BULL. AUSTRAL. MATH. SOC. 11A25, 20D30, 20D40
VOL. 75 (2007) [45–58]

ON ARITHMETIC FUNCTIONS OF FINITE GROUPS

ASHISH KUMAR DAS

The object of this paper is to develop and study group theoretic analogues of some of the fundamental concepts and results of arithmetic functions of positive integers.

1. INTRODUCTION

Arithmetic functions (that is, complex valued functions defined on positive integers) play a very important role not only in the theory of numbers but also in almost every branch of Mathematical sciences. Delsarte [4] and Cohen [3] have developed and studied group-theoretic analogues of arithmetic functions using finite Abelian groups, in place of positive integers, as the variables. However, most of their results do not not extend naturally to nonabelian groups. Recently, Leinster [6] developed and studied analogues of the 'sum-of-divisors' function for finite groups, especially for the nonabelian ones. Lucido and Pournaki [7], Mann [8], Marefat [9], Menegazzo [10], and many others have conducted detailed studies on various types of nontrivial group-theoretic arithmetic functions (of course, without calling them arithmetic functions).

Let $\mathcal{G}$ be the collection of all finite groups (up to isomorphism). Then $\mathcal{G}$ can be regarded as a monoid with respect to the direct product of groups (treating the isomorphic groups as the identical ones). The identity element of $\mathcal{G}$ is given by the trivial group $\{e\}$, the group of order 1. Let $\mathcal{A}(\mathcal{G})$ denote the collection of all complex-valued functions with domain $\mathcal{G}$. Three very elementary yet very important members of $\mathcal{A}(\mathcal{G})$ are $|\ |$, u and ε, given by

$$|G| = \text{ the order of } G, \quad u(G) = 1, \quad \text{and} \quad \varepsilon(G) = \begin{cases} 1, & \text{if } G = \{e\} \\ 0, & \text{otherwise} \end{cases}$$

where $G \in \mathcal{G}$. The object of this paper is to extend the ideas of Delsarte and Cohen to all finite groups (Abelian and nonabelian). Properly speaking, we study the structure of $\mathcal{A}(\mathcal{G})$ by developing group-theoretic analogues of some of the fundamental concepts and results of arithmetic functions (see [1]) of positive integers. We also try to characterise finite groups using analogues of divisor functions. It may be mentioned here that most

Received 5th July, 2006

of the group-theoretic analogues developed in this paper coincide, when restricted to the set of postive integers, with their number-theoretic counterparts; noting that the set of positive integers can be identified with the subset of $\mathcal{G}$ consisting of all finite cyclic groups under the injective map $n \mapsto C_n$ where n is a positive integer and $C_n = \mathbb{Z}/n\mathbb{Z}$ is the cyclic group of order n.

2. Coprime groups, multiplicative functions, and convolutions

Let $G \in \mathcal{G}$ be a finite group. Then G has a composition series given by $\{e\} = H_0 \lhd H_1 \lhd \cdots \lhd H_{n-1} \lhd H_n = G$. The set-with-multiplicities of composition factors associated to this composition series is given by $\mathcal{C}(G) = \{H_i/H_{i-1} : i = 1, 2, \ldots, n\}$ and it is uniquely determined by G upto isomorphism of factors (see [5], Jordan-Hölder Theorem). By convention $\mathcal{C}(\{e\}) = \emptyset$. It is a standard fact that $\forall\ K \trianglelefteq G$ the set $\mathcal{C}(G)$ is the disjoint union (that is, union counting multiplicities) of the sets $\mathcal{C}(G/K)$ and $\mathcal{C}(K)$.

We shall say (see [6]) that the groups $G_1, G_2 \in \mathcal{G}$ are *coprime* or *relatively prime* if $\mathcal{C}(G_1)$ and $\mathcal{C}(G_2)$ have no member (that is, composition factor) in common; in case $\mathcal{C}(G_1)$ and $\mathcal{C}(G_2)$ have no Abelian member in common then G_1 and G_2 will be called *almost coprime*. Thus, the groups G_1 and G_2 will be coprime whenever they have coprime orders, and if G_1 and G_2 are Abelian then the converse is also true. It may be mentioned here that the alternating groups A_5 and A_6 are coprime but they do not have coprime orders.

A function $f \in \mathcal{A}(\mathcal{G})$ which is not identically zero will be called *multiplicative* if we have $f(G_1 \times G_2) = f(G_1)f(G_2)$ whenever $G_1, G_2 \in \mathcal{G}$ are coprime; in case $f(G_1 \times G_2) = f(G_1)f(G_2)$ holds for all $G_1, G_2 \in \mathcal{G}$ then f will be called *completely multiplicative*. Further, we shall say that the function f is *almost completely multiplicative* if we have $f(G_1 \times G_2) = f(G_1)f(G_2)$ whenever $G_1, G_2 \in \mathcal{G}$ are almost coprime. Thus, we have $f(\{e\}) = 1$ if f satisfies any of the multiplicativity conditions. It is easy to see that $|\ |$, u and ε are all completely multiplicative functions.

Given $G \in \mathcal{G}$, let $\Pi\mathcal{C}(G)$ denote the direct product of all members (counting multiplicities) of the set-with-multiplicities $\mathcal{C}(G)$. As a convention, we take $\Pi\mathcal{C}\{e\} = \{e\}$. If f and g are any two functions in $\mathcal{A}(\mathcal{G})$ then we shall define their *convolution* to be the function $f * g \in \mathcal{A}(\mathcal{G})$ given by

$$(f * g)(G) = \sum f(H)g(K),$$

where $G \in \mathcal{G}$, and the summation is over all ordered pairs $(H, K) \in \mathcal{G} \times \mathcal{G}$ which satisfy one of the following conditions:

(i) One of H and K is G, and the other is $\{e\}$,

(ii) $H \times K = \Pi\mathcal{C}(G)$, and none of H and K is $\{e\}$.

REMARK 2.1. If $f, g \in \mathcal{A}(\mathcal{G})$ then one can also define their ordinary product $fg \in \mathcal{A}(\mathcal{G})$ given by $fg(G) = f(G)g(G)\ \forall\ G \in \mathcal{G}$. However, the convolution defined above turns out to be more fruitful.

PROPOSITION 2.2. *$\mathcal{A}(\mathcal{G})$ is a commutative ring with identity ε under the additive and the multiplicative operations given respectively by ordinary addition and convolution of functions.*

PROOF: Note that if $f, g, h \in \mathcal{A}(\mathcal{G})$ then

$$\big((f * g) * h\big)(G) = \big(f * (g * h)\big)(G) = \sum f(L)g(M)h(N),$$

where $G \in \mathcal{G}$, and the summation is over all ordered triples $(L, M, N) \in \mathcal{G} \times \mathcal{G} \times \mathcal{G}$ which satisfy one of the following conditions:

(i) One of L, M and N is G, and the other two are $\{e\}$,

(ii) $L \times M \times N = \Pi\mathcal{C}(G)$, and no two of L, M and N are $\{e\}$.

The associative law for multiplication is thus established. The other properties can be easily proved. □

REMARK 2.3. In general, the convolution of two multiplicative functions in $\mathcal{A}(\mathcal{G})$ is not multiplicative. However, if the groups $G_1, G_2 \in \mathcal{G}$ are coprime as well as completely reducible then $(f * g)(G_1 \times G_2) = (f * g)(G_1)\ (f * g)(G_2)$; noting that on the completely reducible groups the convolution mentioned above coincides with the 'direct convolution' which is multiplicative (see [3]).

Consider the factorisation map $\rho : \mathcal{G} \longrightarrow \mathcal{G}$ given by $\rho(G) = \Pi\mathcal{C}(G)$ where $G \in \mathcal{G}$. By Jordan-Hölder Theorem, ρ is well-defined. Clearly, $\rho(G) = G$ if and only if G is completely reducible in $\mathcal{G}$. It is also easy to see that ρ is a monoid homomorphism and it preserves 'coprimeness' of groups in $\mathcal{G}$. thus, if $f \in \mathcal{A}(\mathcal{G})$ is multiplicative then $f \circ \rho \in \mathcal{A}(\mathcal{G})$ is also multiplicative. In fact, we have

PROPOSITION 2.4. *If $f, g \in \mathcal{A}(\mathcal{G})$ are multiplicative then $(f * g) \circ \rho \in \mathcal{A}(\mathcal{G})$ is also multiplicative.*

PROOF: Follows from Remark 2.3. □

From the definition of convolution, it follows that ρ is distributive over convolution. More precisely, we have

PROPOSITION 2.5. *If $f, g \in \mathcal{A}(\mathcal{G})$ then $(f * g) \circ \rho = (f \circ \rho) * (g \circ \rho)$.*

As an immediate consequence we have

COROLLARY 2.6. *ρ induces a unitary ring homomorphism of $\mathcal{A}(\mathcal{G})$ into itself given by $f \mapsto f \circ \rho$ where $f \in \mathcal{A}(\mathcal{G})$.*

As in the case of the ring of arithemetic functions of positive integers, the ring $\mathcal{A}(\mathcal{G})$ also has invertible elements.

PROPOSITION 2.7. *If $f \in \mathcal{A}(\mathcal{G})$ with $f(\{e\}) \neq 0$ then there is a unique $g \in \mathcal{A}(\mathcal{G})$ such that $f * g = g * f = \varepsilon$.*

PROOF: We shall show that, for each $G \in \mathcal{G}$, the equation $f * g(G) = \varepsilon(G)$ has a unique solution for $g(G)$.

If $G = \{e\}$, then the equation $f * g(\{e\}) = \varepsilon(\{e\}) = 1$ has a unique solution given by

$$g(\{e\}) = \frac{1}{f(\{e\})}.$$

So, let $G \in \mathcal{G}$ be nontrivial, and assume that for each $K \in \mathcal{G}$, with $|K| < |G|$, the equation $f * g(K) = \varepsilon(K)$ has a unique solution for $g(K)$. Now, the equation $f * g(G) = \varepsilon(G) = 0$ can be written as

$$f(\{e\})g(G) = -\sum f(H)g(K),$$

where the summation is over all ordered pairs $(H, K) \in \mathcal{G} \times \mathcal{G}$ such that either $H = G$ and $K = \{e\}$, or $H \times K = \Pi\mathcal{C}(G)$ and none of H and K is $\{e\}$. Clearly each such K satisfies $|K| < |G|$, and so by induction hypothesis $g(G)$ is uniquely determined, namely,

$$g(G) = \frac{-1}{f(\{e\})} \sum f(H)g(K),$$

This completes the proof. □

The function g mentioned in the above proposition will be called the *inverse* of the function f, and will be denoted by f^{-1}.

COROLLARY 2.8. *The set of all functions $f \in \mathcal{A}(\mathcal{G})$ with $f(\{e\}) \neq 0$ forms an Abelian group under the operation given by convolution.*

PROOF: Let $f, g \in \mathcal{A}(\mathcal{G})$ with $f(\{e\}) \neq 0$. Then $g(\{e\}) \neq 0$ if and only if $(f * g)(\{e\}) = f(\{e\})g(\{e\}) \neq 0$. Hence, in view of Proposition 2.2, the corollary follows. □

Returning back to multipliplicative functions in $\mathcal{A}(\mathcal{G})$ we have

PROPOSITION 2.9. *If $f, g \in \mathcal{A}(\mathcal{G})$ are such that $f \circ \rho$ and $(f * g) \circ \rho$ are multiplicative then $g \circ \rho$ is also multiplicative.*

PROOF: Let $G_1, G_2 \in \mathcal{G}$ be any two coprime groups. We shall use induction on the direct factors of $\rho(G_1)$ and $\rho(G_2)$ to prove that $(g \circ \rho)(G_1 \times G_2) = (g \circ \rho)(G_1)(g \circ \rho)(G_2)$

If $G_1 = G_2 = \{e\}$ then

$$1 = \big((f * g) \circ \rho\big)\big(\{e\}\big) = (f \circ \rho)\big(\{e\}\big)(g \circ \rho)\big(\{e\}\big),$$

and so, as the induction hypothesis, we assume that for each direct factor K_1 of $\rho(G_1) = \Pi(G_1)$ and for each direct factor K_2 of $\rho(G_2) = \Pi(G_2)$ with $K_1 \times K_2 \neq \rho(G_1) \times \rho(G_2)$ we have

$$(g \circ \rho)(K_1 \times K_2) = (g \circ \rho)(K_1)(g \circ \rho)(K_2)$$

that is, $g(K_1 \times K_2) = g(K_1)g(K_2)$. Then, since $(f * g) \circ \rho$ is multiplicative, we have

$$\big((f * g) \circ \rho\big)(G_1 \times G_2) = \big((f * g) \circ \rho\big)(G_1)\big((f * g) \circ \rho\big)(G_2)$$

or
$$\sum f(H)g(K) = \Big(\sum f(H_1)g(K_1)\Big)\Big(\sum f(H_2)g(K_2)\Big)$$

or
$$\sum f(H_1 \times H_2)g(K_1 \times K_2) = \sum f(H_1 \times H_2)g(K_1)g(K_2),$$

where the summations are over all ordered pairs (H, K), (H_1, K_1), $(H_2, K_2) \in \mathcal{G} \times \mathcal{G}$ such that $H \times K = \rho(G_1) \times \rho(G_2)$, $H_1 \times K_1 = \rho(G_1)$, and $H_2 \times K_2 = \rho(G_2)$. Therefore, using the induction hypothesis and the fact that $(f \circ \rho)\big(\{e\}\big) = 1$, we have

$$g\big(\rho(G_1) \times \rho(G_2)\big) = g\big(\rho(G_1)\big)g\big(\rho(G_2)\big).$$

This completes the proof. □

COROLLARY 2.10. *The set of all multiplicative functions in $\mathcal{A}(\mathcal{G})$ of the form $f \circ \rho$, where $f \in \mathcal{A}(\mathcal{G})$, is an Abelian group under the operation given by convolution.*

PROOF: It is easy to see that the set under consideration is same as the set of all functions in $\mathcal{A}(\mathcal{G})$ of the form $f \circ \rho$, where $f \in \mathcal{A}(\mathcal{G})$ is a multiplicative function; noting that $f \circ \rho = (f \circ \rho) \circ \rho$. We shall in fact show that this set is a subgroup of the Abelian group considered in Corollary 2.8.

Let $f, g \in \mathcal{A}(\mathcal{G})$ be any two multiplicative functions. Then, by Proposition 2.4, $(f \circ \rho) * (g \circ \rho) = (f * g) \circ \rho$ is multiplicative. Also, we have

$$(f \circ \rho) * (f^{-1} \circ \rho) = (f * f^{-1}) \circ \rho = \varepsilon \circ \rho = \varepsilon.$$

So, $(f \circ \rho)^{-1} = f^{-1} \circ \rho$, and, by the above proposition, $f^{-1} \circ \rho$ is multiplicative. Hence, the corollary follows. □

3. THE MÖBIUS FUNCTION AND THE RELATED RESULTS

The Möbius function, which is one of the most useful examples of arithmetic functions of positive integers, is given by

$$\mu(n) = \begin{cases} (-1)^{\omega(n)}, & \text{if } \omega(n) = \Omega(n) \\ 0, & \text{otherwise} \end{cases}$$

where n is a positive integer, $\omega(n)$ is the number of distinct prime factors of n, and $\Omega(n)$ is the number of prime factors (counting multiplicity) of n.

We define the group-theoretic analogues of ω, Ω and the Möbius function μ as

$\omega(G)$ = number of distinct (that is, non-isomorphic) factors in $C(G)$,

$\Omega(G)$ = number of factors (counting multiplicity) in $C(G)$, and

$$\mu(G) = \begin{cases} (-1)^{\omega(G)}, & \text{if } \omega(G) = \Omega(G) \\ 0, & \text{otherwise} \end{cases}$$

where $G \in \mathcal{G}$. Note that $\omega(\{e\}) = 0 = \Omega(\{e\})$ and so $\mu(\{e\}) = 1$.

Considering G to be $C_2 \times C_2$ and C_4, one can see that the Möbius function $\mu(G)$ defined above is not an extension of the Möbius functions defined by Delsarte and Cohen. However, taking $G = C_n$, we have

$$\omega(C_n) = \omega(n), \quad \Omega(C_n) = \Omega(n), \quad \text{and} \quad \mu(C_n) = \mu(n)$$

because $C_n = C_{p_1{}^{r_1}} \times \cdots \times C_{p_k{}^{r_k}}$, where $p_1{}^{r_1}, \ldots, p_k{}^{r_k}$ is the standard prime factorisation of n, and so $\mathcal{C}(C_n)$ consists of the simple groups C_{p_i}, each having multiplicity r_i, $1 \leqslant i \leqslant k$.

LEMMA 3.1. *$\Omega(G_1 \times G_2) = \Omega(G_1) + \Omega(G_2)$ for all $G_1, G_2 \in \mathcal{G}$, and $\omega(G_1 \times G_2) = \omega(G_1) + \omega(G_2)$ if G_1 and G_2 are coprime.*

PROOF: Given $G_1, G_2 \in \mathcal{G}$, we know that $\mathcal{C}(G_1 \times G_2)$ is the disjoint union (that is, union counting multiplicities) of $\mathcal{C}(G_1)$ and $\mathcal{C}(G_2)$. Hence the lemma follows. □

PROPOSITION 3.2. *The Möbius function $\mu \in \mathcal{A}(\mathcal{G})$ is multiplicative, and $\mu * u = u * \mu = \varepsilon$ that is, $\mu^{-1} = u$ and $u^{-1} = \mu$.*

PROOF: The first part follows from Lemma 3.1. For the second part, one notes that $\mu \circ \rho = \mu$ and $u \circ \rho = u$ where ρ is the factorisation map considered in section 2. So, by Propositions 2.4 and 2.5, $\mu * u$ is multiplicative and $(\mu * u)(G) = (\mu * u)\big(\Pi\mathcal{C}(G)\big)$ $\forall G \in \mathcal{G}$. Now, for $G \neq \{e\}$, $\Pi\mathcal{C}(G)$ is a product of powers of distinct simple groups in $\mathcal{G}$, and

$$\begin{aligned}(\mu * u)(P^k) &= \mu\big(\{e\}\big) + \mu(P) + \mu(P^2) + \cdots + \mu(P^k) \\ &= 1 - 1 + 0 + \cdots + 0 = 0\end{aligned}$$

for each simple group $P \in \mathcal{G}$, for each positive integer k. So, it follows that $(\mu * u)(G)$ $= (u * \mu)(G) = \varepsilon(G)$ $\forall G \in \mathcal{G}$. □

As an immediate consequence, we have the following analogue of the Möbius inversion formula.

PROPOSITION 3.3. *For $f, g \in \mathcal{A}(\mathcal{G})$,*

$$f = g * u \iff g = f * \mu.$$

PROOF: We have to simply 'multiply' the first equation on the right by μ to get the second, and the second equation on the right by u to get the first. □

An important example of a completely multiplicative function of positive integers is the Liouville's function given by

$$\lambda(n) = (-1)^{\Omega(n)}$$

where n is a positive integer. We define the group-theoretic analogues of λ as

$$\lambda(G) = (-1)^{\Omega(G)}$$

where $G \in \mathcal{G}$.

PROPOSITION 3.4. *The Liouville's function $\lambda \in \mathcal{A}(\mathcal{G})$ is completely multiplicative, and $\lambda * \mu^2 = \mu^2 * \lambda = \varepsilon$ that is, $\lambda^{-1} = \mu^2$ where μ^2 is the ordinary product of μ with itself. Also, for each $G \in \mathcal{G}$,*

$$(\lambda * u)(G) = (u * \lambda)(G) = \begin{cases} 1, & \text{if } \rho(G) = \rho(H \times H) \text{ for some } H \in \mathcal{G} \\ 0, & \text{otherwise.} \end{cases}$$

PROOF: The first assertion follows from Lemma 3.1. The remaining assertions are proved using an argument similar to the one that was used to prove the second part of Proposition 3.2, except that in this case we have

$$(\lambda * \mu^2)(P^k) = \lambda(P^k) + \lambda(P^{k-1}) = (-1)^k + (-1)^{k-1} = 0,$$

and

$$\begin{aligned}(\lambda * u)(P^k) &= \lambda\big(\{e\}\big) + \lambda(P) + \lambda(P^2) + \cdots + \lambda(P^k) \\ &= 1 - 1 + 1 - \cdots + (-1)^k = \begin{cases} 0, & \text{if } k \text{ is odd} \\ 1, & \text{if } k \text{ is even} \end{cases}\end{aligned}$$

for each simple group $P \in \mathcal{G}$, and for each positive integer k. Hence, it follows that if $G \in \mathcal{G}$ then $(\lambda * \mu^2)(G) = (\mu^2 * \lambda)(G) = \varepsilon(G)$, and also $(\lambda * u)(G) = 0$ or 1 depending on whether there exists or does not exist a factor in $\mathcal{C}(G)$ having odd multiplicity. □

In Proposition 2.7, we have seen, in particular, how to compute the inverse of a multiplicative function on $\mathcal{G}$. However, for completely multiplicative functions of the form $f \circ \rho$ the computation of the inverse is easy.

PROPOSITION 3.5. *Let $f \in \mathcal{A}(\mathcal{G})$ be a multiplicative function such that $f = f \circ \rho$. Then f is completely multiplicative if and only if $f * (\mu f) = (\mu f) * f = \varepsilon$ that is, $f^{-1} = \mu f$ where μf is the ordinary product of μ and f.*

PROOF: For each $G \in \mathcal{G}$, we have

$$\begin{aligned}\big(f * (\mu f)\big)(G) &= \sum f(H)\mu(K)f(K) = \sum f(H \times K)\mu(K) \\ &= f(G)(u * \mu)(G) = \varepsilon(G)\end{aligned}$$

by proposition 3.2; noting that $(f \circ \rho)(G) = f(G)$, $f\big(\{e\}\big) = 1$ and $\varepsilon(G) = 0$ for $G \neq \{e\}$.

Conversely, since f is mulptiplicative it is enough to show that $f(P^k) = f(P)^k$ for each simple group P in $\mathcal{G}$ and for each positive integer k. Now,

$$\begin{aligned}(\mu f) * f = \varepsilon &\Longrightarrow \big((\mu f) * f\big)(P^k) = 0 \\ &\Longrightarrow \mu\big(\{e\}\big) f\big(\{e\}\big) f(P^k) + \mu(P) f(P) f(P^{k-1}) = 0 \\ &\Longrightarrow f(P^k) = f(P) f(P^{k-1})\end{aligned}$$

and so, by iteration, $f(P^k) = f(P)^k$. This completes the proof. □

4. Divisor functions and their multiplicativity

Some well-known examples of divisor functions which form an integral part of arithmetic functions of positive integers are given by

$$\tau(n) = \sum_{d|n} 1, \quad \sigma(n) = \sum_{d|n} d, \quad \text{and} \quad \sigma_\alpha(n) = \sum_{d|n} d^\alpha$$

where n is a positive integer and α is any complex number.

Taking cue from [6], we define the group-theoretic anlogues of these functions as

$$\tau(G) = \sum_{N \trianglelefteq G} 1, \quad \sigma(G) = \sum_{N \trianglelefteq G} |N|, \quad \text{and} \quad \sigma_\alpha(G) = \sum_{N \trianglelefteq G} |N|^\alpha$$

where $G \in \mathcal{G}$. Thus, $\tau(G)$ is the number of normal subgroups of G, $\sigma(G)$ is the sum of the orders of normal subgroups of G, and $\sigma_\alpha(G)$ the sum of the α^{th} powers of the orders of normal subgroups of G.

Clearly, $\sigma_0(G) = \tau(G)$ and $\sigma_1(G) = \sigma(G)$. Also, in particular, if we take $G = C_n$ then $\sigma_\alpha(C_n) = \sigma_\alpha(n)$; noting that there is an one to one correspondence between the normal subgroups of C_n and the divisors of n given by $N \mapsto |N|$, where $N \trianglelefteq C_n$.

Since every proper non-trivial normal subgroup N of a finite group G satisfies $2 \leqslant |N| \leqslant |G|/2$, we have

$$2\tau(G) + |G| - 3 \leqslant \sigma(G) \leqslant 1 + \tau(G)\frac{|G|}{2}.$$

Proposition 4.1. *If $G \in \mathcal{G}$ then $\sigma(G) = \sum_{g \in G} \tau(G/N_g)$ where N_g is the smallest normal subgroup of G containing g.*

Proof: We know that, $\forall g \in G$, the normal subgroups of G/N_g are in one to one correspondence with the set $\{N : N_g \trianglelefteq N \trianglelefteq G\} = \{N : g \in N \trianglelefteq G\}$, and so $\tau(G/N_g) = |\{N : g \in N \trianglelefteq G\}|$. Therefore,

$$\begin{aligned}\sigma(G) = \sum_{N \trianglelefteq G} |N| &= \sum_{N \trianglelefteq G} \sum_{g \in N} 1 = \sum_{N \trianglelefteq G} \sum_{g \in G} \delta_{g,N}, \\ &= \sum_{g \in G} \sum_{N \trianglelefteq G} \delta_{g,N} = \sum_{g \in G} \sum_{g \in N \trianglelefteq G} 1 = \sum_{g \in G} \tau(G/N_g);\end{aligned}$$

here $\delta_{g,N} = 1$ or 0, according as $g \in N$ or $g \notin N$. □

As a corollary we have the following number theoretic identity.

Corollary 4.2. *For any positive integer n,*

$$\sigma(n) = \sum_{k=0}^{n-1} \tau\big(\gcd(n,k)\big)$$

PROOF: Putting $G = C_n$, in the above proposition, we have

$$\begin{aligned}\sigma(n) = \sigma(C_n) &= \sum_{k=0}^{n-1} \tau\Big(\frac{C_n}{\langle k\rangle}\Big), \quad \langle k\rangle \text{ is the subgroup of } C_n \text{ generated by } k \\ &= \sum_{k=0}^{n-1} \tau\Big(\frac{C_n}{C_{k'}}\Big), \quad \text{where } k' = \frac{n}{\gcd(n,k)} \\ &= \sum_{k=0}^{n-1} \tau\big(C_{\gcd(n,k)}\big) = \sum_{k=0}^{n-1} \tau\big(\gcd(n,k)\big).\end{aligned}$$

□

Given any two groups G_1 and G_2 (finite or infinite, Abelian or non-abelian), we now develop a condition which is equivalent to saying that every normal subgroup of the product $G_1 \times G_2$ is of the form $N_1 \times N_2$ with $N_i \trianglelefteq G_i$, $i = 1, 2$.

We shall say that the groups G_1 and G_2 have a *subgroup in common* if there exist non-trivial subgroups H_1 of G_1, and H_2 of G_2 such that $H_1 \cong H_2$.

THEOREM 4.3. *Let G_1 and G_2 be any two groups. Then the following conditions are equivalent:*

(1) *Every normal subgroup of the product $G_1 \times G_2$ is of the form $N_1 \times N_2$ with $N_1 \trianglelefteq G_1$ and $N_2 \trianglelefteq G_2$.*

(2) *For each $H_1 \triangleleft G_1$ and for each $H_2 \triangleleft G_2$, the centres $Z(G_1/H_1)$ and $Z(G_2/H_2)$ of the quotient groups G_1/H_1 and G_2/H_2 have no subgroup in common.*

PROOF: Suppose that G_1 and G_2 satisfy the second condition. Let $N \trianglelefteq G_1 \times G_2$. Set $H_1 = \pi_1\Big((G_1 \times \{e_2\}) \cap N\Big)$ and $H_2 = \pi_2\Big((\{e_1\} \times G_2) \cap N\Big)$ where e_i are identities of G_i and $\pi_i : G_1 \times G_2 \longrightarrow G_i$ are projections, $i = 1, 2$. Then

$$H_1 \times \{e_2\}, \{e_1\} \times H_2 \subset N \subset \pi_1(N) \times \pi_2(N)$$

and so

$$H_1 \times H_2 = \big(H_1 \times \{e_2\}\big)\big(\{e_1\} \times H_2\big) \subset \pi_1(N) \times \pi_2(N) \tag{4.4}$$

It may be noted here that $H_i \trianglelefteq G_i$ and $H_i \trianglelefteq \pi_i(N)$, $i = 1, 2$. Now, suppose $a_1 \in \pi_1(N)$. Then $(a_1, a_2) \in N$ for some $a_2 \in G_2$; in fact $a_2 \in \pi_2(N)$. Therefore, $\forall g_1 \in G_1$, we have

$$\begin{aligned}(g_1 a_1 {g_1}^{-1}, a_2) &= (g_1, e_2)(a_1, a_2)({g_1}^{-1}, e_2) \in N \\ &\Longrightarrow (g_1 a_1 {g_1}^{-1} {a_1}^{-1}, e_2) \in N \\ &\Longrightarrow g_1 a_1 {g_1}^{-1} {a_1}^{-1} \in H_1 \\ &\Longrightarrow g_1 H_1 a_1 H_1 = a_1 H_1 g_1 H_1 \in G_1.\end{aligned}$$

Thus, $a_1H_1 \in Z(G_1/H_1)$. So, we have $\pi_1(N)/H_1 \subset Z(G_1/H_1)$. Similarly, $\pi_2(N)/H_2 \subset Z(G_2/H_2)$. Note that if $a_1, b_1 \in \pi_1(N)$ then $(a_1, a_2), (b_1, b_2) \in N$ for some $a_2, b_2 \in \pi_2(N)$, and so $(a_1{b_1}^{-1}, a_2{b_2}^{-1})$, $(a_1b_1, a_2b_2) \in N$. Therefore,

$$a_1H_1 = b_1H_1 \Longleftrightarrow a_1{b_1}^{-1} \in H_1 \Longleftrightarrow (a_1{b_1}^{-1}, e_2) \in N$$
$$\Longleftrightarrow (e_1, a_2{b_2}^{-1}) \in N \Longleftrightarrow a_2{b_2}^{-1} \in H_2 \Longleftrightarrow a_2H_2 = b_2H_2.$$

This means that we have a well-defined injective map $f : \pi_1(N)/H_1 \longrightarrow \pi_2(N)/H_2$ given by $f(a_1H_1) = a_2H_2$ where $(a_1, a_2) \in N$. Also,

$$f(a_1H_1b_1H_1) = f(a_1b_1H_1) = a_2b_2H_2 = a_2H_2b_2H_2 = f(a_1H_1)f(b_1H_1),$$

showing that f is a homomorphism. Finally, if $b \in \pi_2(N)$ then $(a, b) \in N$ for some $a \in \pi_1(N)$ and so $f(aH_1) = bH_2$, which implies that f is surjective. Thus f is an isomorphism. Hence it follows from the hypothesis that $\pi_i(N)/H_i$ are trivial subgroups of $Z(G_i/H_i)$, $i = 1, 2$. Therefore, $H_i = \pi_i(N)$, $i = 1, 2$, and so $N = H_1 \times H_2$, by ((4.4)).

Conversely, suppose G_1 and G_2 do not satisfy the second condition. So, there exist $H_i \lhd G_i$, $i = 1, 2$, such that $Z(G_1/H_1)$ and $Z(G_2/H_2)$ have a subgroup in common. Let K_i/H_i be non-trivial subgroups of $Z(G_i/H_i)$, $i = 1, 2$, such that there is an isomorphism $F : K_1/H_1 \longrightarrow K_2/H_2$. Put

$$N = \{(a_1, a_2) \in K_1 \times K_2 : F(a_1H_1) = a_2H_2\}.$$

Let $(a_1, a_2), (b_1, b_2) \in N$ then $F(a_1H_1) = a_2H_2$ and $F(b_1H_1) = b_2H_2$. So, $F(a_1{b_1}^{-1}H_1) = a_2{b_2}^{-1}H_2$. Thus

$$(a_1, a_2)(b_1, b_2)^{-1} = (a_1{b_1}^{-1}, a_2{b_2}^{-1}) \in N,$$

showing that N is a subgroup of $G_1 \times G_2$. Again let $(a_1, a_2) \in N$ and $(g_1, g_2) \in G_1 \times G_2$. Then,

$$(g_1, g_2)(a_1, a_2)(g_1, g_2)^{-1} = (g_1a_1{g_1}^{-1},\ g_2a_2{g_2}^{-1}) \in K_1 \times K_2,$$

since $K_i \trianglelefteq G_i$, $i = 1, 2$. Also, since

$$a_iH_i \in K_i/H_i \subset Z(G_i/H_i),\ i = 1, 2,$$

we have

$$F(g_1a_1{g_1}^{-1}H_1) = F(a_1H_1) = a_2H_2 = g_2a_2{g_2}^{-1}H_2.$$

Thus $(g_1, g_2)(a_1, a_2)(g_1, g_2)^{-1} \in N$, and so $N \trianglelefteq G_1 \times G_2$. On the other hand, suppose N is of standard form $N_1 \times N_2$ where $N_i \trianglelefteq G_i$, $i = 1, 2$. Then, $\pi_i(N) = N_i$, $i = 1, 2$. But since F is bijective, we have $\pi_i(N) = K_i$, $i = 1, 2$. Therefore, $N = K_1 \times K_2$. Since K_1/H_1 is non-trivial, there is some $a_1 \in K_1$ such that $a_1H_1 \neq H_1$. But $(a_1, e_2) \in K_1 \times K_2 = N$. So, $F(a_1H_1) = e_2H_2 = H_2$, the zero element of K_2/H_2. Therefore, since F is injective, we have $a_1H_1 = H_1$, the zero element of K_1/H_1. This contradiction shows that N is not of the form mentioned in the first condition. □

The following corollary generalises [**6**, Proposition 3.3].

COROLLARY 4.4. *If $G_1, G_2 \in \mathcal{G}$ are almost coprime then every normal subgroup of the product $G_1 \times G_2$ is of the form $N_1 \times N_2$ with $N_1 \trianglelefteq G_1$ and $N_2 \trianglelefteq G_2$.*

PROOF: Let $H_1 \lhd G_1$ and $H_2 \lhd G_2$ be such that the centres $Z(G_1/H_1)$ and $Z(G_2/H_2)$ have a subgroup in common. So, there are non-trivial subgroups K_i/H_i of $Z(G_i/H_i)$, $i = 1, 2$, such that $K_1/H_1 \cong K_2/H_2$. Then $\mathcal{C}(K_1/H_1) = \mathcal{C}(K_2/H_2)$. Since $H_i \lhd K_i \trianglelefteq G_i$, we have $\mathcal{C}(K_i/H_i) \subseteq \mathcal{C}(K_i) \subseteq \mathcal{C}(G_i)$, $i = 1, 2$. Thus, $\mathcal{C}(G_1)$ and $\mathcal{C}(G_2)$ have an Abelian member in common. □

By considering $G_1 = S_4$, $G_2 = C_3$, and noting that the symmetric group S_4 and the quotient $S_4/V \cong S_3$ have trivial centres, one can easily see that the converse of the above corollary is not true; V is the normal subgroup $\{e, (12)(34), (13)(24), (14)(23)\}$ of S_4. However, as an immediate consequence of the above corollary we have

PROPOSITION 4.5. *If $f \in \mathcal{A}(\mathcal{G})$ is multiplicative (or, almost completely multiplicative) then the function $F \in \mathcal{A}(\mathcal{G})$ given by*

$$F(G) = \sum_{N \trianglelefteq G} f(N)$$

is also multiplicative (or, almost completely multiplicative).

PROOF: Let $G_1, G_2 \in \mathcal{G}$ be a pair of coprime (or, almost coprime) groups. Clearly, if $N_1 \trianglelefteq G_1$ and $N_2 \trianglelefteq G_2$ then N_1 and N_2 are also coprime (or, almost coprime). So, we have

$$\begin{aligned} F(G_1 \times G_2) &= \sum_{N \trianglelefteq (G_1 \times G_2)} f(N) = \sum_{N_1 \trianglelefteq G_1, N_2 \trianglelefteq G_2} f(N_1 \times N_2) \\ &= \sum_{N_1 \trianglelefteq G_1} \sum_{N_2 \trianglelefteq G_2} f(N_1) f(N_2) = F(G_1) F(G_2). \end{aligned}$$

□

COROLLARY 4.6. *σ_α is almost completely multiplicative.*

PROOF: It is enough to note that $G \mapsto |G|^\alpha$, for $G \in \mathcal{G}$, defines a completely multiplicative function in $\mathcal{A}(\mathcal{G})$. □

5. CHARACTERISATION OF GROUPS USING DIVISOR FUNCTIONS

Most trivial characterisation of groups using divisor functions is perhaps the following:

$$\sigma_\alpha(G) = |G|^\alpha + 1 \iff G \text{ is a simple group}$$

where $G \in \mathcal{G}$, and α is a complex number. Also, we know that any finite Abelian group G has a (normal) subgroup of order d for every divisor d of $|G|$, and G has exactly one such subgroup for every divisor d if and only if G is cyclic. Therefore, for any Abelian group $G \in \mathcal{G}$, we have $\sigma_\alpha(G) \geqslant \sigma_\alpha(|G|)$, and the equality holds if and only if G is cyclic.

LEMMA 5.1. *Let $G \in \mathcal{G}$ be such that $G = \bigcup_{N \lhd G} N$. Then $\tau(G) \geqslant 5$.*

PROOF: Since $|N| \leqslant |G|/2 \quad \forall N \lhd G$, and since the identity element of G is a common member of all normal subgroups of G, it follows that any two proper normal subgroups of G can contain at the most $|G| - 1$ distinct elements. Hence G must have atleast three proper nontrivial normal subgroups, which in turn implies that $\tau(G) \geqslant 5$. □

PROPOSITION 5.2. *Let $G \in \mathcal{G}$. If $\sigma(G) \leqslant 2|G| + 2$ then $G \neq \bigcup_{N \lhd G} N$.*

PROOF: Let us assume that $G = \bigcup_{N \lhd G} N$. Then, for each $g \in G$, the smallest normal subgroup N_g of G containing g is a proper normal subgroup of G, and so $G/N_g \neq \{e\}$ which means $\tau(G/N_g) \geqslant 2$. Therefore, by Proposition 4.1, we have

$$\begin{aligned}\sigma(G) &= \sum_{g \in G} \tau(G/N_g) = \tau(G) + \sum_{g \in G, g \neq e} \tau(G/N_g) \\ &\geqslant \tau(G) + 2\big(|G| - 1\big).\end{aligned}$$

Since $\sigma(G) \leqslant 2|G| + 2$, it follows that $\tau(G) \leqslant 4$ which contrdicts the Lemma 5.1. Hence the proposition follows. □

From [2, Theorem 1], we know that if $G \in \mathcal{G}$ is such that $G \neq \bigcup_{N \lhd G} N$ then every Abelian quotient of G (that is, every quotient of G which is Abelian) is cyclic. Hence, we have the following corollary to the above proposition, which is also an improvement to the 'Abelian Quotient Theorem' proved in [6]:

COROLLARY 5.3. *If G is a finite group with $\sigma(G) \leqslant 2|G| + 2$ then every Abelian quotient of G is cyclic.*

REMARK 5.4. If $q : G \longrightarrow G'$ is a homomorphism of groups $G, G' \in \mathcal{G}$ then $\tau\big(q(G)\big) \leqslant \tau(G)$, since $q^{-1}(M) \trianglelefteq G \; \forall \; M \trianglelefteq q(G)$. In particular, we have $\tau(G/N) \leqslant \tau(G) \quad \forall \; G \in \mathcal{G}$ and $\forall \; N \trianglelefteq G$; moreover, the inequality is strict if N is nontrivial.

PROPOSITION 5.5. *Let $G \in \mathcal{G}$ be such that $\tau(G) = 5$ and $G = \bigcup_{N \lhd G} N$. Then $G = C_2 \times C_2$.*

PROOF: By ([2, Theorem 1]), there is a normal subgroup of G such that $G/N = C_p \times C_p$ for some prime p. So,

$$\begin{aligned}\tau(G/N) = \tau(C_p \times C_p) = p + 3 &\Longrightarrow \tau(G) \geqslant p + 3, \text{ since } \tau(G) \geqslant \tau(G/N), \\ &\Longrightarrow p = 2 \Longrightarrow N = \{e\},\end{aligned}$$

otherwise $5 = \tau(G) > \tau(G/N) = p + 3 = 5$ which is absurd. Hence the proposition follows. □

The Proposition 5.5 tells us that if $G \neq C_2 \times C_2$ then the hypothesis of the Corollary 5.3 can be further improved to $\sigma(G) \leqslant 2|G| + 3$.

In [6], Leinster has studied the groups $G \in \mathcal{G}$ which satisfy the condition $\sigma(G) = 2|G|$, and he termed such groups as 'perfect groups' (not to be confused with the ones which are more standard and mean something else). He proved that an Abelian group $G \in \mathcal{G}$ is perfect if and only if $G = C_n$ where n is a perfect number that is, $\sigma(n) = 2n$, and he conjectured that there are infinitely many nonabelian perfect groups. However, it requires some effort to find examples of nonabelian perfect groups. Leinster has exhibited only three examples of such groups, namely,

$$S_3 \times C_5,\ A_5 \times C_{61} \times C_{31} \times C_8,\ A_6 \times C_{361} \times C_{127} \times C_8.$$

We mention below few more examples of nonabelian perfect groups:

Consider the generalised quaternion group $\mathbb{Q}_{4m}$ of order $4m$, $m \geqslant 2$, given by

$$\mathbb{Q}_{4m} = \langle a, b \mid a^{2m} = 1, b^2 = a^m, bab^{-1} = a^{-1} \rangle.$$

It can be easily proved that if m is odd then the proper normal subgroups of $\mathbb{Q}_{4m}$ are precisely the subgroups of the cyclic group generated by a. Therefore, $\sigma(\mathbb{Q}_{4m}) = 4m + \sigma(2m)$ if m is odd. Using multiplicativity of σ one can see that the nonabelian group $\mathbb{Q}_{12}$, $\mathbb{Q}_{20} \times C_{19}$, $\mathbb{Q}_{28} \times C_{13}$, $\mathbb{Q}_{244} \times A_5 \times C_{43} \times C_{11}$ and $\mathbb{Q}_{220} \times C_{109}$ are all perfect groups in the sense of Leinster.

References

[1] T.M. Apostol, *Introduction to analytic number theory*, Springer International Student Edition (Narosa Publishing House, New Delhi, 1993).

[2] M.A. Brodie, R.F. Chamberlain and L.-C. Kappe, 'Finite coverings by normal subgroups', *Proc. Amer. Math. Soc.* **104** (1988), 669–674.

[3] E. Cohen, 'Arithemetical functions of finite abelian groups', *Math. Ann.* **142** (1961), 165–182.

[4] P.S. Delsarte, 'Fonctions de Möbius sur les groupes abeliens finis', *Ann. of Math.* **49** (1948), 600–609.

[5] N. Jacobson, *Basic algebra, vol I* (W.H. Freeman and Company, U.S.A., 1974).

[6] T. Leinster, 'Perfect number and groups', `arXiv:math.GR/0104012 v1 Apr 2001`.

[7] M.S. Lucido and M.R. Pournaki, 'Elements with square roots in finite groups', *Algebra Colloq.* **12** (2005), 677–690.

[8] A. Mann, 'Finite groups containing many involutions', *Proc. Amer. Math. Soc.* **122** (1994), 383–326.

[9] Y. Marefat, 'Conjugacy structure type and degree structure type in finite p-groups', *Turkish J. Math.* **24** (2000), 321–326.

[10] F. Menegazzo, 'The number of generators of a finite group', *Irish Math. Soc. Bull.* **50** (2003), 117–128.

Department of Mathematics
North Eastern Hill University
Permanent Campus
Shillong-793022, Meghalaya
India
e-mail: akdas@nehu.ac.in