J. Group Theory **16** (2013), 69–80
DOI 10.1515/jgt-2012-0034

On a theorem of P. Hall

Tsunenobu Asai, Naoki Chigira, Takashi Niwasaki and Yugen Takegahara

Communicated by Robert M. Guralnick

Abstract. For a finite group A and for a finite group G on which A acts, the number of crossed homomorphisms from A to G is a multiple of $\gcd(|A/B|, |G|)$ provided that B is a normal subgroup of A such that A/B is cyclic. We prove a character-theoretic version of this fact, which was inspired by a theorem of P. Hall.

1 Introduction

Throughout the paper let A and G be finite groups. We suppose that A acts on G via an action $\rho \in \mathrm{Hom}(A, \mathrm{Aut}\, G)$, where $\mathrm{Aut}\, G$ is the group of automorphisms of G. Given $a \in A$ and $x \in G$, we denote by $x^{\rho(a)}$ the effect of $\rho(a)$ on x, and simply write $x^a = x^{\rho(a)}$. Let AG be the semidirect product of G by A such that $a^{-1}xa = x^a$ for all $a \in A$ and $x \in G$. We denote by n a natural number. For each $a \in A$, set $M_n(G, a) = \{x \in G \mid (ax)^n = 1\}$. As $(ax)^n = a^n x^{a^{n-1}} \cdots x^a x$ with $x \in G$, it follows that $M_n(G, a) \neq \emptyset$ if and only if $a^n = 1$.

This paper is motivated by the following special case of [14, Theorem 1.7] (see also [8, (41.23) Theorem]).

Hall's theorem. *Let χ be a $\mathbb{C}$-character of AG. Then for any $a \in A$,*

$$\frac{1}{\gcd(n, |G|)} \sum_{x \in M_n(G,a)} \chi(ax)$$

is an algebraic integer.

We aim to give concise proofs of Hall's theorem and related results, and present a generalization of them (cf. Theorem 1.3).

If a is the identity of A in Hall's theorem, then the assertion is due to Frobenius [12] and the proof is given in [3, 8, 16, 20, 22]. (In this case, it is proved that $(1/\gcd(n, |G|)) \sum_{x \in M_n(G,1)} \chi(x)$ is a rational integer.)

A mapping φ from A to G is called a crossed homomorphism with respect to the action ρ if

$$\varphi(a_1 a_2) = \varphi(a_1)^{a_2} \varphi(a_2) \quad \text{for all } a_1, a_2 \in A.$$

We denote by $\mathrm{Z}_\rho(A, G)$ the set of crossed homomorphisms from A to G with respect to the action ρ. The subgroups $\{a\varphi(a) \mid a \in A\}$, $\varphi \in \mathrm{Z}_\rho(A, G)$, of AG are the complements of G in AG. If $A = \langle a \rangle$, that is, A is a cyclic group generated by an element a, and if $|A| = n$, then the correspondence

$$\mathrm{Z}_\rho(A, G) \to M_n(G, a), \quad \varphi \mapsto \varphi(a), \tag{1.1}$$

is one-to-one. By using this concept, we can see that Hall's theorem is deduced from the following special case (see the proof of Hall's theorem in Section 3).

Theorem 1.1. *Suppose that A is a cyclic group generated by an element a, and let χ be a $\mathbb{C}$-character of AG. Then*

$$\frac{1}{\gcd(|A|, |G|)} \sum_{\varphi \in \mathrm{Z}_\rho(A,G)} \chi(a\varphi(a))$$

is an algebraic integer.

If $\chi = 1_{AG}$, the trivial $\mathbb{C}$-character of AG, in Theorem 1.1, we obtain the following enumeration version, which is equivalent to [14, Theorem 1.6].

Theorem 1.2. *If A is cyclic, then $|\mathrm{Z}_\rho(A, G)|$ is a multiple of* $\gcd(|A|, |G|)$.

If A acts trivially on G, then Theorem 1.2 is [10, Section 2, II], namely,

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

In Sections 2 and 3 we give alternative proofs of Theorems 1.1 and 1.2 and Hall's theorem. As for the proof of Frobenius' theorem, we can refer to several papers and books (see, e.g., [4, 5, 9–11, 13, 15, 18, 23]). Among others Brauer's methods in [4] is applicable to the proof of [19, Theorem 1.1] which is a certain generalization of Theorem 1.2 and is a special case of [14, Theorem 1]. We adapt Brauer's remarkable idea, which is described in Section 2, for our proofs of Theorems 1.1 and 1.2.

In Section 4 we establish the following main theorem of this paper, which is a generalization of Theorem 1.1.

Theorem 1.3. *Let B be a normal subgroup of A. Suppose that A/B is a cyclic group generated by a coset aB of B with $a \in A$. Let χ be a $\mathbb{C}$-character of AG satisfying $b\psi(b) \in \operatorname{Ker}\chi$ for any $b \in B$ and $\psi \in \mathrm{Z}_\rho(A, G)$. Then*

$$\frac{1}{\gcd(|A/B|, |G|)} \sum_{\psi \in \mathrm{Z}_\rho(A,G)} \chi(a\psi(a))$$

is an algebraic integer.

If $\chi = 1_{AG}$ in Theorem 1.3, we obtain the following generalization of Theorem 1.2.

Theorem 1.4. *Let B be a normal subgroup of A, and suppose that A/B is a cyclic group. Then $|\mathrm{Z}_\rho(A,G)|$ is a multiple of* $\gcd(|A/B|, |G|)$.

Let A' be the commutator subgroup of A. If A acts trivially on G, then the assertion of Theorem 1.4 with $B = A'$ is given in [2, Theorem 3.5].

We can now state an interesting consequence of Theorem 1.4:

Corollary 1.5. *Let $e(A/A')$ be the exponent of A/A'. Then $|\mathrm{Z}_\rho(A,G)|$ is a multiple of* $\gcd(e(A/A'), |G|)$.

As a special case of Corollary 1.5, we obtain a result due to Cameron and Müller (cf. [6, Theorem 1]):

Corollary 1.6. *Let p be a prime. If A is a p-group and if $|G|$ is a multiple of p, then $|\mathrm{Z}_\rho(A,G)|$ is a multiple of p.*

2 The proof of Theorem 1.2

We view $\mathrm{Z}_\rho(A,G)$ as a right G-set with the action given by

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

for all $\varphi \in \mathrm{Z}_\rho(A,G)$, $g \in G$, and $a \in A$ (see also [21, p. 243, Exercise 3]). Here, $a\varphi^g(a) = (a\varphi(a))^g$, whence $\varphi^g \in \mathrm{Z}_\rho(A,G)$. Given a subgroup H of G and given $\varphi \in \mathrm{Z}_\rho(A,G)$, we set

$$\mathcal{X}_H(\varphi) = \{\psi \in \mathrm{Z}_\rho(A,G) \mid \psi(a)H = \varphi(a)H \text{ for all } a \in A\}.$$

Obviously, $\psi \in \mathcal{X}_H(\varphi)$ if and only if $\mathcal{X}_H(\psi) = \mathcal{X}_H(\varphi)$.

Lemma 2.1. *Let H be a subgroup of G, and suppose that $\varphi, \varphi' \in \mathrm{Z}_\rho(A,G)$. Then the following statements hold:*

(1) *$\mathcal{X}_H(\varphi) = \mathcal{X}_H(\varphi')$ if and only if $\mathcal{X}_H(\varphi) \cap \mathcal{X}_H(\varphi') \neq \emptyset$.*

(2) *If $h \in H$, then $\mathcal{X}_H(\varphi^h) = \{\psi^h \mid \psi \in \mathcal{X}_H(\varphi)\}$.*

Proof. The statements are straightforward. □

Let H be a subgroup of G, and define

$$\Omega_H = \{\mathcal{X}_H(\varphi) \subset \mathrm{Z}_\rho(A,G) \mid \varphi \in \mathrm{Z}_\rho(A,G)\}.$$

Then by Lemma 2.1 (1), $\mathrm{Z}_\rho(A,G)$ is a disjoint union of its subsets in Ω_H. If $\mathcal{X}_H(\psi) = \mathcal{X}_H(\varphi)$, then it follows from Lemma 2.1 (2) that $\mathcal{X}_H(\psi^h) = \mathcal{X}_H(\varphi^h)$

for all $h \in H$. Hence H acts on Ω_H by $\mathcal{X}_H(\varphi)^h = \mathcal{X}_H(\varphi^h)$ for all $h \in H$ and $\mathcal{X}_H(\varphi) \in \Omega_H$.

Let $\varphi \in \mathrm{Z}_\rho(A, G)$. We set

$$\mathcal{Y}_H(\varphi) = \bigcup_{h \in H} \mathcal{X}_H(\varphi)^h$$

and

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

which is the stabilizer of $\mathcal{X}_H(\varphi)$ in H, and

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

which is a subgroup of AG. Given a subgroup F of G such that $\widetilde{A}_\varphi \leq N_{AG}(F)$, we define the homomorphism ρ_φ from A to $\mathrm{Aut}\, F$ by $x^{\rho_\varphi(a)} = x^{a\varphi(a)}$ for all $a \in A$ and $x \in F$. Here $x^{a\varphi(a)} = \varphi(a)^{-1}a^{-1}xa\varphi(a)$.

The methods in [4, Sections 3 and 4] suggest the next lemma.

Lemma 2.2. *Let H be a subgroup of G, and suppose that $\varphi \in \mathrm{Z}_\rho(A, G)$. Then the following statements hold:*

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

(b) $\widetilde{A}_\varphi \leq N_{AG}(\widetilde{H}_\varphi)$.

(c) $\mathcal{X}_H(\varphi) = \mathcal{X}_{\widetilde{H}_\varphi}(\varphi)$.

(d) $|\mathcal{X}_{\widetilde{H}_\varphi}(\varphi)| = |\mathrm{Z}_{\rho_\varphi}(A, \widetilde{H}_\varphi)|$.

(e) $|\mathcal{Y}_H(\varphi)| = |H : \widetilde{H}_\varphi| \cdot |\mathrm{Z}_{\rho_\varphi}(A, \widetilde{H}_\varphi)|$.

Proof. (a) If $h \in H$ and if $a \in A$, then

$$\varphi(a)H = \varphi^h(a)H \iff \varphi(a)H = (h^a)^{-1}\varphi(a)H \iff h^{a\varphi(a)} \in H.$$

Hence the statement (a) follows.

(b) The statement (b) is an immediate consequence of (a).

(c) Since $\mathcal{X}_H(\varphi) \supset \mathcal{X}_{\widetilde{H}_\varphi}(\varphi)$, it suffices to verify that

$$\mathcal{X}_H(\varphi) \subset \mathcal{X}_{\widetilde{H}_\varphi}(\varphi).$$

To this end, let $\psi \in \mathcal{X}_H(\varphi)$. For any elements $a, b \in A$, if $x = \varphi(a)^{-1}\psi(a)$ and $y = \varphi(b)^{-1}\psi(b) (\in H)$, then

$$\varphi(ab) \cdot x^{b\varphi(b)}H = \varphi(a)^b\varphi(b) \cdot x^{b\varphi(b)} \cdot yH = \psi(a)^b\psi(b)H = \psi(ab)H,$$

whence $x^{b\varphi(b)} \in \varphi(ab)^{-1}\psi(ab)H = H$. This, together with (a), shows that

$$\varphi(a)^{-1}\psi(a) \in \widetilde{H}_\varphi$$

for all $a \in A$. Thus $\psi \in \mathcal{X}_{\widetilde{H}_\varphi}(\varphi)$, which proves (c).

(d) Let $\zeta \in Z_{\rho_\varphi}(A, \widetilde{H}_\varphi)$, and define a mapping $\varphi \cdot \zeta$ from A to G by setting $\varphi \cdot \zeta(a) = \varphi(a)\zeta(a)$ for all $a \in A$. Then $\varphi \cdot \zeta \in \mathcal{X}_{\widetilde{H}_\varphi}(\varphi)$, because

$$\begin{aligned}\varphi(a_1a_2)\zeta(a_1a_2) &= \varphi(a_1)^{a_2}\varphi(a_2)\zeta(a_1)^{a_2\varphi(a_2)}\zeta(a_2)\\ &= \varphi(a_1)^{a_2}\zeta(a_1)^{a_2}\varphi(a_2)\zeta(a_2)\end{aligned}$$

for all $a_1, a_2 \in A$ and $\varphi(a)\zeta(a)\widetilde{H}_\varphi = \varphi(a)\widetilde{H}_\varphi$ for all $a \in A$. Obviously, this correspondence is injective. If $\psi \in \mathcal{X}_{\widetilde{H}_\varphi}(\varphi)$, then

$$\varphi(a_1a_2)^{-1}\psi(a_1a_2) = (\varphi(a_1)^{-1}\psi(a_1))^{a_2\varphi(a_2)}\varphi(a_2)^{-1}\psi(a_2)$$

for all $a_1, a_2 \in A$, and hence there exists an element ζ of $Z_{\rho_\varphi}(A, \widetilde{H}_\varphi)$ satisfying $\zeta(a) = \varphi(a)^{-1}\psi(a)$ for all $a \in A$, i.e., $\psi = \varphi \cdot \zeta$. Thus the correspondence

$$Z_{\rho_\varphi}(A, \widetilde{H}_\varphi) \to \mathcal{X}_{\widetilde{H}_\varphi}(\varphi), \quad \zeta \mapsto \varphi \cdot \zeta$$

is one-to-one, and thereby, the statement (d) follows.

(e) The assertion is an immediate consequence of (c) and (d). □

In order to prove Theorem 1.2 we quote an argument in the proof of [2, Proposition 3.3].

Lemma 2.3. *Let A and G be p-groups. Define normal subgroups $H_0, H_1, \ldots$ of G inductively by $H_0 = \{1\}$ and*

$$H_i/H_{i-1} = \{xH_{i-1} \in Z(AG/H_{i-1}) \cap G/H_{i-1} \mid x^p \in H_{i-1}\}$$

for each positive integer i. Here $Z(AG/H_{i-1})$ is the center of AG/H_{i-1}. Then the following statements hold:

(1) *If $x \in H_i$ and if $y \in AG$, then $(yx)^{p^i} = y^{p^i}$.*

(2) *If $H_{i-1} \neq G$, then $|H_i| \geq p^i$.*

Proof. (1) We have $(yx)^p = y^p z_1$ for some $z_1 \in H_{i-1}$. Likewise,

$$(yx)^{p^2} = y^{p^2} z_2 \quad \text{for some } z_2 \in H_{i-2}.$$

Continuing this procedure, we have

$$(yx)^{p^j} = y^{p^j} z_j \quad \text{with } z_j \in H_{i-j},\ j = 1, 2, \ldots, i.$$

But, $H_0 = \{1\}$. Thus $(yx)^{p^i} = y^{p^i}$.

(2) If $H_{j-1} \neq G$ with $1 \leq j \leq i$, then

$$|H_j/H_{j-1}| \geq p.$$

The assertion is an immediate consequence of this fact. □

The next lemma is applied to Theorems 1.1 and 1.2.

Lemma 2.4. *Let p be a prime. Suppose that A is a cyclic group and that G is a p-group. If $|G|$ divides $|A|$, then $|\mathrm{Z}_\rho(A,G)| = |G|$.*

Proof. Suppose that $A = \langle a \rangle$ and $n = |A|$. Since the correspondence (1.1) is one-to-one, we get $|\mathrm{Z}_\rho(A,G)| = \sharp\{x \in G \mid (ax)^n = 1\}$. Suppose that $n = mp^s$ with $\gcd(p,m) = 1$, and set $B = \langle a^m \rangle$. Then $|B| = p^s$, and $|G|$ divides p^s. Hence Lemma 2.3 with $A = B$ and $y = a^m$ means that $(a^m x)^{p^s} = 1$ for all $x \in G$. Observe now that $(ax)^n = (ax)^{mp^s} = (a^m x^{a^{m-1}} \cdots x^a x)^{p^s} = 1$ for all $x \in G$. Then we obtain $|\mathrm{Z}_\rho(A,G)| = |G|$. □

Recall that $\mathrm{Z}_\rho(A,G)$ is the disjoint union of its subsets in Ω_H. We choose crossed homomorphisms, say $\varphi_H^{(1)}, \varphi_H^{(2)}, \ldots$, so that $\mathrm{Z}_\rho(A,G)$ is the disjoint union of $\mathcal{Y}_H(\varphi_H^{(1)}), \mathcal{Y}_H(\varphi_H^{(2)}), \ldots$, i.e.,

$$\mathrm{Z}_\rho(A,G) = \dot{\bigcup_{i \geq 1}} \mathcal{Y}_H(\varphi_H^{(i)}). \tag{2.1}$$

We are now ready to prove Theorem 1.2.

Proof of Theorem 1.2. Let p be a prime. Using Sylow's theorem, we choose a p-subgroup H of G whose order is the largest power of p dividing $\gcd(|A|,|G|)$. Let $\varphi \in \mathrm{Z}_\rho(A,G)$. Then Lemma 2.4, together with Lemma 2.2, shows that

$$|\mathcal{Y}_H(\varphi)| = |H|.$$

Hence it follows from (2.1) that $|\mathrm{Z}_\rho(A,G)|$ is a multiple of $|H|$. Since p is arbitrary, we conclude that the assertion holds. □

Remark 2.5. In Theorem 1.2, if $|G|$ divides $|A|$, then $|\mathrm{Z}_\rho(A,G)| = |G|$. This fact, which includes Lemma 2.4, is an immediate consequence of the following result due to Brauer [4, Lemma]: *Let L be a group and M a normal subgroup of finite order. If $\sigma \in L$ and if $\alpha \in M$, then $\sigma^{|M|}$ and $(\sigma\alpha)^{|M|}$ are conjugate in L.*

3 The proofs of Theorem 1.1 and Hall's theorem

We provide the key to a character version of Theorem 1.2 (see also [14, pp. 475–476] and [17, Lemma 8.14]).

Lemma 3.1. *Let K be a finite group and F a normal subgroup of K. Let χ be a $\mathbb{C}$-character of K, and suppose that $\{\xi_1, \xi_2, \ldots, \xi_s\}$ is the set consisting of all*

irreducible $\mathbb{C}$-characters ξ of K with $F \leq \operatorname{Ker}\xi$. Then the function

$$\Phi : K \to \mathbb{C}, \quad z \mapsto \frac{1}{|F|}\sum_{x\in F}\chi(zx),$$

on K is expressed by

$$\Phi = \sum_{i=1}^{s}[\chi, \xi_i]_K\xi_i,$$

where $[\chi, \xi_i]_K$ is the inner product of χ and ξ_i.

Proof. By hypothesis, the set of irreducible $\mathbb{C}$-characters of K/F consists of $\widetilde{\xi_i} : K/F \to \mathbb{C}$, $zF \mapsto \xi_i(z)$, with $i = 1, 2, \ldots, s$. The function $\widetilde{\Phi} : K/F \to \mathbb{C}$, $zF \mapsto \Phi(z)$, on K/F is a class function such that

$$[\widetilde{\Phi}, \widetilde{\xi_i}]_{K/F} = \frac{|F|}{|K|}\sum_{zF\in K/F}\frac{1}{|F|}\sum_{x\in F}\chi(zx)\overline{\xi_i(z)} = [\chi, \xi_i]_K$$

for all i. Thus $\widetilde{\Phi} = \sum_{i=1}^{s}[\chi, \xi_i]_K\widetilde{\xi_i}$, which yields the lemma. □

Alternative proof. We may assume that χ is irreducible. By hypothesis, the idempotent $e := (1/|F|)\sum_{x\in F} x$ of the group algebra $\mathbb{C}F$ is central in $\mathbb{C}K$. Observe that any $\mathbb{C}$-representation, say Γ, of K affording χ is viewed as a ring epimorphism from $\mathbb{C}K$ to the full matrix algebra of degree $\chi(1)$ over $\mathbb{C}$. Then $\Gamma(e)$ is the identity matrix I or the zero matrix O. Obviously, if $F \leq \operatorname{Ker}\Gamma$, then $\Gamma(e) = I$. But, if $F \not\leq \operatorname{Ker}\Gamma$, then $\Gamma(e) = O$, because $\Gamma(x)\Gamma(e) = \Gamma(e)$ for all $x \in F$. Moreover, $\Phi(z)$ is the trace of $\Gamma(z)\Gamma(e)$ for all $z \in K$. Hence $\Phi = \chi$ if $F \leq \operatorname{Ker}\chi$, and is 0 otherwise. This completes the proof. □

The following result is essential for Theorem 1.1.

Theorem 3.2. *Let p be a prime. Suppose that A is a cyclic group generated by an element a. Let χ be a $\mathbb{C}$-character of AG. Then*

$$\frac{1}{\gcd(|A|, |G|_p)}\sum_{\varphi\in Z_\rho(A,G)}\chi(a\varphi(a))$$

is an algebraic integer. Here $|G|_p$ is the p-part of $|G|$.

Proof. By Sylow's theorem, there exists a subgroup, say H, of G which is of order $\gcd(|A|, |G|_p)$. By (2.1), we have

$$\sum_{\varphi\in Z_\rho(A,G)}\chi(a\varphi(a)) = \sum_{i\geq 1}\sum_{\varphi\in\mathcal{Y}(\varphi_H^{(i)})}\chi(a\varphi(a)).$$

Hence it suffices to verify that for any $\varphi \in \mathrm{Z}_\rho(A, G)$,

$$\frac{1}{\gcd(|A|, |G|_p)} \sum_{\psi \in \mathcal{Y}_H(\varphi)} \chi(a\psi(a))$$

is an algebraic integer.

Suppose that $r = |H : \widetilde{H}_\varphi|$ and that $h_1, h_2, \ldots, h_r$ is a right transversal of $\widetilde{H}_\varphi$ in H. Then Lemma 2.1 (1) yields $\mathcal{Y}_H(\varphi) = \dot{\bigcup}_{1 \le j \le r} \mathcal{X}_H(\varphi)^{h_j}$. This fact, together with Lemma 2.1 (2), implies that

$$\begin{aligned}\sum_{\psi \in \mathcal{Y}_H(\varphi)} \chi(a\psi(a)) &= \sum_{j=1}^{r} \sum_{\psi \in \mathcal{X}_H(\varphi)^{h_j}} \chi(a\psi(a)) \\ &= \sum_{j=1}^{r} \sum_{\psi \in \mathcal{X}_H(\varphi)} \chi(a\psi^{h_j}(a)).\end{aligned}$$

Since $a\psi^{h_j}(a) = (a\psi(a))^{h_j}$ for all $\psi \in \mathcal{X}_H(\varphi)$ and j, we obtain

$$\sum_{\psi \in \mathcal{Y}_H(\varphi)} \chi(a\psi(a)) = |H : \widetilde{H}_\varphi| \sum_{\psi \in \mathcal{X}_H(\varphi)} \chi(a\psi(a)). \tag{3.1}$$

Observe that by Lemma 2.2, $\mathcal{X}_H(\varphi) = \mathcal{X}_{\widetilde{H}_\varphi}(\varphi)$ and $|\mathcal{X}_{\widetilde{H}_\varphi}(\varphi)| = |\mathrm{Z}_{\rho_\varphi}(A, \widetilde{H}_\varphi)|$. Thus Lemma 2.4 yields $|\mathcal{X}_H(\varphi)| = |\widetilde{H}_\varphi|$, whence

$$\sum_{\psi \in \mathcal{X}_H(\varphi)} \chi(a\psi(a)) = \sum_{x \in \widetilde{H}_\varphi} \chi(a\varphi(a)x).$$

Moreover, it follows from Lemmas 2.2 and 3.1 that $(1/|\widetilde{H}_\varphi|) \sum_{x \in \widetilde{H}_\varphi} \chi(a\varphi(a)x)$ is an algebraic integer. The assertion now follows from (3.1). □

We can now prove Theorem 1.1 and Hall's theorem.

Proof of Theorem 1.1. Since $\chi(a\varphi(a))$ with $\varphi \in \mathrm{Z}_\rho(A, G)$ is an algebraic integer, Theorem 1.1 is a direct consequence of Theorem 3.2 (see, e.g., [7, (4.5) Proposition]). We can also give another explanation. Let π be the set of primes dividing $|G|$, and let $\{\ell_p\}_{p \in \pi}$ be a set of integers satisfying

$$\sum_{p \in \pi} \ell_p \frac{\gcd(|A|, |G|)}{\gcd(|A|, |G|_p)} = 1.$$

Then

$$\frac{1}{\gcd(|A|, |G|)} \sum_{\varphi \in \mathrm{Z}_\rho(A,G)} \chi(a\varphi(a)) = \sum_{p \in \pi} \frac{\ell_p}{\gcd(|A|, |G|_p)} \sum_{\varphi \in \mathrm{Z}_\rho(A,G)} \chi(a\varphi(a)).$$

Thus the assertion follows from Theorem 3.2. □

Proof of Hall's theorem. Let $a \in A$, and suppose that $|\langle a\rangle| = m$. We may assume that m divides n. Let C be a cyclic group generated by c, and suppose that $|C| = n$. Now view G as the C-set with the action defined by $x^c = x^a$ for all $x \in G$, and denote by CG the semidirect product of G by C with respect to this action. Then $M_n(G, c) = M_n(G, a)$. Moreover, $\langle c^m\rangle$ is a normal subgroup of CG and $CG/\langle c^m\rangle \cong \langle a\rangle G$. Hence the assertion follows from Theorem 1.1. □

4 The proof of Theorem 1.3

Let B be a normal subgroup of A, and let $\kappa \in \mathrm{Z}_{\rho|_B}(B, G)$. Set

$$\widetilde{B}_\kappa = \{b\kappa(b) \mid b \in B\}.$$

Then $\widetilde{B}_\kappa$ is a subgroup of AG. We set $G_\kappa = C_G(\widetilde{B}_\kappa)$, which is the stabilizer of κ. Since G is a normal subgroup of AG and $\widetilde{B}_\kappa \cap G = \{1\}$, it follows that $G_\kappa = N_G(\widetilde{B}_\kappa)$. We next set

$$\mathrm{Z}_\rho(A, G; B, \kappa) = \{\psi \in \mathrm{Z}_\rho(A, G) \mid \psi|_B = \kappa\}.$$

Let $\varphi \in \mathrm{Z}_\rho(A, G; B, \kappa)$. The homomorphism $A \to \widetilde{A}_\varphi$, $a \mapsto a\varphi(a)$, which guarantees $\widetilde{B}_\kappa$ to be a normal subgroup of $\widetilde{A}_\varphi$, determines an isomorphism, say γ_φ, from A/B to $\widetilde{A}_\varphi/\widetilde{B}_\kappa$. We now define a homomorphism $\widetilde{\rho}_\varphi$ from $\widetilde{A}_\varphi/\widetilde{B}_\kappa$ to $\mathrm{Aut}\, G_\kappa$ by

$$x^{\widetilde{\rho}_\varphi(a\varphi(a)\widetilde{B}_\kappa)} = x^{a\varphi(a)}$$

for all $a \in A$ and $x \in G_\kappa$, and define $\overline{\rho}_\varphi = \widetilde{\rho}_\varphi \circ \gamma_\varphi$. By definition,

$$x^{\overline{\rho}_\varphi(aB)} = x^{a\varphi(a)}$$

for all $a \in A$ and $x \in G_\kappa$.

The following lemma is essentially shown in [1].

Lemma 4.1. *Let B be a normal subgroup of A, and let $\kappa \in \mathrm{Z}_{\rho|_B}(B, G)$. If we have $\mathrm{Z}_\rho(A, G; B, \kappa) \neq \emptyset$, then for each $\varphi \in \mathrm{Z}_\rho(A, G; B, \kappa)$, there exists a one-to-one correspondence*

$$\mathrm{Z}_\rho(A, G; B, \kappa) \to \mathrm{Z}_{\overline{\rho}_\varphi}(A/B, G_\kappa), \quad \psi \mapsto \zeta$$

such that $\zeta(aB) = \varphi(a)^{-1}\psi(a)$ for all $a \in A$.

Proof. Let $\psi \in \mathrm{Z}_\rho(A, G; B, \kappa)$. Since $a\varphi(a), a\psi(a) \in N_{AG}(\widetilde{B}_\kappa)$, it follows that $\varphi(a)^{-1}\psi(a) \in N_G(\widetilde{B}_\kappa) = G_\kappa$ for all $a \in A$. If $a \in A$ and if $a' = ab$ with $b \in B$, then

$$\varphi(a')^{-1}\psi(a') = \varphi(ab)^{-1}\psi(ab) = (\varphi(a)^{-1}\psi(a))^{b\kappa(b)} = \varphi(a)^{-1}\psi(a).$$

We now define a mapping ζ from A/B to G_κ by setting $\zeta(aB) = \varphi(a)^{-1}\psi(a)$ for all $a \in A$. Then $\zeta \in \mathrm{Z}_{\overline{\rho}_\varphi}(A/B, G_\kappa)$. Conversely, let $\zeta \in \mathrm{Z}_{\overline{\rho}_\varphi}(A/B, G_\kappa)$, and define a mapping ψ from A to G by setting $\psi(a) = \varphi(a)\zeta(aB)$ for all $a \in A$. Then $\psi \in \mathrm{Z}_\rho(A, G; B, \kappa)$. Thus the lemma follows. □

We are now in a position to prove Theorem 1.3.

Proof of Theorem 1.3. We have

$$\sum_{\psi \in \mathrm{Z}_\rho(A,G)} \chi(a\psi(a)) = \sum_{\kappa \in \mathrm{Z}_{\rho|_B}(B,G)} \sum_{\psi \in \mathrm{Z}_\rho(A,G;B,\kappa)} \chi(a\psi(a)). \tag{4.1}$$

Let $\kappa \in \mathrm{Z}_{\rho|_B}(B, G)$, and suppose that $\varphi \in \mathrm{Z}_\rho(A, G; B, \kappa)$. Then there exists a one-to-one correspondence

$$\mathrm{Z}_{\overline{\rho}_\varphi}(A/B, G_\kappa) \to \mathrm{Z}_{\widetilde{\rho}_\varphi}(\widetilde{A}_\varphi/\widetilde{B}_\kappa, G_\kappa), \quad \zeta \mapsto \zeta \circ \gamma_\varphi^{-1}.$$

This, combined with Lemma 4.1, shows that

$$\begin{aligned}\sum_{\psi \in \mathrm{Z}_\rho(A,G;B,\kappa)} \chi(a\psi(a)) &= \sum_{\zeta \in \mathrm{Z}_{\overline{\rho}_\varphi}(A/B,G_\kappa)} \chi(a\varphi(a)\zeta(aB)) \\ &= \sum_{\tilde{\zeta} \in \mathrm{Z}_{\widetilde{\rho}_\varphi}(\widetilde{A}_\varphi/\widetilde{B}_\kappa,G_\kappa)} \chi(a\varphi(a)\tilde{\zeta}(a\varphi(a)\widetilde{B}_\kappa)).\end{aligned}$$

Moreover, χ is viewed as a $\mathbb{C}$-character of $(\widetilde{A}_\varphi/\widetilde{B}_\kappa)G_\kappa$, because $\widetilde{B}_\kappa \leq \mathrm{Ker}\,\chi$ by hypothesis. Hence it follows from Theorem 1.1 that

$$\frac{1}{\gcd(|A/B|, |G_\kappa|)} \sum_{\psi \in \mathrm{Z}_\rho(A,G;B,\kappa)} \chi(a\psi(a))$$

is an algebraic integer. Now let $g \in G$. Recall that $a\psi^g(a) = (a\psi(a))^g$ for all $\psi \in \mathrm{Z}_\rho(A, G; B, \kappa)$ and that

$$\mathrm{Z}_\rho(A, G; B, \kappa^g) = \{\psi^g \mid \psi \in \mathrm{Z}_\rho(A, G; B, \kappa)\}.$$

Then

$$\begin{aligned}\sum_{\psi \in \mathrm{Z}_\rho(A,G;B,\kappa^g)} \chi(a\psi(a)) &= \sum_{\psi \in \mathrm{Z}_\rho(A,G;B,\kappa)} \chi(a\psi^g(a)) \\ &= \sum_{\psi \in \mathrm{Z}_\rho(A,G;B,\kappa)} \chi(a\psi(a)).\end{aligned}$$

Also, $\kappa^g = \kappa$ if and only if $g \in G_\kappa$. Hence

$$\frac{1}{\gcd(|A/B|, |G|)} \sum_{G_\kappa g \in G_\kappa \backslash G} \sum_{\psi \in Z_\rho(A,G;B,\kappa^g)} \chi(a\psi(a))$$
$$= \frac{|G|}{|G_\kappa|} \cdot \frac{\gcd(|A/B|, |G_\kappa|)}{\gcd(|A/B|, |G|)} \cdot \frac{1}{\gcd(|A/B|, |G_\kappa|)} \sum_{\psi \in Z_\rho(A,G;B,\kappa)} \chi(a\psi(a)),$$

which is an algebraic integer. The assertion now follows from (4.1). □

Bibliography

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

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

[3] R. Brauer, A characterization of the characters of groups of finite order, *Ann. of Math. (2)* **57** (1953), 357–377.

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

[5] W. Burnside, *Theory of Groups of Finite Order*, Dover, New York, 1955.

[6] P. J. Cameron and T. W. Müller, A cohomological property of p-groups, *Arch. Math. (Basel)* **82** (2004), 200–204.

[7] C. W. Curtis and I. Reiner, *Methods of Representation Theory*, Volume I, Wiley-Interscience, New York, 1981.

[8] C. W. Curtis and I. Reiner, *Representation Theory of Finite Groups and Associative Algebras*, AMS Chelsea Publishing, Providence, RI, 2006.

[9] A. W. M. Dress, C. Siebeneicher and T. Yoshida, An application of Burnside rings in elementary finite group theory, *Adv. Math.* **91** (1992), 27–44.

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

[11] G. Frobenius, Über einen Fundamentalsatz der Gruppentheorie, *Sitzungsberichte der Königlich Preußischen Akademie der Wissenschaften zu Berlin* (1903), 987–991; in: *Gesammelte Abhandlungen*, Band III, Springer-Verlag, Berlin (1968), 330–334.

[12] G. Frobenius, Über einen Fundamentalsatz der Gruppentheorie II, *Sitzungsberichte der Königlich Preußischen Akademie der Wissenschaften zu Berlin* (1907), 428–437; in: *Gesammelte Abhandlungen*, Band III, Springer-Verlag, Berlin (1968), 394–403.

[13] M. Hall Jr., *The Theory of Groups*, Second edition, Chelsea, New York, 1976.

[14] P. Hall, On a theorem of Frobenius, *Proc. Lond. Math. Soc. (2)* **40** (1936), 468–501.

[15] B. Huppert, *Endliche Gruppen I*, Springer-Verlag, Berlin, 1967.

[16] B. Huppert, *Character Theory of Finite Groups*, de Gruyter Expositions in Mathematics 25, Walter de Gruyter, Berlin, 1998.

[17] I. M. Isaacs, *Character Theory of Finite Groups*, AMS Chelsea Publishing, Providence, 2006.

[18] I. M. Isaacs and G. R. Robinson, On a theorem of Frobenius: Solutions of $x^n = 1$ in finite groups, *Amer. Math. Monthly* **99** (1992), 352–354.

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

[20] L. Solomon, On Schur's index and the solutions of $G^n = 1$ in a finite group, *Math. Z.* **78** (1962), 122–125.

[21] M. Suzuki, *Group Theory I*, Springer-Verlag, New York, 1982.

[22] B. Wagner, A permutation representation theoretical version of a theorem of Frobenius, *Bayreuth. Math. Schr.* **6** (1980), 23–32.

[23] H. Zassenhaus, *The Theory of Groups*, Dover, New York, 1999.

Received August 22, 2011; revised June 29, 2012.

Author information

Tsunenobu Asai, Department of Mathematics, Kinki University,
Higashi-Osaka, Osaka 577-8502, Japan.
E-mail: asai@math.kindai.ac.jp

Naoki Chigira, Department of Mathematics, Kumamoto University,
Kumamoto 860-8555, Japan.
E-mail: chigira@kumamoto-u.ac.jp

Takashi Niwasaki, Department of Mathematics, Ehime University,
Matsuyama 790-8577, Japan.
E-mail: niwasaki.takashi.mb@ehime-u.ac.jp

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