PACIFIC JOURNAL OF MATHEMATICS
Vol. 44, No. 1, 1973

GROUPS OF ARITHMETIC FUNCTIONS UNDER DIRICHLET CONVOLUTION

ROY W. RYDEN

If f is an arithmetic function, let $T(f) = \{(a, b) \mid f(ab) = f(a)f(b)\}$. If S is a set of pairs of positive integers, let $f \in M(S)$ if $T(f) \supseteq S$. In this paper we determine all sets S such that $M(S)$ is a group under Dirichlet convolution.

1. Introduction. An *arithmetic function* f is a complex-valued function whose domain is the set $N = \{1, 2, 3, \cdots\}$. The *multiplicative set* belonging to f is the set $T(f) = \{(a, b) \mid f(ab) = f(a)f(b)\}$. If S is any nonempty subset of $N \times N$, then we say that $f \in M(S)$ if $f \neq 0$ and $T(f) \supseteqq S$. We shall let $\mathscr{R}$ denote the set $\{(a, b) \mid GCD(a, b) = 1\}$. Furthermore, for convenience we shall assume that all of our sets $S \subseteqq N \times N$ are *symmetric* $\cdots$ $(a, b) \in S$ if and only if $(b, a) \in S$.

It is well-known (see [1]) that $M(\mathscr{R})$, the set of all *multiplicative* functions, forms an Abelian group under the *Dirichlet convolution*

$$[f^*g]\,(n) = \sum_{d \mid n} f(d)g(n/d)\ .$$

In this paper we intend to characterize completely all those sets S such that $M(S)$ is a group under*. It is not hard to show that all of our results carry through for the generalized convolution defined by Goldsmith [2]. We shall work with* for simplicity.

Some of the contents of this paper appeared in the author's Ph.D. thesis written at the University of Oregon under the direction of Professor Ivan Niven.

2. The multiplicative closure of a set. It is convenient for us to introduce a closure operation on subsets of $N \times N$. Properties of this operation which are not necessary for this paper will be discussed by the author elsewhere.

If $S \subseteqq N \times N$, then the transformation

$$(a_1, a_2, \cdots, a_n) \longleftrightarrow (b_1, b_2, \cdots, b_n, b_{n+1})$$

is said to be an *S-step* if

(i) $\qquad a_j = b_j \qquad$ for $j = 1, 2, \cdots, n-1$

(ii) $\qquad a_n = b_n b_{n+1}$

and

(iii) $\qquad (b_n, b_{n+1}) \in S\ ,$

where all n-tuples for $n \geqq 3$ are to be considered as *unordered*. It should be emphasized that an S-step is a transformation which can go either from $(a_1, a_2, \cdots, a_n)$ to $(b_1, b_2, \cdots, b_n, b_{n+1})$, or from $(b_1, b_2, \cdots, b_n, b_{n+1})$ to $(a_1, a_2, \cdots, a_n)$. An *S-chain* is any sequence of S-steps. We say that a pair (a, b) is in S^*, the *multiplicative closure* of S, if there exists a finite S-chain leading from the 1-tuple (ab) to the pair (a, b). A set S is *closed* if $S = S^*$.

THEOREM 2.1. (i) *$S \subseteqq S^*$, and $A \subseteqq B$ implies $A^* \subseteqq B^*$;*
(ii) *$S^{**} = S^*$;*
(iii) *$T(f)$ is closed for all functions f.*

Proof. (i) Notice that $(a_1a_2) \to (a_1, a_2)$ *is an* S-chain if $(a, b) \in S$. To see that (ii) holds, let $(a_1, \cdots, a_n) \leftrightarrow (b_1, \cdots, b_n, b_{n+1})$ be an S^*-step where $a_i = b_i$ for $i = 1, 2, \cdots, n-1$, $b_nb_{n+1} = a_n$ and $(b_n, b_{n+1}) \in S^*$. Then there exists a finite S-chain:

$$(b_nb_{n+1}) \longrightarrow (c_1, c_2) \longrightarrow \cdots \longrightarrow (d_1, d_2, d_3) \longrightarrow (b_n, b_{n+1}) \ .$$

Notice that the following is a finite S-chain:

$$\begin{aligned}(a_1, \cdots, a_n) &\longrightarrow (a_1, \cdots, a_{n-1}, c_1, c_2)\\ &= (b_1, b_2, \cdots, b_{n-1}, c_1, c_2)\\ &\longrightarrow \cdots\\ &\longrightarrow (b_1, \cdots, b_{n-1}, d_1, d_2, d_3)\\ &\longrightarrow (b_1, \cdots, b_{n-1}, b_n, b_{n+1}) \ .\end{aligned}$$

Hence any finite S^*-chain can be represented as a finite S-chain and (ii) follows.

To prove (iii), if $(nm) \to (n_1, n_2) \to \cdots \to (b_1, b_2, m) \to (n, m)$ is a $T(f)$-chain, then

$$\begin{aligned}f(nm) &= f(n_1)f(n_2)\\ &= \cdots\\ &= f(b_1)f(b_2)f(m)\\ &= f(n)f(m) \ ,\end{aligned}$$

so that $(n, m) \in T(f)^*$ implies that $(n, m) \in T(f)$.

If φ is Euler's totient function, then it is not hard to see that $T(\varphi) = \mathscr{R}$. Hence we can conclude from 2.1 that the set $\mathscr{R}$ is closed.

A set S is *divisible* if $(a, b) \in S$ implies that $(d, d') \in S$ whenever $d \mid a$ and $d' \mid b$. Notice that $\mathscr{R}$ is a divisible set.

THEOREM 2.2. *If S is a divisible subset of $\mathscr{R}$, then S^* is also* *a divisible subset of* $\mathscr{R}$.

Proof. The fact that $S^* \subseteqq \mathscr{R}$ is immediate because $\mathscr{R}$ is closed. If $(a, b) \in S^*$ and $p^\alpha \| a$ and $q^\beta \| b$ where p and q are primes, then $(p^\alpha, q^\beta) \in S$. If not, then $(p^\alpha x, q^\beta y) \notin S$ by the divisibility of S so that if $(ab) \to (u, v) \to \cdots \to (a, b)$ is an S-chain then one and only one "co-ordinate" of each-tuple involved must be divisible by $p^\alpha q^\beta$. But this is a contradiction because $p^\alpha | a$ and $q^\beta | b$. Therefore $(p^i, q^j) \in S$ for all $i \leqq \alpha, j \leqq \beta$, by the divisibility of S.

Assume that $d | a$, $d' | b$, and $(\delta, \delta') \in S^*$ for all $\delta | d$, $\delta' | d'$, and $(\delta, \delta') \neq (d, d')$. Since $(a, b) \in S^*$ let $(ab) \to (u, v)$ be a first S-step where $(u, v) \in S$, $u = d_1 d_1' d_1''$, $v = d_2 d_2' d_2''$, $d_1 d_2 = d$, and $d_1' d_2' = d'$. By the divisibility of S we have $(d_1 d_1', d_2 d_2') \in S$, $(d_1, d_2) \in S$, and $(d_1', d_2') \in S$. By the choice of (d, d') we have (d_1, d_1') and $(d_2, d_2') \in S^*$. Hence the following S-chain obtains:

$$\begin{aligned}(dd') = (d_1 d_1' d_2 d_2') &\longrightarrow (d_1 d_1', d_2 d_2')\\ &\longrightarrow (d_1, d_1', d_2 d_2')\\ &\longrightarrow (d_1, d_1', d_2, d_2')\\ &\longrightarrow (d_1 d_2, d_2 d_2')\\ &\longrightarrow (d, d')\end{aligned}$$

so that $(d, d') \in S^*$.

3. The main results. A set S is said to have *property* P if $f * g \in M(S)$ whenever f and g are in $M(S)$. The main theorem of this paper is the following characterization.

THEOREM 3.1. *A set S has property P if, and only if S^* is a divisible subset of $\mathscr{R}$. In particular, all divisible subsets of $\mathscr{R}$ have property P.*

The proof of Theorem 3.1 will follow from a sequence of lemmas. A set S has property P' if $f * 1 \in M(S)$ whenever $f \in M(S)$ where 1 is the function with constant value 1.

LEMMA 3.2. *If S has property P, then S has property P'.*

LEMMA 3.3. *If S has property P', then $S \subseteqq \mathscr{R}$.*

Proof. $1 * 1$ is the number of divisors function τ, and it is easy to see that $T(\tau) = \mathscr{R}$. Therefore $\tau \in M(S)$ implies $\mathscr{R} = T(\tau) \supseteqq S$.

LEMMA 3.4. *If S has property P', then $(1, 1) \in S$.*

Proof. If $(1, 1) \notin S$, define $f(1) = 2$, $f(n) = 0$ for all $n > 1$. Then $f \in M(S)$ but $f^*1 \notin M(S)$.

LEMMA 3.5. *Let S be closed and have property P'. If $(a, b) \in S$, then $(1, d) \in S$ for all $d \mid a$ and $(1, d') \in S$ for all $d' \mid b$.*

Proof. Assume $(1, d) \notin S$ for $d \mid a$ and d is the smallest divisor of a with this property. We may assume that $(\delta, \delta') \notin S$ where $\delta\delta' = d$ and $\delta \neq 1 \neq \delta'$, because, by the minimality of d, the following S-chain obtains:

$$(d) \longrightarrow (\delta, \delta') \longrightarrow (1, \delta, \delta') \longrightarrow (1, d) \ .$$

Since S is closed, $(1, d) \in S$.

Define f via $f(1) = 0$, $f(d) = 1$, $f(x) = 0$ otherwise. It is easy to see that $f \in M(S)$ by the previous remarks, but

$$[f^*1](ab) \neq [f^*1](a) \cdot [f^*1](b) \ ,$$

a contradiction.

Let k be fixed and let g be defined via $g(1) = 1$, $g(k) = 1$, and $g(m) = 0$ otherwise. It is easy to check that $T(g)$ contains all coprime pairs except those of the form $(d, k/d)$ where $d \neq 1$ or k.

LEMMA 3.6. *If S is closed and has property P', then S must be divisible.*

Proof. Suppose that the set

$$\{(a, b) \in S \mid (d, d') \notin S \text{ for some } d \mid a,\ d' \mid b,\ d \neq 1 \neq d'\}$$

is nonempty, and let (a, b) be an element of this set which is minimal with respect to the product $ab = n$. Also pick an appropriate (d, d') to be minimal with respect to its product $dd' = k$.

(1) If $\delta \mid d$ and $\delta' \mid d'$ and $\delta\delta' < dd'$, then $\delta \mid a$, $\delta' \mid b$, and so $(\delta, \delta') \in S$.

(2) If $(d_1, d_1') \in S$ where $d_1d_1' = k$, $d_1 \neq 1 \neq d_1'$, then $(\delta, \delta') \in S$ for all $\delta \mid d_1$ and $\delta' \mid d_1'$ by the minimality of $ab = n$.

We may assume, however, that $(d_1, d_1^1) \notin S$ whenever

$$d_1d_1' = k, d_1 \neq 1 \neq d_1' \ .$$

For if $(d_1, d_1') \in S$, let $d_1 = d_2d_2'$ and $d_1' = d_3d_3'$ where $d_2d_3 = d$ and $d_2'd_3' = d'$. Then the following chain obtains:

$$\begin{aligned}(dd') &\longrightarrow (d_1, d_1') \longrightarrow (d_2, d_2', d_1') \longrightarrow (d_2, d_2', d_3, d_3') \\ &\longrightarrow (d_2d_3, d_2'd_3') = (d, d') \ .\end{aligned}$$

Since S is a closed set, it follows from this that $(d, d') \in S$, which is contrary to our assumption.

It follows that $g \in M(S)$ where g is the function defined above. It is not hard to see that $[g^*1](ab) \geqq 2$ but $[g^*1](a) = 1 = [g^*1](b)$, a contradiction.

THEOREM 3.7. *Let S be a closed set. Then the following statements are equivalent.*

(i) *S has property P,*

(ii) *S has property P',*

and

(iii) *$S \subseteqq \mathscr{R}$ and S is divisible.*

Proof. We have shown $(1) \Rightarrow (2) \Rightarrow (3)$. Let $f, g \in M(S)$ and $(a, b) \in S$. Then

$$\begin{aligned}[f^*g](ab) &= \sum_{d|a, d'|b} f(dd')g(a/d\, b/d') \\ &= \sum_{d|a, d'|b} f(d)f(d')g(a/d)g(b/d') \\ &= \sum_{d|a} f(d)g(a/d) \sum_{d'|b} f(d')g(b/d') \\ &= [f^*g](a) \cdot [f^*g](b) .\end{aligned}$$

Proof of Theorem 3.1. If $f \in M(S)$, then $f \in M(S^*)$. Hence, if S has property P, then S^* has property P. Therefore S has property P if and only if S^* is a divisible subset of $\mathscr{R}$. In particular all divisible subsets of $\mathscr{R}$ have property P. It should be noted, however, that there exist examples of sets $S \subseteqq \mathscr{R}$ which are *not* divisible but whose closures are divisible.

The function E which has value 1 at 1 and 0 elsewhere is the identity under Dirichlet convolution. Therefore it is easy to see that a function f has an inverse $\hat{f}$ if and only if $\hat{f}(1) \neq 0$, in which case, $\hat{f}(1) = 1/f(1)$, and $\hat{f}(n) = (-1/f(1))(\sum_{d|n, d \neq n} \hat{f}(d)f(n/d))$.

THEOREM 3.8. *Let $S \subseteqq N \times N$. Then $M(S)$ is a group if and only if $S \subseteqq \mathscr{R}$, $\{(1, n)\}_{n=1}^{\infty} \subseteqq S$, and S^* is a divisible set.*

Proof. All that remains to show is that given $S \subseteqq \mathscr{R}$, $\{(1, n)\}_{n=1}^{\infty} \subseteqq S$, and S^* divisible, then $f \in M(S)$ implies that $\hat{f} \in M(S)$. First, $f(1) = 1$ so that $\hat{f}$ exists and $\hat{f}(n) = \hat{f}(1)\hat{f}(n)$. Let $(a, b) \in S$ and assume that $(d, d') \in T(\hat{f})$ for all $d \mid a$, $d' \mid b$ and $dd' < ab$. Then

$$
\begin{aligned}
-\hat{f}(ab) &= \sum_{\substack{d|a,d'|b \\ dd' \neq ab}} \hat{f}(dd')f(ab/dd') \\
&= \sum \hat{f}(d)\hat{f}(d')f(a/d)f(b/d') \\
&= \sum_{d|a,d\neq a} \hat{f}(d)f(a/d) \cdot \sum_{d'|b,d'\neq b} \hat{f}(d')f(b/d') \\
&\quad + \sum_{d|a,d\neq a} \hat{f}(d)f(a/d)\hat{f}(b) + \sum_{d'|b,d'\neq b} \hat{f}(d')f(b/d')\hat{f}(a) \\
&= (-\hat{f}(a)\hat{f}(b)) + \hat{f}(b)(-\hat{f}(a)) + \hat{f}(a)(-\hat{f}(b)) \\
&= -\hat{f}(a)\hat{f}(b)\,.
\end{aligned}
$$

This completes the proof.

REFERENCES

1. E. D. Cashwell and E. J. Everett, *The ring of number-theoretic functions*, Pacific J. Math., **9** (1959), 975-985.

2. D. L. Goldsmith, *A generalized convolution for arithmetic functions*, Duke Math. J., **38**, (1971), 279-283.

Received September 1971. Research supported in part by the National Science Foundation under grant GP-12015.

CALIFORNIA STATE UNIVERSITY, HUMBOLDT