

P. HALL'S STRANGE FORMULA FOR ABELIAN p -GROUPS

Dedicated to professor Tsuyoshi Ohyama's 60-th birthday

TOMOYUKI YOSHIDA

(Received August 27, 1991)

1. Introduction

The purpose of this paper is to study some summations over non-isomorphic abelian p -groups. In particular, for a finite group (or a group which has finitely many solutions of the equation $x^{p^n}=1$ for each $n \geq 1$) G , we study two Dirichlet series as follows:

$$S_G^A(z) := \sum_A' s(A, G) |A|^{-z},$$
$$H_G^A(z) := \sum_A' \frac{h(A, G)}{|\text{Aut } A|} |A|^{-z},$$

where the summation is taken over a complete set of representatives of isomorphism classes of finite abelian p -groups and

$$s(A, G) := \#\{A_1 \leq G \mid A_1 \cong A\},$$
$$h(A, G) := |\text{Hom}(A, G)|.$$

(The above series $S_G^A(z)$ and $H_G^A(z)$ are called the zeta functions of Sylow and Frobenius type in the paper [Yo91] because they appeared in the study of Sylow's third theorem and Frobenius' theorem on the number of solutions of the equation $x^n=1$ on a finite group.)

The main theorem states a relation between them:

Theorem 3.1.

$$H_G^A(z) / S_G^A(z) = \prod_{m=1}^{\infty} (1 - p^{-m-z})^{-1}.$$

In particular, the left hand side is independent of G .

The proof of this theorem is based on the LDU-decomposition of the Hom-set matrix of the category of finite abelian p -groups and on the generating functions related to the Hom-set matrix. See [Yo 87], [Yo 91].

As a corollary, we get P. Hall's strange formula ([Ha 38]):

Corollary 4.4.

$$\sum'_A \frac{1}{|A|} = \sum'_A \frac{1}{|\text{Aut } A|},$$

where the summation is taken over all non-isomorphic abelian p -groups.

In his paper [Ha 38], P. Hall proved this formula as follows: Since the number of isomorphism classes of abelian groups of order p^n equals the partition number $p(n)$,

$$\sum'_A \frac{1}{|A|} = \sum_{n=0}^{\infty} \frac{p(n)}{p^n} = \frac{1}{f_{\infty}(1/p)}.$$

Here for $0 \leq n \leq \infty$, we define

$$f_n(x) := (1-x)(1-x^2)\cdots(1-x^n).$$

Thus an identity of Euler ([An 76,] Corollary 2.2) gives

$$\sum'_A \frac{1}{|A|} = \sum_{n=0}^{\infty} \frac{(1/p)^n}{f_n(1/p)}. \quad (1)$$

Let A be an abelian group of order p^n and of type

$$(1^{\lambda_1} 2^{\lambda_2} \cdots n^{\lambda_n}),$$

that is, A is the direct product of λ_1 cyclic groups of order p , λ_2 cyclic groups of order p^2 , and so on. Let

$$\mu_i := \lambda_i + \lambda_{i+1} + \cdots,$$

so that

$$\mu_1 \geq \mu_2 \geq \cdots \geq 0, \quad \mu_1 + \mu_2 + \cdots = n.$$

Then the order of the automorphism group of A is given by

$$|\text{Aut } A| = \prod_{i \geq 1} f_{\mu_i - \mu_{i+1}}(1/p) p^{\mu_i^2}.$$

Thus in order to prove Corollary 4.4, it will suffice to show that

$$\frac{x^n}{f_n(x)} = \sum_{\sum \mu_i = n} \frac{x^{\mu_1^2 + \mu_2^2 + \cdots}}{f_{\mu_1 - \mu_2}(x) f_{\mu_2 - \mu_3}(x) \cdots}, \quad (2)$$

where the summation is taken over all $(\mu) = (\mu_1, \mu_2, \cdots)$ such that $\mu_1 \geq \mu_2 \geq \cdots \geq 0$ and $\mu_1 + \mu_2 + \cdots = n$.

P. Hall proved (2) by a combinatorial method in his paper ([Ha 38]). His

formula (3) implies another strange formula:

Corollary 4.3. *For any $n \geq 0$,*

$$\sum'_{|A|=p^n} \frac{1}{|\text{Aut } A|} = \sum'_{\text{rk}(A)=n} \frac{1}{|A|}, \tag{3}$$

where the summations are taken over all non-isomorphic abelian p -groups of order p^n , resp. of rank n .

In fact, the RHS of (3) equals the n -th term of the RHS of (1).

As a more general corollary of the main theorem, we have the following identity, which is not found in P. Hall's papers [Ha 38], [Ha 40]:

Corollary 4.2. *Let C be an abelian group of order p^m . Then*

$$\sum'_{|A|=p^m} \frac{|\text{Epi}(C, A)|}{|\text{Aut } A|} = \sum'_{\text{rk}(A)=m-n} \frac{1}{|A|}, \tag{4}$$

where $\text{Epi}(C, A)$ denotes the set of epimorphic homomorphisms from C to A .

We can develop a similar theory for the summations on any category of groups which is closed under subgroups and homomorphic images. Furthermore, in the case of elementary abelian p -groups, it is related with a topological property of p -subgroup complex of a finite group G . See [Yo 91].

I would like to thank the referee of this paper for reading carefully it and pointing out many errors.

2. The Hom-set matrix

In this section, we study the relation between the number of homomorphisms from abelian p -groups into a finite group G and the number of abelian p -subgroups in G . The category of finite groups has the unique epi-mono-factorization property, and so we can apply the method of [Yo 87] to this category

Let A, B, G be finite groups, and define

$$\begin{aligned} h(A, G) &:= |\text{Hom}(A, G)|, \\ s(A, G) &:= \#\{H \leq G \mid H \cong A\}, \\ q(A, B) &:= \#\{A' \trianglelefteq A \mid A/A' \cong B\}, \\ d(A, B) &:= \begin{cases} |\text{Aut } A| & \text{if } A \cong B \\ 0 & \text{otherwise.} \end{cases} \end{aligned}$$

where $\text{Aut } A$ denotes the automorphism group of A . Then $q(A, B) \cdot |\text{Aut } B|$ (resp. $|\text{Aut } A| \cdot s(A, B)$) equals the number of epimorphic (resp. monomorphic) homomorphisms from A to B . We view these families of integers

$(h(A, G)), (s(A, G)), (q(A, G)), (d(A, B))$ as matrices H, A, Q, D , respectively, indexed by isomorphism classes of finite groups.

Lemma 2.1. $H=QDS$ as matrices, that is,

$$|\text{Hom}(A, G)| = \sum'_G \#\{A' \trianglelefteq A \mid A/A' \cong C\} \cdot |\text{Aut } C| \cdot s(C, G), \tag{1}$$

where Σ' denotes the summation over a set of complete representatives of isomorphism classes of finite groups.

Proof. Since each homomorphism from A to G induces a unique epimorphism from A onto its image in G , we have that

$$|\text{Hom}(A, G)| = \sum_{H \leq G} |\text{Epi}(A, H)|,$$

where $\text{Epi}(A, H)$ denotes the set of epimorphisms from A to H . By the homomorphism theorem,

$$|\text{Epi}(A, H)| = \#\{B \trianglelefteq A \mid A/B \cong H\} \cdot |\text{Aut } H| = q(A, H) d(H, H),$$

and hence

$$|\text{Hom}(A, G)| = \sum'_G \#\{A' \trianglelefteq A \mid A/A' \cong C\} \cdot |\text{Aut } C| \cdot s(C, G),$$

as required. □

REMARK. Arranging the isomorphism classes of finite groups in order of the orders, Q (resp. S) makes a lower (resp. upper) uni-triangular matrix. Thus this lemma give an LDU-decomposition of the hom-set matrix H . Similar decomposition holds for any locally finite category with unique epi-mono factorization property. See [Yo 87].

Let p be a prime. We are mainly interested in abelian-groups. First of all, we introduce the *Möbius function* of abelain p -groups:

$$\mu(B) := \begin{cases} (-1)^r p^{\binom{r}{2}} & \text{if } B \cong C_p^r \\ 0 & \text{else.} \end{cases} \tag{2}$$

Then the following lemma is well-known:

Lemma 2.2. For an abelian p -group A ,

$$\sum_{B \leq A} \mu(B) = \begin{cases} 1 & \text{if } A=1 \\ 0 & \text{else.} \end{cases}$$

For the proof, refer to P. Hall [Ha 36] (2.7), [St 86] Example 3.10.2, [Mc 79], p. 97. Note that it suffices to prove it only for an elementary abelian group A . We can now prove the inversion formula.

Proposition 2.3. *Let A be a p -group and G a finite group. Then*

$$s(A, G) = \frac{1}{|\text{Aut } A|} \sum_{B \leq A} \mu(B) h(A/B, G). \tag{3}$$

Proof. By lemma 2.1 we have that

$$\begin{aligned} \text{RHS} &= \sum_{B \leq A} \frac{\mu(B)}{|\text{Aut } A|} \sum'_C q(A/B, C) |\text{Aut } C| s(C, G) \\ &= \sum'_C \frac{|\text{Aut } C|}{|\text{Aut } A|} \left(\sum_{B \leq A} \mu(B) q(A/B, C) \right) s(C, G), \end{aligned}$$

where Σ' denotes the summation over a complete set of representatives of all finite abelian p -groups. Thus it will suffice to show that

$$\sum_{B \leq A} \mu(B) q(A/B, C) = \begin{cases} 1 & \text{if } A \cong C \\ 0 & \text{else.} \end{cases} \tag{4}$$

But this is proved as follows:

$$\begin{aligned} \text{LHS} &= \sum_{B \leq A} \mu(B) \cdot \#\{D/B \leq A/B \mid A/D \cong C\} \\ &= \sum_{\substack{B \leq A \\ : A/D \cong C}} \left(\sum_{B \leq D} \mu(B) \right) \\ &= \begin{cases} 1 & \text{if } A \cong C \\ 0 & \text{else} \end{cases} \end{aligned}$$

by Lemma 2.2, as required. Hence the proposition was proved. □

3. Zeta functions of Sylow and Frobenius type

Throughout this section, G denotes a finite group, and $A, B, C \dots$ denote abelian p -groups. Furthermore, Σ' means a summation over a complete set of isomorphism classes of abelian p -groups. As before, let $s(A, G)$ be the number of subgroups of G isomorphic to A , and let $h(A, G)$ be the number of homomorphisms from A to G .

For any abelian p -groups A, B, C , we define the *Hall polynomial* $g_{B,c}^A$ by

$$g_{B,c}^A := \#\{B_i \leq A \mid B_i \cong B, A/B_i \cong C\}.$$

See [Mc 79] for the general theory of Hall polynomials.

We now define the zeta functions of Sylow and Frobenius types as follows:

$$S_G^{A^p}(z) := \sum'_A s(A, G) |A|^{-z}, \tag{1}$$

$$H_G^{A^p}(z) := \sum'_A \frac{h(A, G)}{|\text{Aut } A|} |A|^{-z}, \tag{2}$$

where, of course, A runs over a complete set of representatives of isomorphism classes of abelian p -groups. Clearly,

$$S_G^{Ap}(z) \in \mathbb{Z}[[p^{-z}]], \quad H_G^{Ap}(z) \in \mathbb{Q}[[p^{-z}]].$$

The following theorem is the main theorem of this paper:

Theorem 3.1. *For any finite group G ,*

$$\frac{H_G^{Ap}(z)}{S_G^{Ap}(z)} = \prod_{m=1}^{\infty} (1 - p^{-m-z})^{-1} \quad (\operatorname{Re} z > -1). \tag{3}$$

In particular, the left hand side is independent of the finite group G .

To prove this theorem, we need the following lemma due to P. Hall [Ha 40] (10). The proof given here is different from the one by P. Hall. See Corollary 4.5.

Lemma 3.2. (P.Hall). *For any finite abelian p -group B, C ,*

$$\sum'_A \frac{1}{|\operatorname{Aut} A|} g_{B,C}^A = \frac{1}{|\operatorname{Aut} B| \cdot |\operatorname{Aut} C|}, \tag{4}$$

where A runs over non-isomorphic abelian p -groups.

Proof. Define a set

$$\mathcal{E}_A(C, B) := \{(f, g) \mid 1 \rightarrow B \xrightarrow{f} A \xrightarrow{g} C \rightarrow 1\}$$

and a map

$$\begin{aligned} \pi : \mathcal{E}_A(C, B) &\rightarrow \{B_1 \leq A \mid A/B_1 \cong C\} \\ &: (f, g) \rightarrow f(B). \end{aligned}$$

Clearly, π is surjective, and if $\pi(f, g) = \pi(f', g')$, then there exist unique $\tau \in \operatorname{Aut} B$ and $\rho \in \operatorname{Aut} C$ such that $f' = f\tau, g' = \rho g$. Thus the cardinality of each fiber equals $|\operatorname{Aut} B| \cdot |\operatorname{Aut} C|$, and so

$$g_{B,C}^A = \frac{|\mathcal{E}_A(C, B)|}{|\operatorname{Aut} B| \cdot |\operatorname{Aut} C|}. \tag{5}$$

Next we let $\operatorname{Aut} A$ act on $\mathcal{E}_A(C, B)$ by

$$\sigma \cdot (f, g) := (\sigma f, g\sigma^{-1})$$

for $\sigma \in \operatorname{Aut} A, (f, g) \in \mathcal{E}_A(C, B)$. There exists a bijective correspondence between the stabilizer of (f, g) and the group homomorphisms:

$$(\operatorname{Aut} A)_{(f,g)} \leftrightarrow \operatorname{Hom}(C, B),$$

by $\sigma \leftrightarrow \eta$, where $a \cdot f(\eta(g(a))) = \sigma(a)$, and so the cardinality of each $\text{Aut } A$ -orbit equals

$$|\text{Aut } A| / |\text{Hom}(C, B)| .$$

Thus

$$|\mathcal{E}_A(C, B)| = \frac{|\text{Aut } A|}{|\text{Hom}(C, B)|} \cdot |\mathcal{E}_A(C, B) / \text{Aut } A| . \tag{6}$$

On the other hand, by the definition of the equivalence of module-extensions, we have that

$$|\text{Ext}^1(C, B)| = \sum'_A |\mathcal{E}_A(C, B) / \text{Aut } A| \tag{7}$$

By (5), (6), (7), we have that

$$\sum'_A \frac{1}{|\text{Aut } A|} g_{B,C}^A = \frac{|\text{Ext}^1(C, B)|}{|\text{Aut } B| \cdot |\text{Aut } C| \cdot |\text{Hom}(C, B)|} .$$

It remains to prove that

$$|\text{Ext}^1(C, B)| = |\text{Hom}(C, B)| . \tag{8}$$

Since there exists an exact sequence $1 \rightarrow F \rightarrow F \rightarrow C \rightarrow 1$, where F is a finitely generated free abelian group, the long exact sequence gives an exact sequence

$$\begin{aligned} 0 \rightarrow \text{Hom}(C, B) &\rightarrow \text{Hom}(F, B) \rightarrow \text{Hom}(F, B) \\ &\rightarrow \text{Ext}^1(C, B) \rightarrow \text{Ext}^1(F, B) = 0 , \end{aligned}$$

which implies that $|\text{Ext}^1(C, B)| = |\text{Hom}(C, B)|$. This proves the lemma. \square

Lemma 3.3. *Let $\mu(B)$ denote the Mobius function of finite abelian p -groups. Then*

$$\sum'_B \frac{\mu(B)}{|\text{Aut } B|} |B|^{-z} = \prod_{m=1}^{\infty} (1 - p^{-m-z}), \quad \text{Re } z > -1 , \tag{9}$$

where B runs over non-isomorphic abelian p -groups.

Proof. Since

$$\mu(B) = \begin{cases} (-1)^n p^{\binom{n}{2}} & \text{if } B \cong C_p^n \\ 0 & \text{if } B \text{ is not elementary abelian,} \end{cases}$$

we have

$$\begin{aligned} \text{LHS} &= \sum_{n=0}^{\infty} \frac{(-1)^n p^{\binom{n}{2}}}{|\text{GL}(n, p)|} p^{-nz} \\ &= \sum_{n=0}^{\infty} \frac{(-p^{-z})^n}{(p-1)(p^2-1)\cdots(p^n-1)} \end{aligned}$$

Thus the required identity follows from the q -binomial theorem ([An 76], Theorem 2.1):

$$\sum_{n=0}^{\infty} \frac{x^n}{(p-1)(p^2-1)\cdots(p^n-1)} = \prod_{m=1}^{\infty} (1+p^{-m}x), \quad |x| < p. \tag{10}$$

□

Proof of Theorem 3.1. The inversion formula Proposition 2.3 gives

$$\begin{aligned} s(A, G) &= \frac{1}{|\text{Aut } A|} \sum_{B \leq A} \mu(B)h(A/B, G) \\ &= \frac{1}{|\text{Aut } A|} \sum'_{B, C} \mu(B)h(C, G)g_{B, C}^A. \end{aligned}$$

Thus

$$\begin{aligned} S_G^{Ap}(z) &= \sum'_A s(A, G)|A|^{-z} \\ &= \sum'_{A, B, C} \frac{\mu(B)h(C, G)}{|\text{Aut } A|} g_{B, C}^A |A|^{-z} \\ &= \sum'_{B, C} \left(\sum'_A \frac{g_{B, C}^A}{|\text{Aut } A|} \right) \mu(B)h(C, G)|B|^{-z}|C|^{-z}. \end{aligned}$$

By Lemma 3.2, we have

$$\begin{aligned} S_G^{Ap}(z) &= \sum'_{B, C} \frac{1}{|\text{Aut } B| \cdot |\text{Aut } C|} \mu(B)h(C, G)|B|^{-z}|C|^{-z} \\ &= \left(\sum'_B \frac{\mu(B)}{|\text{Aut } B|} |B|^{-z} \right) \cdot \left(\sum'_C \frac{h(C, G)}{|\text{Aut } C|} |C|^{-z} \right). \end{aligned}$$

By lemma 3.3, we conclude that

$$S_G^{Ap}(z) = \prod_{m=1}^{\infty} (1-p^{-m-z}) \cdot H_G^{Ap}(z).$$

This proves the theorem. □

4. Corollaries

Theorem 3.1 implies some identities as a special cases.

Corollary 4.1. *Let $\mathcal{A}_p(G)$ denote the set of abelian p -subgroups of a finite group G . Then*

$$\frac{1}{|\mathcal{A}_p(G)|} \sum'_A \frac{h(A, G)}{|\text{Aut } A|} = \sum'_A \frac{1}{|A|}, \tag{1}$$

where the summation is over non-isomorphic abelian p -groups.

Proof. Put $z=0$ in Theorem 3.1. □

Corollary 4.2. *Let C be an abelian group of order p^n . Then for any $m \geq 0$,*

$$\sum'_{|A|=p^m} \frac{|\text{Epi}(C, A)|}{|\text{Aut } A|} = \sum'_{\text{rk}(A)=m-n} \frac{1}{|A|},$$

where $\text{Epi}(C, A)$ denotes the set of epimorphic homomorphisms from C to A .

Proof. By Lemma 2.1, we have

$$H_C(z) = \sum'_A \frac{h(A, G)}{|\text{Aut } A|} |A|^{-z} = \sum'_G \sum'_A \frac{|\text{Epi}(A, C)|}{|\text{Aut } A|} |A|^{-z} s(C, G). \tag{2}$$

The following formula is well-known ([An 76]), (2.1.1)):

$$\begin{aligned} \prod_{m=1}^{\infty} (1 - xp^{-m})^{-1} &= \sum_{k=0}^{\infty} \sum_{n=0}^{\infty} p(k, n) p^{-k} x^n \\ &= \sum'_A \frac{1}{|A|} x^{\text{rk}(A)}, \end{aligned} \tag{3}$$

where $p(k, n)$ denotes the number of partitions of k into n parts and, of course, it is equal to the number of non-isomorphic abelian p -groups of order p^k and of rank n . Thus Theorem 3.1 yields that

$$\begin{aligned} H_C(z) &= S_C(z) \cdot \prod_{m=1}^{\infty} (1 - p^{-z-m})^{-1} \\ &= \sum'_G s(C, G) |C|^{-z} \cdot \sum'_A \frac{1}{|A|} p^{-z \text{rk}(A)} \\ &= \sum'_G \left(\sum'_A \frac{1}{|A|} p^{-z \text{rk}(A)} \right) |C|^{-z} s(C, G). \end{aligned} \tag{4}$$

Thus comparing (2) and (4), an easy induction argument yields that

$$\sum'_A \frac{|\text{Epi}(A, C)|}{|\text{Aut } A|} |A|^{-z} = \sum'_A \frac{1}{|A|} p^{-z \cdot \text{rk}(A)} |C|^{-z}. \tag{5}$$

We now assume that $|C|=p^n$. Then the right hand side of (5) is

$$\begin{aligned} \text{RHS} &= \sum'_A \frac{1}{|A|} p^{-z \cdot (\text{rk}(A)+n)} \\ &= \sum_{m=0}^{\infty} \sum'_{\text{rk}(A)=m-n} \frac{1}{|A|}. \end{aligned}$$

Hence

$$\sum'_{|A|=p^m} \frac{|\text{Epi}(A, C)|}{|\text{Aut } A|} = \sum'_{\text{rk}(A)=m-n} \frac{1}{|A|},$$

as required. □

As a special case of this corollary, we have the following identities (refer to [Ha 40], (7)).

Corollary 4.3. *For any $n \geq 0$,*

$$\sum'_{|A|=p^n} \frac{1}{|\text{Aut } A|} = \sum'_{\text{rk}(A)=n} \frac{1}{|A|}, \tag{6}$$

where the summations are taken over all non-isomorphic abelian p -groups of order p^n , resp. of rank n .

Corollary 4.3 implies P. Hall's strange formula ([Ha 38]):

Corollary 4.4 (P.Hall): $\sum'_A \frac{1}{|\text{Aut } A|} = \sum'_A \frac{1}{|A|}.$

The final corollary is the fundamental theorem of finite abelian groups.

Corollary 4.5. *Any finite abelian p -group is a direct product of some cyclic groups.*

Proof. The formula which P. Hall proved in his paper [Ha 38] is

$$\sum'_{A: \text{known}} \frac{1}{|\text{Aut } A|} = \prod_{m=1}^{\infty} (1-p^{-m})^{-1} = \sum'_{A: \text{known}} \frac{1}{|A|},$$

where A runs over all non-isomorphic abelian p -groups which are direct products of some cyclic groups. On the other hand, the formula proved in this section is just

$$\sum'_{A: \text{all}} \frac{1}{|\text{Aut } A|} = \sum'_{A: \text{known}} \frac{1}{|A|}, \tag{7}$$

where in the first summation, A runs over *all* non-isomorphic abelian p -groups. Comparing the above two formulae, we conclude that all abelian p -groups are known. □

REMARK. In the proof of (7), we used only the property that a finite abelian group A has a free resolution of the type

$$1 \rightarrow F \rightarrow F \rightarrow A \rightarrow 1.$$

See (8) in the proof of Lemma 3.2.

References

[An 76] G.E. ANDREWS: The Theory of Partitions, Addison-Wesley, London, 1976.

- [Ha 38] P. HALL: *A partition formula connected with Abelian groups*, Comment. Math. Helvet. **11** (1938), 126–129.
- [Ha 40] P. HALL: *On groups of automorphisms*, J. reine angew. Math. **182** (1940), 194–204.
- [Mc 79] I.G. MACDONALD: *Symmetric Functions and Hall Polynomials*, Clarendon Press, 1979.
- [St 81] R.P. STANLEY: *A Book Review of I.G. Macdonald's book "Symmetric functions and Hall polynomials"* (Oxford 1979), Bull. Amer. Math. Soc. (New Series), **4** (1981), 254–265.
- [St 86] R.P. STANLEY: *Enumerative Combinatorics, Vol. I*, Wadsworth & Brooks, 1986.
- [Yo 87] T. YOSHIDA: *On the Burnside rings of finite groups and finite categories*, Advanced Studies in Pure Math. **11** (1987), "Commutative Algebra and Combinatorics", 337–353.
- [Yo 91] T. YOSHIDA: $|\text{Hom}(A, G)|$, J. Algebra, to appear.

Department of Mathematics
Kumamoto University
Kurokami 2-3 9-1
Kumamoto 860
Japan

