u.

2. THE CASE OF p-GROUPS

Let $C_2(G)$ denote the commutator subgroup of a group G, and, for each integer i with $i \geq 3$, define inductively $C_i(G)$ to be the commutator subgroup of $C_{i-1}(G)$ and G. By [14, Chap. 4, Theorem 2.5], the lower central series

$$G \geq C_2(G) \geq C_3(G) \geq \cdots$$

reaches $\{1\}$ after a finite number of terms if and only if G is nilpotent. We use the following result which is due to Hall (see [7, §3] and [14, Chap. 4, §3]).

Theorem 2.1. *For elements x and y of a group G and for a positive integer n, there exist $c_i \in C_i(G)$, $2 \leq i \leq n$, such that*

$$x^n y^n = (xy)^n c_2^{e_2} \cdots c_n^{e_n},$$

where the exponent e_i is the i-th binomial coefficient:

$$e_i = \binom{n}{i} = \frac{n(n-1)\cdots(n-i+1)}{i!}.$$

The following corollary to Theorem 2.1 is a part of [1, Corollary 2.2].

Corollary 2.2. *Let u be a positive integer, and let G be a finite p-group such that* $\exp C_2(G) \leq p^{u-1}$ *and* $|C_2(G)| \leq p^u$. *Then* $\exp \Omega_u(G) \leq p^u$.

Proof. We have that p^{u-1} divides $p^u(p^u-1)/2$ in any case. Also, if $3 \leq i \leq u+2$, then p^{u-i+2} divides

$$\binom{p^u}{i} = \frac{p^u}{i}\binom{p^u-1}{i-1},$$

because $i \leq p^{i-2} \leq p^u$ except that $p=2$ and $i=3$. Now the corollary follows from Theorem 2.1. □

Throughout this section, u is a positive integer, P is a finite p-group, and θ is an automorphism of P whose order divides p^u. Let C be an arbitrary cyclic group of order p^u. We define the homomorphism ρ from C to the automorphism group of P by $\rho(c) = \theta$ for a generator c of C. Let CP be the semidirect product of C and P with respect to the action ρ [14, Chap. 1, (8.3)]. Then we have

$$L_{p^u}(P,\theta) = \{x \in P \mid (xc^{-1})^{p^u} = 1\}. \tag{1}$$

For calculation of commutators, we often use the following properties.

(F1) *Suppose that a finite group G is the product of an abelian subgroup and a normal subgroup H. Then $C_2(G) = [H,G]$* ([1, Lemma 2.4]).

(F2) *Under the hypothesis of* (F1), *if G is a p-group and $H \neq \{1\}$, then $C_2(G)$ is a proper subgroup of H* ([1, Lemma 2.5]).

The fact (F1) is an immediate consequence of [14, Chap. 4, (1.1)], and (F2) is deduced from (F1) and [14, Chap. 4, Theorem 2.9(iii)]. In (F2), if G/H is cyclic, then the assertion is a special case of [14, Chap. 4, p. 43, Corollary 2].

Put $C_1(CP) = P$. If $C_1(CP) \neq \{1\}$, then, by (F2), $C_2(CP)$ is a proper subgroup of $C_1(CP)$. Hence, for each integer i with $i \geq 1$, if $C_i(CP) \neq \{1\}$, then $C_{i+1}(CP)$ is a proper subgroup of $C_i(CP)$. Let j be the least integer such that $|C_{j+1}(CP)| \leq p^{u-1}$. We define a C-invariant normal subgroup $Q_u(CP)$ of P by

$$Q_u(CP) = \Omega_u(C_j(CP))$$

if $j \geq 1$, and $Q_u(CP) = P$ otherwise [1, Definition 2.6]. To simplify the notation, we denote $Q_u(CP)$ by $Q(CP)$. By the definition, we have

$$|Q(CP)| \geq \gcd(p^u, |P|) \quad \text{and} \quad |[Q(CP), CP]| \leq p^{u-1}.$$

Furthermore, we have the following.

Lemma 2.3. *Under the hypothesis above, the following statements hold.*

(a) *Let d be any element of CP, and let $G = \langle d \rangle Q(CP)$. Then $|C_2(G)| \leq p^{u-1}$.*

(b) *We have $\exp Q(CP) \leq p^u$ and $Q(CP) \subseteq L_{p^u}(P, \theta)$.*

Proof. (a) Since $|C_2(G)| \leq |[Q(CP), CP]|$ by (F1), it follows that $|C_2(G)| \leq p^{u-1}$, as desired. (b) By the definition of $Q(CP)$ and Corollary 2.2, we have $\exp Q(CP) \leq p^u$. Hence, the statement (a), together with Corollary 2.2, implies that $\exp CQ(CP) = p^u$. Thereby, $(xc^{-1})^{p^u} = 1$ for any $x \in Q(CP)$. Now, by Eq. (1), we conclude that $Q(CP) \subseteq L_{p^u}(P, \theta)$. □

The following result includes an essential part of the Hall's Theorem.

Proposition 2.4. *Let N be a C-invariant normal subgroup of P such that $\exp N \leq p^u$. Suppose that, for an arbitrary element d of CP, $\exp C_2(\langle d \rangle N) \leq p^{u-1}$ and $|C_2(\langle d \rangle N)| \leq p^u$. Then*

$$\sharp L_{p^u}(P, \theta) \equiv 0 \mod |N|.$$

In particular, $\sharp L_{p^u}(P, \theta) \equiv 0 \bmod |Q(CP)|$ and $\sharp L_{p^u}(P, \theta) \equiv 0 \bmod \gcd(p^u, |P|)$.

Proof. For any $a \in L_{p^u}(P, \theta)$, the cyclic group $D = \langle ca^{-1} \rangle$ generated by ca^{-1} is of order p^u by Eq. (1) and Remark after the proof, and hence the hypothesis and Corollary 2.2 imply that $\exp DN \leq p^u$. Therefore, for any $a \in L_{p^u}(P, \theta)$ and for any $x \in N$, we have $(ca^{-1}x^{-1})^{p^u} = 1$, which, together with Eq. (1), means that $xa \in L_{p^u}(P, \theta)$. Thus N acts on $L_{p^u}(P, \theta)$ by the left multiplication, and therefore $\sharp L_{p^u}(P, \theta)$ is a multiple of $|N|$, as desired. Hence the last assertions follow from Lemma 2.3 and the fact that $|Q(CP)| \geq \gcd(p^u, |P|)$. This completes the proof. □

Remark. For any $x \in P$ such that $(cx)^{p^u} = 1$, the order of cx is p^u, because $(cx)^{p^{u-1}} \in c^{p^{u-1}}P \neq P$.

Let $\mathrm{Z}(C, P)$ be the set of complements of P in CP, i.e.,

$$\mathrm{Z}(C, P) = \{D \leq CP \mid DP = CP,\ D \cap P = \{1\}\},$$

and let $z(C, P) = \sharp\mathrm{Z}(C, P)$. By the remark above and [1, Lemma 3.1],

$$z(C, P) = \sharp\{x \in P \mid (cx)^{p^u} = 1\}.$$

Thus $z(C, P) = \sharp L_{p^u}(P, \theta)$ (see Eq. (1)) and Proposition 2.4 is equivalent to the following proposition.

Proposition 2.5. *Under the hypothesis of Proposition* 2.4, $z(C, P) \equiv 0 \bmod |N|$. *In particular,* $z(C, P) \equiv 0 \bmod |Q(CP)|$ *and* $z(C, P) \equiv 0 \bmod \gcd(|C|, |P|)$.

The last congruence of Proposition 2.5 is the statement of [2, Proposition 3.3].

The following theorem is a consequence of the Kulakoff's Theorem and [12, Theorem 6.2(Thompson)], and is also a part of [13, Theorem A].

Theorem 2.6. *The number $a_p(P)$ is not a multiple of p^2 if and only if P is either cyclic or non-abelian exceptional.*

To get a generalization, Theorem 2.8, of the "only if" part in this theorem, we prepare the following lemma, which is just [1, Theorem 7.2] provided $p = 2$.

Lemma 2.7. *Suppose that $u > 1$. If $z(C, P)$ is not a multiple of* $\gcd(p^{u+1}, |P|)$, *then $|P| \geq p^{u+1}$ and every C-invariant abelian normal subgroup of P is cyclic.*

Proof. Although a proof is completely analogous to that of [1, Theorem 7.2], we give another proof of the lemma.

We choose a counter-example to the lemma such that $|P|$ is minimal. It follows from Proposition 2.5 that $|P| \geq p^{u+1}$ and $|Q(CP)| = p^u$. Also, we emphasize that $P \neq Q(CP)$. Let $p^w = \exp Q(CP)$. We define the C-invariant normal subgroup N of P containing $Q(CP)$ by

$$N/Q(CP) = \Omega_1(P/Q(CP) \cap Z(CP/Q(CP))).$$

Then $\exp N \leq p^{w+1}$, and $|N| \geq p^{u+1}$ because $P \neq Q(CP)$. Take any $d \in CP$. Then, by (F1) and the definition of N,

$$C_2(\langle d \rangle N) \leq [N, CP] \leq Q(CP).$$

So we have $\exp C_2(\langle d \rangle N) \leq p^w$ and $|C_2(\langle d \rangle N)| \leq p^u$.

If $w < u$, then $\exp N \leq p^{w+1} \leq p^u$ and $\exp C_2(\langle d \rangle N) \leq p^w \leq p^{u-1}$ for any $d \in CP$, and hence $z(C, P) \equiv 0 \bmod |N|$ by Proposition 2.5 , which is a contradiction. Therefore $u = w$, and thus $Q(CP)$ is a cyclic group of order p^u. Now, to get a contradiction, we will show that $\exp N \leq p^u$ and $\exp C_2(CP) \leq p^{u-1}$.

By our choice of P, there exists a C-invariant non-cyclic abelian normal subgroup of P. Take a C-invariant elementary abelian normal subgroup T of P of order greater than p, and put $R = Q(CP)T$. Then $|R| \geq p^{u+1}$. We have that $\mathrm{Z}(C, P)$ is a disjoint union of subsets of the form $\mathrm{Z}(D, R)$ for $D \in \mathrm{Z}(C, P)$. So, by the hypothesis, there is a $D \in \mathrm{Z}(C, P)$ such that $z(D, R)$ is not a multiple of p^{u+1}. If $|R| < |P|$, then, by the hypothesis, either $|R| \leq p^u$ or T is cyclic, which a contradiction. Thus $P = R = Q(CP)T$. By (F2), we have $C_2(P) \leq \Omega_{u-1}(Q(CP))$, and hence $|C_2(P)| \leq p^{u-1}$. Now Corollary 2.2 yields $\exp P = p^u$. In particular, $\exp N \leq p^u$.

Set $S = \Omega_{u-1}(Q(CP))T$. Then $C_2(S) \leq \Omega_{u-2}(Q(CP))$ by (F2), and therefore $|C_2(S)| \leq p^{u-2}$. Hence Corollary 2.2 implies that $\exp S = p^{u-1}$. Use the notation $\overline{CP} = CP/T$, and the like. Then, by using (F2), we obtain $C_2(\overline{CP}) \lneq \overline{P}$. Therefore $C_2(\overline{CP}) \leq \overline{S}$, which forces $C_2(CP) \leq S$. Thus $\exp C_2(CP) \leq p^{u-1}$, as desired.

By the preceding paragraphs, $|C_2(\langle d \rangle N)| \leq p^u$ and $\exp C_2(\langle d \rangle N) \leq p^{u-1}$ for any $d \in CP$, and $\exp N \leq p^u$. Hence Proposition 2.5 yields $z(C, P) \equiv 0 \bmod |N|$, which is a contradiction. Consequently, there is no counter-example. We have thus completed the proof. □

Now Theorem 2.6, together with Lemma 2.7, yields the following essential result to Theorem 1.2.

Theorem 2.8. *Suppose that $\sharp L_{p^u}(P, \theta)$ is not a multiple of $\gcd(p^{u+1}, |P|)$. Then P is an exceptional p-group of order greater than p^u. Furthermore, if P is the four-group, then θ is an involution.*

Proof. By the hypothesis, $z(C, P)$ is not a multiple of $\gcd(p^{u+1}, |P|)$. Then it follows from Proposition 2.5 that $|P| \geq p^{u+1}$.

Case (1) First, we assume that $u > 1$. Let

$\mathscr{X}_1$ be the set of abelian subgroups of P of order p^2,
$\mathscr{X}_2$ the set of abelian normal subgroups of P of order p^2,
$\mathscr{X}_3$ the set of C-invariant abelian normal subgroups of P of order p^2,
$\mathscr{X}_4$ the set of C-invariant cyclic normal subgroups of P of order p^2,
$\mathscr{X}_5$ the set of cyclic normal subgroups of P of order p^2, and
$\mathscr{X}_6$ the set of cyclic subgroups of P of order p^2.

By Lemma 2.7, we have $\mathscr{X}_3 = \mathscr{X}_4$. Hence

$$\sharp\mathscr{X}_1 \equiv \sharp\mathscr{X}_2 \equiv \sharp\mathscr{X}_3 = \sharp\mathscr{X}_4 \equiv \sharp\mathscr{X}_5 \equiv \sharp\mathscr{X}_6 \mod p.$$

Since $\sharp\mathscr{X}_1 \equiv 1 \bmod p$ by [4, §4, I] (or [3, §121]), it follows that $\sharp\mathscr{X}_6 \equiv 1 \bmod p$. Enumerating the elements of P of order p^2, we obtain $(p^2 - p)\sharp\mathscr{X}_6 = a_{p^2}(P) - a_p(P)$. Now, by the Frobenius Theorem and the preceding facts,

$$\frac{a_p(P)}{p} \equiv \sharp\mathscr{X}_6 \equiv 1 \mod p.$$

Hence Theorem 2.6 implies that P is exceptional (see also [13, Theorem A(ii)]).

Case (2) We now assume that $u = 1$. By the hypothesis,

$$z(C, P) = \frac{a_p(CP) - a_p(P)}{p-1} \not\equiv 0 \mod p^2,$$

and so the Frobenius Theorem yields

$$\begin{array}{llll} \text{either} & \dfrac{a_p(P)}{p} \not\equiv 0 \mod p, & & \\ \text{or else} & \dfrac{a_p(P)}{p} \equiv 0 \mod p & \text{and} & \dfrac{a_p(CP)}{p} \not\equiv 0 \mod p. \end{array}$$

Now, in the former case, P is cyclic or non-abelian exceptional by Theorem 2.6. Also, in the latter case, CP is exceptional, but P is neither cyclic nor non-abelian exceptional by Theorem 2.6. Then $p = 2$ and CP is a dihedral group of order 8 and P is an elementary abelian group of order 4 (see [14, Chap. 4, (4.2)]). Thus the theorem follows. □

Theorem 2.8 is a generalization of the "only if" part of [13, Theorem A (i)] too. Also, Theorem 2.8 with $p > 2$ is the following paraphrase of [1, Theorem 7.1] of which we give another alternative proof.

Theorem 2.9. *Suppose that $p > 2$, that $|P| \geq p^{u+1}$, and that $\sharp L_{p^u}(P, \theta)$ is not a multiple of p^{u+1}. Then P is cyclic.*

Proof. We use induction on $|P|$. We define a C-invariant cyclic maximal subgroup R of P. If $|P| \geq p^{u+2}$, then let R be a C-invariant maximal subgroup of P. (Note that the number of maximal subgroups of a finite p-group is congruent to 1 modulo p.) In this case, $|R| \geq p^{u+1}$ and, by the hypothesis, there exists a $D \leq CP$ such that $z(D, R)$ is not multiple of p^{u+1}, whence the inductive assumption implies that R is cyclic. If $|P| = p^{u+1}$, then, by an argument similar to the proof of Lemma 2.7, $Q(CP)$ is a C-invariant cyclic maximal subgroup of P, and let $R = Q(CP)$. Thus R is defined in every case. Then CP/R is abelian, because $P/R \leq Z(CP/R)$. So $C_2(CP)$ is cyclic, and, since $p > 2$, CP is regular (see, e.g., [14, Chap. 4 (3.13)(iii)]). Thus $L_{p^u}(P, \theta) = \{x \in P \mid x^{p^u} = 1\} = \Omega_u(P)$ (see, e.g., [14, Chap. 4 Theorem 3.14(i)(ii)]). Now, by the Frobenius Theorem and the hypothesis, $\Omega_u(P)$ is the only subgroup of P of order p^u. Consequently, by [3, §104], P is cyclic. This completes the proof. □

3. PRELIMINARIES FOR GENERAL CASES

In this section, we provide the lemmas for the proofs of Theorems 1.1 and 1.2. Let G be a finite group and H a subgroup. Take elements y and z of G. We denote by $X_n(HyH, z)$ the set of elements x in the double coset HyH of H that satisfy the equation $x^n = z$. Let p^u be the highest power of a prime p dividing n, and let Λ be the set of elements t of G that satisfy the equation $t^{n/p^u} = z$.

From now, we suppose that $z \in C_G(H)$. Then H acts on Λ by the conjugation action; let $O_1, O_2, \ldots, O_r$ be the orbits with respect to this action.

Lemma 3.1. *Let $t_i \in O_i$ for each i. Then*

$$\sharp X_n(HyH, z) = \sum_{i=1}^{r} |H : C_H(t_i)| \sharp X_{p^u}(HyH, t_i).$$

Proof. By the definition of $O_1, O_2, \ldots, O_r$, we have

$$X_n(HyH, z) = \bigcup_{i=1}^{r} \bigcup_{C_H(t_i)h \in C_H(t_i)\backslash H} X_{p^u}(HyH, t_i^h).$$

Furthermore,

$$\sharp X_{p^u}(HyH, t) = \sharp X_{p^u}(HyH, t^h)$$

for all $t \in \Lambda$ and $h \in H$. Thus the lemma follows. □

For each subgroup K of H, let $X_n(HyH, z; K)$ denote the set consisting of all elements x of $X_n(HyH, z)$ with $H \cap H^x = K$, and let $\mathscr{Y}(H, K)$ denote the set of all double cosets KwK of K in G with $KwK \cap X_n(HyH, z; K) \neq \emptyset$. Note that $z \in C_G(H)$ and that the set $X_n(HyH, z; K)$ may be an empty set.

Lemma 3.2. *Let K be a subgroup of H. Suppose that, for each $KwK \in \mathscr{Y}(H, K)$, $\sharp X_n(KwK, z) \equiv 0 \bmod \gcd(n, |K|)$. Then*

$$\sum_{N_H(K)h \in N_H(K)\backslash H} \sharp X_n(HyH, z; K^h) \equiv 0 \mod \gcd(|H : K|n, |H|).$$

Proof. If $KwK \in \mathscr{Y}(H, K)$, then $H \cap H^x = K$ for any $x \in KwK$. Hence we have

$$X_n(HyH, z; K) = \bigcup_{KwK \in \mathscr{Y}(H,K)} X_n(KwK, z). \tag{2}$$

The conjugation action of $N_H(K)$ on $\mathscr{Y}(H, K)$ is the homomorphism φ from $N_H(K)$ to the symmetric group $\Sigma(\mathscr{Y}(H, K))$ on the set $\mathscr{Y}(H, K)$ such that

$$(KwK)^{\varphi(h)} = Kw^hK$$

for all $h \in N_H(K)$ and $KwK \in \mathscr{Y}(H, K)$. We have $\sharp X_n(KwK, z) = \sharp X_n(Kw^hK, z)$ for all $h \in N_H(K)$ and $w \in G$, because $z \in C_G(H)$. Take $h \in N_H(K)$ and $KwK \in \mathscr{Y}(H, K)$ such that $KwK = Kw^hK$. Then $k_1wk_2 = h^{-1}wh$ for some

$k_1, k_2 \in K$, and hence $w^{-1}(hk_1)w = hk_2^{-1} \in H \cap H^w = K$, which forces $h \in K$. Thus $\operatorname{Ker}\varphi = K$ and $N_H(K)/K$ acts semi-regularly on $\mathscr{Y}(H, K)$. Also, by the hypothesis, $\sharp X_n(KwK, z) \equiv 0 \bmod \gcd(n, |K|)$ for each $KwK \in \mathscr{Y}(H, K)$. Combining these facts with Eq. (2), we have

$$\sharp X_n(HyH, z; K) \equiv 0 \mod |N_H(K) : K| \gcd(n, |K|).$$

Since $z \in C_G(H)$, it follows that

$$\sharp X_n(HyH, z; K) = \sharp X_n(HyH, z; K^h)$$

for any $h \in H$. Thus the number of elements x in HyH such that $x^n = z$ and that $H \cap H^x$ is conjugate to K is a multiple of

$$|H : N_H(K)||N_H(K) : K| \gcd(n, |K|) = \gcd(|H : K|n, |H|).$$

This completes the proof of Lemma 3.2. □

4. THE PROOFS OF THEOREMS

First, we prove Theorem 1.1. The proof goes in line with that of [8, Theorem 1].

Proof of Theorem 1.1. We use induction on $|H|$. The theorem clearly holds if $H = \{1\}$. So we may assume that $|H| > 1$. Let p be a prime dividing $\gcd(n, |H|)$. Take $y \in G$ and suppose that $z \in C_G(H)$.

Step 1. Let P be a Sylow p-subgroup of H. Then HyH is a disjoint union of double cosets, say $Py_1P, Py_2P, \ldots$, of P in G. If H is not a p-group, then, by the inductive assumption,

$$\sharp X_n(Py_iP, z) \equiv 0 \mod \gcd(n, |P|)$$

for each i, which yields

$$\sharp X_n(HyH, z) \equiv 0 \mod \gcd(n, |P|).$$

Thereby, we may assume that H is a p-group.

Step 2. Let p^u be the highest power of p dividing n. For any element t of G such that $C_H(t)$ is a proper subgroup of H, HyH is a disjoint union of double cosets of $C_H(t)$ in G, and, by the inductive assumption,

$$\sharp X_{p^u}(HyH, t) \equiv 0 \mod \gcd(p^u, |C_H(t)|).$$

So, if

$$\sharp X_{p^u}(HyH, t) \equiv 0 \mod \gcd(p^u, |H|)$$

for each $t \in G$ such that $t^{n/p^u} = z$ and $C_H(t) = H$, then, by Lemma 3.1,

$$\sharp X_n(HyH, z) \equiv 0 \mod \gcd(p^u, |H|).$$

Thus we may assume that $n = p^u$.

Step 3. For each proper subgroup K of H and for each $w \in G$, the inductive assumption yields

$$\sharp X_n(KwK, z) \equiv 0 \mod \gcd(n, |K|),$$

and hence Lemma 3.2 implies that

$$\sum_{N_H(K)h \in N_H(K)\backslash H} \sharp X_n(HyH, z; K^h) \equiv 0 \mod \gcd(|H : K|n, |H|).$$

Now, if $H^y \neq H$, then, for any element x in HyH, $H^x \neq H$, and therefore $H \cap H^x$ is a proper subgroup of H. Hence, by the preceding argument, we may assume that $H^y = H$.

Step 4. By the preceding steps, H is a p-group, $n = p^u$, and $H^y = H$. Then

$$\sharp X_n(HyH, z) = \sharp\{h \in H \mid (yh)^n = z\}.$$

We may assume that $y^n = z$. Let θ be the automorphism of H such that $h^\theta = h^{y^{-1}}$ for all $h \in H$. Then $\theta^n = 1$, because $h^{\theta^n} = h^{y^{-n}} = h^{z^{-1}} = h$. For each $h \in H$, $(yh)^n = z$ if and only if

$$z = z^{h^{-1}} = (hy)^n = h \cdot h^\theta \cdot h^{\theta 2} \cdots h^{\theta^{n-1}} z.$$

Hence $\sharp X_n(HyH, z) = \sharp L_n(H, \theta)$. Now, by Proposition 2.4, $\sharp L_n(H, \theta)$ is a multiple of $\gcd(n, |H|)$, and so is $\sharp X_n(HyH, z)$. This completes the proof. □

The proof of Theorem 1.2 runs closely parallel to that of Theorem 1.1.

Proof of Theorem 1.2. Take $y \in G$ and suppose that $z \in C_G(H)$.

Step 1. Let P be a Sylow p-subgroup of H. By Theorem 1.1, $\sharp X_n(HyH, z)$ is a multiple of $\gcd(n, |H|)$. Also, HyH is a disjoint union of double cosets, say $Py_1P, Py_2P, \ldots$, of P in G. Hence, if

$$\sharp X_n(Py_iP, z) \equiv 0 \mod \gcd(pn, |P|)$$

for each i, then

$$\sharp X_n(HyH, z) \equiv 0 \mod \gcd(pn, |H|).$$

Thereby, we may assume that H is a p-group.

Step 2. Let p^u be the highest power of p dividing n. For any element t of G, HyH is a disjoint union of double cosets of $C_H(t)$ in G, and so Theorem 1.1 yields

$$|H : C_H(t)| \sharp X_{p^u}(HyH, t) \equiv 0 \mod \gcd(|H : C_H(t)|p^u, |H|).$$

Here, since H is a p-group, $|H : C_H(t)|$ is a power of p. Hence, if

$$\sharp X_{p^u}(HyH, t) \equiv 0 \mod \gcd(p^{u+1}, |H|)$$

for each $t \in G$ such that $t^{n/p^u} = z$ and $C_H(t) = H$, then, by Lemma 3.1,

$$\sharp X_n(HyH, z) \equiv 0 \mod \gcd(p^{u+1}, |H|).$$

Thus we may assume that $n = p^u$.

Step 3. For each subgroup K of H and for each $w \in G$, Theorem 1.1 yields

$$\sharp X_n(KwK, z) \equiv 0 \mod \gcd(n, |K|),$$

whence, by Lemma 3.2,

$$\sum_{N_H(K)h \in N_H(K)\backslash H} \sharp X_n(HyH, z; K^h) \equiv 0 \mod \gcd(|H : K|n, |H|).$$

Here, since H is a p-group, $|H : K|$ is a power of p. Now, if $H^y \neq H$, then $\sharp X_n(HyH, z)$ is a multiple of $\gcd(pn, |H|)$, because, for any $x \in HyH$, $H \cap H^x$ is a proper subgroup of H and $|H : H \cap H^x|$ is divisible by p. Hence $H^y = H$.

Step 4. By the preceding steps, H is a p-group, $n = p^u$, and $H^y = H$. Further, we may assume that $y^n = z$. Then, by an argument similar to Step 4 of the proof of Theorem 1.1,

$$\sharp X_n(HyH, z) = \sharp L_n(H, \theta),$$

where θ is the automorphism of H such that $h^\theta = h^{y^{-1}}$ for all $h \in H$. Hence, if $\sharp X_n(HyH, z)$ is not a multiple of $\gcd(pn, |H|)$, then neither is $\sharp L_n(H, \theta)$, and so, by Theorem 2.8, H is an exceptional p-group of order greater than p^u. This completes the proof. □

5. FURTHER RESULTS

The following theorem is a consequence of Sylow's theorem.

Theorem 5.1. *Let H be a finite group, and let θ be an automorphism of H whose order divides p^u. Assume that $\sharp L_{p^u}(H, \theta) = \gcd(p^u, |H|)$. Then $L_{p^u}(H, \theta)$ is a subgroup of H.*

Proof. We may assume that $u \geq 1$. Let C be a cyclic group generated by θ. Then C is a p-subgroup of the semidirect product CH of C and H. For a Sylow p-subgroup J of CH containing C, put $P = J \cap H$. Then P is a C-invariant Sylow p-subgroup of H, because both J and H are C-invariant. Now, by Lemma 2.3, $Q(CP) \subseteq L_{p^u}(H, \theta)$. Therefore, since $|Q(CP)| \geq \gcd(p^u, |P|) = \gcd(p^u, |H|)$, $L_{p^u}(H, \theta)$ is equal to the subgroup $Q(CP)$ of P. This completes the proof. □

Example. The quaternion group Q_8 is defined by the relations

$$a^2 = b^2, \qquad bab^{-1} = a^{-1}, \qquad a^4 = 1$$

with generators a and b. Then

$$Q_8 = \{1,\, a,\, a^2,\, a^3,\, b,\, ab,\, a^2b,\, a^3b\}.$$

It is well known that the group $\mathrm{Aut}\, Q_8$ of automorphisms of Q_8 is isomorphic to the symmetric group of degree 4. For every $\theta \in \mathrm{Aut}\, Q_8$ that corresponds to a cycle of length 4, we have that $L_4(Q_8, \theta)$ is a cyclic subgroup of Q_8 of order 4. As an example, take $\theta \in \mathrm{Aut}\, Q_8$ such that $a^\theta = b$ and $b^\theta = a^3$. Then θ fixes each element of $\langle ab \rangle$, and $|\langle \theta \rangle| = 4$. In this case, we get $L_4(Q_8, \theta) = \langle ab \rangle$. Also, for the semidirect product G of $\langle \theta \rangle$ and Q_8, $Q(G) = C_2(G) = \langle ab \rangle$.

Let $C_\infty(H)$ be the last term of the lower central series of a group H, i.e., $C_\infty(H) = C_k(H)$ for the least integer k such that $C_k(H) = C_{k+1}(H)$. In particular, $C_\infty(H) = \{1\}$ if and only if H is nilpotent. We get the following generalization of [5, Theorem 9.4.1].

Theorem 5.2. *Let H be a finite solvable group, and let θ be an automorphism of H whose order divides $n/\gcd(n, |C_\infty(H)|)$. Assume that $\sharp L_n(H, \theta) = \gcd(n, |H|)$. Then $L_n(H, \theta)$ is a subgroup of H.*

Proof. We argue by induction on $|H|$ and prove the theorem by two steps.

Step 1. We first consider the case where H is nilpotent. So H is a direct product of Sylow subgroups (see, e.g., [14, Chap. 4, Theorem 2.12]). We may assume that H is a p-group for a prime p. Put $|H| = p^a$ and $n = p^b c$, where c is prime to p. If $b \geq a$, then $L_n(H, \theta) = H$ and the result follows. Suppose that $a > b$. If $b = 0$, then $L_n(H, \theta) = \{1\}$ and the result follows. So we may assume that $b > 0$. Then, by Theorem 1.3, H is an exceptional p-group. Also, if H is abelian, then the theorem clearly holds. So we suppose that $p = 2$ and that H is a non-abelian exceptional 2-group. Put $|\langle \theta \rangle| = 2^d e$ for an odd integer e.

Case (1a) Assume that $b > d$ and put $n = 2m$ for an integer m. Then we have that the order of θ divides m. Let F be a minimal normal subgroup of $\langle \theta \rangle H$ contained in H, and let $\overline{\theta}$ be the automorphism of H/F induced by θ. By the Hall's Theorem, $\sharp L_m(H/F, \overline{\theta}) \geq \gcd(m, |H/F|)$. For the natural mapping $\phi : H \longrightarrow H/F$, if the image $\phi(x)$ of $x \in H$ is an element of $L_m(H/F, \overline{\theta})$, then $(x\theta^{-1})^m \in F$ and hence $(x\theta^{-1})^n = (x\theta^{-1})^{2m} = 1$, because F is elementary abelian. This fact means that

$$\phi^{-1}(L_m(H/F, \overline{\theta})) = \{x \in H \mid \phi(x) \in L_m(H/F, \overline{\theta})\} \subseteq L_n(H, \theta).$$

Now

$$\sharp L_n(H, \theta) \geq \sharp \phi^{-1}(L_m(H/F, \overline{\theta})) \geq \gcd(m, |H/F|)|F| \geq \gcd(n, |H|)$$

and equality holds throughout. Therefore $\sharp L_m(H/F, \overline{\theta}) = \gcd(m, |H/F|)$ and, by the inductive hypothesis, $L_m(H/F, \overline{\theta})$ is a subgroup of H/F. Furthermore, we have $L_n(H, \theta) = \phi^{-1}(L_m(H/F, \overline{\theta}))$. Thus $L_n(H, \theta)$ is a subgroup of H.

Case (1b) Assume that $b = d$. Then $|\langle\theta\rangle| = 2^b$ by the structure of the group Aut H of automorphisms of H. (Indeed, since H is a non-abelian exceptional 2-group, Aut H is a 2-group unless H is a quaternion group of order 8, in which case Aut H is isomorphic to the symmetric group of degree 4 [14].) Now $\langle\theta\rangle H$ is a 2-group, and, for any $x \in H$, $(x\theta^{-1})^n = 1$ if and only if $(x\theta^{-1})^{2^b} = 1$. Hence $L_n(H, \theta) = L_{2^b}(H, \theta)$ and $L_n(H, \theta)$ is a subgroup of H by Theorem 5.1. Thus the proof is complete in the case where H is nilpotent.

Step 2. By Step 1, we may suppose that H is solvable but not nilpotent. In particular, $C_\infty(H) \neq \{1\}$. Let F be a minimal normal subgroup of $\langle\theta\rangle H$ contained in $C_\infty(H)$, and let $\overline{\theta}$ be the automorphism of H/F induced by θ. So F is an elementary abelian p-group for a prime p.

Case (2a) Assume that n is divisible by p and put $n = pm$ for an integer m. Then the order of $\overline{\theta}$ divides $m/\gcd(m, |C_\infty(H/F)|)$, and so $\sharp L_m(H/F, \overline{\theta}) \geq \gcd(m, |H/F|)$ by the Hall's Theorem. Now, by an argument similar to Case (1a) in Step 1, we conclude that $L_n(H, \theta)$ is a subgroup of H.

Case (2b) Assume that n is not divisible by p. Then there exist integers a and b such that $an + bp = 1$. For any $y \in H$, let $\overline{y}$ denote the coset yF of F in H. We claim that $L_n(H/F, \overline{\theta})$ is a subgroup of H/F of order $\gcd(n, |H|)$. Take $y \in H$ such that $\overline{y} \in L_n(H/F, \overline{\theta})$. Then $(\overline{y}\overline{\theta}^{-1})^n = \overline{1}$, and so $(y\theta^{-1})^{nbp} = 1$. Also, $(y\theta^{-1})^{bp}\theta \in H$ because $\theta^{an} = 1 \in \langle\theta\rangle H$, and therefore

$$(y\theta^{-1})^{bp}\theta \in L_n(H, \theta) = \{x \in H \mid (x\theta^{-1})^n = 1\}.$$

If $\overline{y'} \in L_n(H/F, \overline{\theta})$ for $y' \in H$ and if $(y\theta^{-1})^{bp}\theta = (y'\theta^{-1})^{bp}\theta \in L_n(H, \theta)$, then $(\overline{y'}\,\overline{\theta}^{-1})^n = \overline{1}$ and

$$\overline{y'}\,\overline{\theta}^{-1} = (\overline{y'}\,\overline{\theta}^{-1})^{bp} = (\overline{y}\overline{\theta}^{-1})^{bp} = \overline{y}\overline{\theta}^{-1},$$

which yields $\overline{y'} = \overline{y}$. So we have $\sharp L_n(H/F, \overline{\theta}) \leq \sharp L_n(H, \theta)$. Further, the Hall's Theorem implies that $\sharp L_n(H/F, \overline{\theta}) \geq \gcd(n, |H/F|)$, and therefore

$$\gcd(n, |H/F|) = \gcd(n, |H|) = \sharp L_n(H, \theta) \geq \sharp L_n(H/F, \overline{\theta}) \geq \gcd(n, |H/F|).$$

From this we have

$$\sharp L_n(H/F, \overline{\theta}) = \gcd(n, |H/F|) = \gcd(n, |H|).$$

Since the order of $\overline{\theta}$ divides $n/\gcd(n, |C_\infty(H/F)|)$, by the inductive assumption, $L_n(H/F, \overline{\theta})$ is a subgroup of H/F of order $\gcd(n, |H|)$, as claimed.

Let K be a subgroup of H containing F such that $K/F = L_n(H/F, \overline{\theta})$, and put $C = \langle\theta\rangle$. Since the semidirect product CK of C and K is solvable, it follows from [6, Theorem] that CK possesses a p-complement E containing C (see also [5, Sect. 9.3]). Then $|E| = |C| \gcd(n, |H|)$ and $E = CS$ where $S = E \cap K$. For any $x \in S$, we have $(x\theta^{-1})^n \in E \cap F = \{1\}$. Thus $S \subseteq L_n(H, \theta)$. On the other hand, we have $|S| = \gcd(n, |H|)$. Hence $S = L_n(H, \theta)$ by the hypothesis, and thus $L_n(H, \theta)$ is a subgroup of H. This completes the proof. □

Remark. If A_4 is the alternating group on 4 letters $\{1, 2, 3, 4\}$ and if θ is the automorphism of A_4 induced by the conjugation of the transposition $(1\,2)$, then

$$L_6(A_4, \theta) = \{x \in A_4 \mid (x \cdot x^\theta)^3 = 1\} = \{x \in A_4 \mid x \cdot x^\theta = 1\}$$

and $\sharp L_6(A_4, \theta) = 6 = \gcd(6, |A_4|)$, though $L_6(A_4, \theta)$ is not a subgroup of A_4. Thus, in general, for an automorphism θ of a finite solvable group H such that $\theta^n = 1$ and $\sharp L_n(H, \theta) = \gcd(n, |H|)$, $L_n(H, \theta)$ is not necessarily a subgroup of H unless the order of θ divides $n/\gcd(n, |C_\infty(H)|)$.

REFERENCES

1. T. Asai and Y. Takegahara, $|\mathrm{Hom}(A, G)|$, IV, *J. Algebra* **246** (2001), 543–563.

2. T. Asai and T. Yoshida, $|\mathrm{Hom}(A, G)|$, II, *J. Algebra* **160** (1993), 273–285.

3. W. Burnside, "Theory of Groups of Finite Order," Dover, New York, 1955.

4. G. Frobenius, Verallgemeinerung des Sylowschen Satzes, *Sitzungsberichte der Königlich Preußischen Akademie der Wissenschaften zu Berlin* (1895), 981–993; In :"Gesammelte Abhandlungen," Bd. II, pp. 664–676, Springer-Verlag Berlin/New York, 1968.

5. M. Hall, Jr., "The Theory of Groups," 2nd ed., Chelsea, New York, 1976.

6. P. Hall, A note on soluble groups, *J. London Math. Soc.* **3** (1928), 98–105.

7. P. Hall, A contribution to the theory of groups of prime-power order, *Proc. London Math. Soc.* (2) **36** (1933), 29–95.

8. P. Hall, On a theorem of Frobenius, *Proc. London Math. Soc.* (2) **40** (1936), 468–501.

9. N. Iiyori and H. Yamaki, On a conjecture of Frobenius, *Bull. Amer. Math. Soc.* **25** (1991), 413–416.

10. I. M. Isaacs, "Character Theory of Finite Groups," Dover, New York, 1994.

11. A. Kulakoff, Über die Anzahl der eigentlichen Untergruppen und der Elemente von gegebener Ordnung in p-Gruppen, *Math. Ann.* **104** (1931), 778–793.

12. T. Y. Lam, Artin exponent of finite groups, *J. Algebra* **9** (1968), 94–119.

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

14. M. Suzuki, "Group Theory I, II," Springer-Verlag, New York, 1982, 1986.