ROCKY MOUNTAIN
JOURNAL OF MATHEMATICS
Volume 29, Number 3, Fall 1999

A SUBGROUP OF THE GROUP OF UNITS IN THE RING OF ARITHMETIC FUNCTIONS

TRUEMAN MacHENRY

In memory of Toni Dehn

0. Introduction. Å is the ring of arithmetic functions with convolution as multiplication. It is well known that Å is a unique factorization domain [**3**]. Its ideal structure has been studied by Shapiro [**5**]. The group of units, particularly the subgroup of multiplicative functions, has been investigated by many people over the years. The multiplicative functions can be characterized as those arithmetic functions which are completely determined by their values at prime powers. Among them are the *completely* multiplicative functions, namely, those that are characterized by their values at the primes. The subgroup of the group of multiplicative functions generated by the completely multiplicative functions, the (group of) *rational functions*, was studied in a paper of Carroll and Gioia [**2**]. The name *rational functions* is due to Vaidyanathaswamy [**6**, pp. 611–612]. It is this subgroup, denoted here by $M^{\blacksquare}$, that we are concerned with.

Among other results, we show that $M^{\blacksquare}$ is a free (abelian) group; in particular, it is torsion-free and each element has a unique representation in terms of a generating set consisting of completely multiplicative functions. The group $M^{\blacksquare}$ is especially rich in subgroups. Our general approach is to look for "interesting" subgroups, that is, we shall use the subgroup structure as a useful means of classifying the arithmetic functions in this group.

Let

$$M_k = \{\gamma \in M^{\blacksquare}; \gamma = \alpha * \cdots * \alpha, k \text{ times}, \alpha \in M_1\}$$

and

$$M_k^{\sim} = \{\gamma^{-1} \in M^{\blacksquare}; \gamma \in M_k\},$$

where M_1 is the set of completely multiplicative functions. Then every element of $M^{\blacksquare}$ can be written as a (convolution) product $\gamma_* * \gamma_j^{-1}$,

Received by the editors on June 16, 1997, and in revised form on October 15, 1997.

1. The group $M^{\blacksquare}$.

Theorem 1.1 [**2**, Theorem 2.2]. *$\gamma \in M_k$ implies that $\gamma^{-1}(p^n) = 0$ for $n > k$.*

Theorem 1.2. *$\gamma \in M_k$ and $\gamma \not\simeq \delta$ implies that $\gamma^{-1} \notin M_n$ for any $n \in \mathbf{N}$.*

Proof. Suppose not. Let k be the least integer for which the result is false. Let $\gamma = \beta * \chi$, $\beta, \chi \in M^{\blacksquare}$. We have from Theorem 1.1 that $\gamma^{-1}(p^t) = 0$ for $t > k$ and $\gamma(p^t) = 0$ for $t > n$. We can suppose that $\beta \in M_1$ and that $\chi \in M_{k-1}$, so that $\chi = \gamma * \beta^{-1}$. Now $\chi(p^r) = \gamma(p^r) + \gamma(p^{r-1})\beta^{-1}(p)$, $\gamma(p^{r-j}) = 0$, $r - j \geq n+1$ and $\beta^{-1}(p^j) = 0$, $j \geq 2$. Thus $\gamma(p^{r-j})\beta(p^j) = 0$ if $j \geq 2$ or if $j \leq r - n - 1$. So if $r = n+3$, $\chi(p^r) = 0$. Thus $\chi^{-1} \in M_{n+2}$. $\beta(p^r) = \gamma * \chi^{-1}(p^r) = \sum \gamma(p^{r-j})\chi^{-1}(p^j)$. $\chi^{-1}(p^j) = 0$, $j \geq k$. Also $\gamma(p^{r-j}) = 0$ for $r-j \geq n+1$, i.e., if $j \leq r-n-1$. So $r \geq k+n+1$, then $\gamma(p^{r-j}) = 0$ when $j \leq k$, and $\chi(p^j) = 0$ when $j \geq k$; thus, $\beta(p^r) = 0$ for $r \geq k+n+1$. Hence, $\beta^{-1} \in M_{k+n+1}$. But $\beta \in M_1$, so $\beta(p^r) = \beta(p)^r$ for $r \geq k+n+1$, and hence $\beta(p) = 0$. $\beta = \delta$ and $\gamma \in M_{k-1}$, the desired contradiction. The case $k = 1$ follows easily from an obvious adaptation of the argument concerning β used above. □

Theorem 1.3. *Each element of $M^{\blacksquare}$ has a unique representation in terms of generators from M_1.*

Proof. It is sufficient to prove the result for $\gamma \in M^*$ and representations of γ in M^*. Suppose $\gamma = \alpha_1 * \cdots * \alpha_r = \beta_1 * \cdots * \beta_s$, $\delta \neq \alpha_i$, $\delta \neq \beta_j$ and $\alpha_i, \beta_j \in M_1$, and suppose that $r \leq s$. Now, by Theorem 1.1, γ^{-1} is uniquely determined by its values $a_j = \gamma^{-1}(p^j)$, $j \leq r$, thus $r = s$. Moreover, the $\alpha_i(p)$ are the roots of the polynomial $x^r + a_1 x^{r-1} + \cdots + a_r$. Therefore, for some permutation π of $\{1, \ldots, r\}$, $\alpha_i = \beta_{\pi(i)}$. □

Corollary 1.3.1. *$M^{\blacksquare}$ is torsion-free.*

numbers $a_1, \ldots, a_k$, a unique $\gamma \in M_k$ is determined locally by letting $\gamma^{-1}(p^i) = a_i$. We seek now explicit expressions for the $\gamma(p^n)$ in terms of both the r_i and the a_i. Let $P_\gamma(x) = x^k + a_1 x^{k-1} + \cdots + a_k$.

Define

$$\Delta_k = \Delta(r_1, \ldots, r_k) = \begin{vmatrix} 1 & \cdots & 1 \\ r_1 & \cdots & r_k \\ \vdots & \ddots & \vdots \\ r_1^{k-1} & \cdots & r_k^{k-1} \end{vmatrix}$$

and

$$\Delta_{k,n} = \Delta_{k,n}(r_1, \ldots, r_k) = \begin{vmatrix} 1 & \cdots & 1 \\ r_1 & \cdots & r_k \\ \vdots & \ddots & \vdots \\ r_1^{k-2} & \cdots & r_k^{k-2} \\ r_1^{n+k-2} & \cdots & r_k^{n+k-2} \end{vmatrix}.$$

Theorem 2.1. *Let $P(x)$ be a monic polynomial of degree k with coefficients $a_i \in \mathbf{C}$, $i = 1, \ldots, k$, and with roots $r_1, \ldots, r_k$. Let γ be the arithmetic function in M^* determined by $P_\gamma(x)$. Then $\gamma(p^n) = \Delta_{k,n+1}/\Delta_k$, when $k > 1$, $\gamma(p^n) = r^n$, when $k = 1$.*

The theorem follows from this lemma.

Lemma 2.1.1.

$$r_j^n = -\sum_i a_i r_j^{n-i}, \quad j = 1, \ldots, k, \quad k \geq 2.$$

Proof. First assume the truth of the lemma; then the theorem follows by an easy induction. Let $\gamma(p^{m-1}) = \Delta_{k,m}/\Delta_k$ for $m < n$. Using the lemma we have $\gamma(p^n) = -(1/\Delta_k)\sum_j \Delta_{k,n-j}$. The theorem now follows using the multilinearity of the determinant function with respect to the last row, with the help of the lemma. For $k = 1$, the computation is direct. □

and

$$F_{k,n+1}(t) = t_1 F_{k,n}(t) + \cdots + t_k F_{k,n-k+1}(t),$$

where $t = (t_1, \ldots, t_k)$, $k \in \mathbf{N}$, n an integer; and $G_{k,n}(t_1, \ldots, t_k)$ by

$$G_{k,n}(t) = 0, \quad n < 0,$$
$$G_{k,0}(t) = k,$$
$$G_{k,n+1}(t) = t_1 G_{k,n}(t) + \cdots + t_k G_{k,n-k+1}(t).$$

Theorem 3.1 [**1**]. $\gamma(p^{n+1}) = F_{k,n}(a)$, $a = (a_1, \ldots, a_k)$.

The theorem follows from

Lemma 3.1.1. $\gamma(p^{n+1}) = -\sum a_j \gamma(p^{n-j+1})$.

Proof. This follows immediately from the fact that $\gamma * \gamma^{-1}(p^s) = \delta(p^s)$ is 0 when $s > 0$ and is 1 when $s = 0$, the fact that $\gamma^{-1}(p^s) = a_s$ when $s < k+1$, and the fact that $F_{k,1}(a) = 1$ (and $F_{k,0}(a) = 0$). □

Proof of the theorem. The theorem now follows from the definition by letting $t_i = -a_i$. □

Remark. With Theorems 2.1 and 3.1 we now have direct expressions for the values of γ directly in terms of both of the coefficients and the roots of the defining polynomial. Moreover, the expressions in terms of coefficients are recursive. The following theorem gives a direct expression for the G-polynomials in terms of the roots.

Theorem 3.2. $G_{k,n}(a) = r_1^n + \cdots + r_k^n$, *where* $\{r_j\}$ *is the set of roots of the polynomial* $x^k + a_1 x^{n-1} + \cdots + a_k$, $j = 1, \ldots, k$.

Proof. $G_{k,0}(a) = k$. By definition, $G_{k,n+1}(a) = \sum t_j G_{k,n-j+1}(a)$ which is equal to $\sum t_j (r_1^{n-j+1} + \cdots + r_k^{n-j+1})$ by induction. Letting $t_j = -a_j$, this becomes $-\sum a_j (r_1^{n-j+1} + \cdots + r_k^{n-j+1})$ which, in turn, equals $-\sum_i \sum_j a_j r_i^{n-j+1}$. But this is just $r_1^{n+1} + \cdots + r_k^{n+1}$ by Lemma 2.1.1. □

can generate the Pell and their companion numbers, the sequences $\{2^n - 1\}$ and $\{2^n + 1\}$ and, more generally, the Lehmer numbers and the companion Lehmer numbers. Perhaps it would be more appropriate to call these two sequences of polynomials *Lehmer polynomials* and *co-Lehmer polynomials.*

4. Locally periodic arithmetic functions in $M^{\blacksquare}$. We call $\gamma \in M^*$ *locally periodic* if $\gamma(p^{n+s}) = \gamma(p^n)$ for $n = 0, 1, \ldots,$ and for some natural number s. We would like to characterize the γ which have this property.

Recall that a γ in M^* is completely determined by its polynomial $P_\gamma(x)$, that $P_\gamma(x)P_\chi(x) = P_{\gamma*\chi}(x)$, and that $\gamma * \chi$ has a unique representation in terms of completely multiplicative functions.

Theorem 4.1. *Let $r_1, \ldots, r_k$ be the roots of $P_\gamma(x)$, $\gamma \in M_k$, γ is locally periodic only if $r_1, \ldots, r_k$ are roots of unity.*

Lemma 4.1.1. *If $\gamma \in M^*$ is locally periodic and $\gamma = \alpha * \chi$, $\alpha \in M_1$, then χ is locally periodic.*

Lemma 4.1.2. *If $\alpha \in M_1$ is locally periodic, then r is a root of unity, where $P_\alpha(x) = x - r$.*

Proof of Lemma 4.1.1. Suppose that γ has period s, and write $\chi = \gamma * \alpha^{-1}$, and let $x - r$ be the polynomial for α. Then $\chi(p^n) = \gamma(p^n) + \gamma(p^{n-1})r = \gamma(p^{n+s}) + \gamma(p^{n+s-1})r = \chi(p^{n+s})$, i.e., $\chi(p^n) = \chi(p^{n+s})$. $\square$

The proof of Lemma 4.1.2 is an immediate consequence of the definition of the F-polynomials for $k = 1$. Note that it is a consequence of Lemma 4.1.1 that the α that appears in the product decomposition of γ is locally periodic and so satisfies Lemma 4.1.2.

Theorem 4.1 now follows by induction. On the other hand, it is easily seen that $x^m - 1$ determines a locally periodic function with period m; therefore, it is a consequence of Lemma 4.1.1 that cyclotomic polynomials determine locally periodic functions as well (which we value vectors

$$\begin{array}{ll} (1,-1,0,\dots) & \text{period } 3; \\ (1,0,-1,0,\dots) & \text{period } 4; \\ (1,1,0,-1,-1,0,\dots) & \text{period } 6; \end{array}$$

and

$$\begin{array}{ll} (1,0,\dots) & \text{period } 2. \end{array}$$

REFERENCES

1. T.B. Carroll, *Severence classes and multiplicative arithmetic functions*, Ph.D. Dissertation, Western Mich. Univ., 1973.

2. T.B. Carroll and A.A. Gioia, *On a subgroup of the group of multiplicative arithmetic functions*, J. Austr. Math. Soc. **20** (1974), 348–352.

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

4. P.J. McCarthy, *Introduction to arithmetical functions*, Springer-Verlag, New York, 1985.

5. H.N. Shapiro, *On the convolution ring of arithmetic functions*, Comm. Pure Appl. Math. **1** (1972), 287–336.

6. R. Vaidyanathaswamy, *Multiplicative arithmetic functions*, Trans. Amer. Math. Soc. **33** (1931), 579–662.

York University, 4700 Keele Street, Downsview, Ontario M3J 1P3, Canada
E-mail address: MACHENRY@MATHSTAT.YORKU.CA