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.

where $\gamma_k \in M_k$ and $\gamma_j \in M_j$. We denote the convolution identity by δ, thus

$$\delta(n) = \begin{cases} 1 & n = 1; \\ 0 & \text{otherwise.} \end{cases}$$

$\delta \in M_k \cap M_j^{\sim}$. Observing that $M_k \subseteq M_{k+1}$ and $M_k^{\sim} \subseteq M_{k+1}^{\sim}$, we define

$$M^* = \cup M_k, \qquad M^{\sim *} = \cup M_k^{\sim}.$$

Then we can also write $M^{\blacksquare} = M^* * M^{\sim *}$, with the obvious interpretation of the product.

It is well known that if $\gamma \in M_k$, then $\gamma^{-1}(p^n) = 0$, $n > k$, for each prime p [**2**]. It is also probably well known that $M^* \cap M^{\sim *} = \{\delta\}$, that is, that the inverse of a nontrivial element in some M_k is not in M_j for any j, (Proposition 1.2 below). From these facts follow the freeness of $M^{\blacksquare}$, Corollary 1.3.2. Using these ideas, we are able to give a recipe for constructing multiplicative functions which are not in $M^{\blacksquare}$, thus showing that M is strictly larger than $M^{\blacksquare}$. Of course, both are uncountable.

The following point of view will prove useful. Let $\gamma \in M_k$. Then γ is implicitly determined locally, i.e., at each prime number p, by a (monic) polynomial of degree k (its Bell polynomial at p). So, fixing p, we study the local behavior of $M^{\blacksquare}$. Thus, given a prime p and a polynomial $x^k + a_1 x^{k-1} + \cdots + a_k = P(x)$, an arithmetic function γ is determined locally by letting $\gamma^{-1}(p^n) = a_n$ if $n \leq k$ and 0 otherwise.

In Section 2 we determine $\gamma(p^n)$ explicitly in terms of the roots of the polynomial $P(x)$ and the discriminant of $P(x)$. In Section 3 we produce two recursive families of polynomials $\{F_{k,n}(t_1, \ldots, t_k)\}$ and $\{G_{k,n}(t_1, \ldots, t_k)\}$ which have the following virtues:

(i) $\gamma(p^n) = F_{k,n+1}(a_1, \ldots, a_k)$, Theorem 3.1. This gives an explicit local representation of γ in terms of the coefficients a_i of $P(x)$.

(ii) The G-polynomials are related to the F-polynomials by partial derivation.

In Section 4 we discuss the locally periodic functions. A function γ in M^* is *locally periodic* if, for some fixed positive integer s, $\gamma(p^{n+s}) = \gamma(p^n)$. Here we prove that γ is locally periodic if and only if the roots of the polynomials determining γ, $P_\gamma(x)$, are roots of unity and $P_\gamma(x)$ itself is a factor of a polynomial of the form $x^L - 1$, Theorems 4.1 and 4.2.

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 $\gamma \not\approx \delta$ 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. $\square$

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 $\{1, \ldots, r\}$, $\alpha_i = \beta_{\pi(i)}$. $\square$

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

In fact,

Corollary 1.3.2. *$M^{\blacksquare}$ is free.*

Since M_1 is infinite, in fact, uncountable, $M^{\blacksquare}$ is an infinitely-generated (uncountable) free abelian group.

The elements of $M^{\blacksquare}$ whose M_1-generators have the same values at each prime p clearly form a subgroup of $M^{\blacksquare}$. We call this subgroup the *uniform* subgroup of $M^{\blacksquare}$ and the multiplicative functions in this subgroup, *uniform* functions. The uniform subgroup is clearly a proper subgroup of $M^{\blacksquare}$. Now let $\{\chi_k\}$ be a family of uniform functions, one for each natural number k, such that $\chi_k^{-1}(p^t) = \chi_{k+1}(p^t)$ for $t \leq k$ and $\chi_{k+1}(p^{k+1}) \neq 0$. Construct a multiplicative function θ by defining θ^{-1} uniformly on all primes p to agree with the inverse of the uniform function χ_k on its first k values. Now an element of M_k or of $M_k^{\sim}$ is completely determined locally by k constants, e.g., by the values of its completely multiplicative generators at p, or by the coefficients of its polynomial $P(x)$. Thus θ is certainly not in M^* nor in $M^{*\sim}$. If $\theta = \gamma * \chi^{-1}$, where $\gamma \in M_k$ and $\chi \in M_j$, then $\theta * \gamma^{-1} \in M_j^{-1}$ and hence is determined by finitely many constants. But this is clearly not the case.

Theorem 1.4. *$M^{\blacksquare}$ is a proper subgroup of M.*

Remarks. It would be of interest to know if M is locally free, or even torsion free, and to know what is the structure of the quotient group $M/M^{\blacksquare}$.

2. Local properties of $M^{\blacksquare}$. The local generating function, i.e., the Bell series relative to p, for $\alpha \in M_1$ is $1/(1-\alpha(p)x)$, thus a generating function for α^{-1} is $1-\alpha(p)x$. Consider $\gamma \in M_k$. $\gamma = \alpha_1 * \cdots * \alpha_k$, where $\alpha_i \in M_1$. Let $\alpha_i(p) = r_i$. Using the fact that the convolution product of arithmetic functions translates as the pointwise product of their generating functions, we have as a generating function for γ, $x^k + a_1 x^{k-1} + \cdots + a_k$, where the a_j are up to sign the appropriate symmetric functions of the r_i. In particular, $a_1 = -\sum r_j$, $a_k = (-1)^k \sqcap_j r_j$. Thus, given any prime p and any set of complex numbers $a_1, \dots, a_k$, 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

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

and

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

Theorem 2.1. *Let $P(x)$ be a monic polynomial of degree k with coefficients $a_i \in \mathbf{C}$, $i = 1, \dots, k$, and with roots $r_1, \dots, r_k$. 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.

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

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. □

Proof of the lemma. $a_i = (-1)^j \sum r_{j_1} \cdots r_{ji}$, so the righthand side of the formula in the lemma becomes

$$-\left(\sum r_j\right) r_s^{n-1} + \cdots + (-1)^i \left(\sum r_{j1} \cdots r_{ji}\right) r_s^{n-i} \\ \pm \cdots + (-1)^k (r_1 \cdots r_k) r_s^{n-k}, \quad s = 1, \ldots, k.$$

That is,

$$a_i = -r_s^n - \sum_{j \neq s} r_j r_s^{n-1} + \cdots + (-1)^j \sum_{j \neq s} r_{j1} \cdots \\ r_{ji} r_s^{n-k} \pm \sum_{j \neq s} r_{j1} \cdots r_{j(i-1)} r_s^{n-k+1} + \cdots \pm \prod_{jr \neq s} r_{it} r_s^{n-k+1}.$$

Cancellation leaves $-r_s^n$, which gives the lemma. □

Corollary 2.1.2. *Δ_k is a factor of $\Delta_{k,n}$.*

Corollary 2.1.3.

$$\gamma(p^{n+1}) = \sum_{\sum_{i_j = n}} r_1^{i_1} \cdots r_k^{i_k}.$$

Remark. The case $k = 2$ is of interest, for then Theorem 2.1 gives the multiplicative function (in $M^{\blacksquare}$) as $(r_1^{n+1} - r_2^{n+1})/(r_1 - r_2)$ where r_1 and r_2 are the roots of the quadratic polynomial $x^2 + a_1 x + a_2$. In the case that $a_1 = -1$ and $a_2 = -1$, these are just the Fibonacci numbers. More generally, for $k = 2$, we get the Lehmer numbers.

Remark. Δ_k^2 is the discriminant of the polynomial P_γ which determines the arithmetic function γ.

3. The polynomials $F(t_1, \ldots, t_k)$ and $G(t_1, \ldots, t_k)$. First we consider the polynomials $P(x; t_1, \ldots, t_k) = x^k - t_1 x^{k-1} - \cdots - t_k$ in x with parameters $t_1, \ldots, t_k$. With respect to these parameters we define $F_{k,n}(t_1, \ldots, t_k)$ inductively by

$$F_{k,n}(t) = 0, \quad n < 1,$$
$$F_{k,1}(t) = 1,$$

and

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

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

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

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

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* $x^k + a_1 x^{n-1} + \cdots + a_k$, $j = 1, \dots, k$.

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. □

There is a number of pretty connections between the F-polynomials and the G-polynomials, for example:

Theorem 3.3.

$$G_{k,0} = k, \qquad G_{k,n} = F_{k,n+1} + \sum_{j=1}^{k-1} j t_{j+1} F_{k,n-j}, \quad n \geq 1.$$

The proof is straightforward and will be omitted. □

Theorem 3.4.

$$\frac{\partial G_{k,n}}{\partial t_j} = n F_{k,n}, \quad n \geq 0.$$

Again, the proof will be omitted. □

The two systems of polynomials are also related to each other by derivation.

When $k = 2$, we have lists that begin

$$\begin{array}{ll}
F_{2,0} = 0 & G_{2,0} = 2 \\
F_{2,1} = 1 & G_{2,1} = t_1 \\
F_{2,2} = t_1 & G_{2,2} = t_1^2 + 2t_2 \\
F_{2,3} = t_1^2 + t_2 & G_{2,3} = t_1^3 + 3t_1 t_2 \\
F_{2,4} = t_1^3 + 2t_1 t_2 & G_{2,4} = t_1^4 + 4t_1^2 t_2 + 2t_2^2 \\
F_{2,5} = t_1^4 + 3t_1^2 t_2 + t_2 & G_{2,5} = t_1^5 + 5t_1^3 t_2 + 5t_1 t_2^2 \\
\quad \cdots & \quad \cdots
\end{array}$$

Thus, for the case $k = 2$, it is reasonable to call these polynomials, respectively, *generalized Fibonacci polynomials* and *generalized Lucas polynomials*. When $(t_1, t_2) = (1, 1)$, the F-polynomials generate the Fibonacci numbers, the G-polynomials generate the Lucas numbers. (I am not aware that the term *Lucas polynomials* has been used before.) In fact, by appropriate selection of values for t_1 and t_2, we 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 $n = 0, 1, \dots,$ 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 $r_1, \dots, r_k$ be the roots of $P_\gamma(x)$, $\gamma \in M_k$, γ is locally periodic only if $r_1, \dots, r_k$ 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 might as well call *cyclotomic functions*).

Corollary 4.1.3. *If γ is locally periodic, then so is every convolution factor of γ locally periodic.*

However, it is not the case that the product of two locally periodic functions is necessarily a locally periodic function. For example, $(x-1)^2$ determines a function which is not locally periodic.

Theorem 4.2. *If $\gamma, \gamma \in M_k$, is locally periodic with period s, and if the roots of $P_\gamma(x)$ are the j_ith roots of unity, $r_1, \dots, r_k$, $r_i \neq r_j$, for $i \neq j$, then*

(i) *$s = L - k + 2$ where $L = LCM\{j_1, \dots, j_k\}$, and*

(ii) *γ is a (convolution) factor of χ, $\chi \in M_L$, where χ is periodic with period L and $P_\chi = x^L - 1$.*

Proof. We have from Theorem 2.1 that when $n + k - 2 = L$, then $\gamma(p^{n-1}) = 0$. This occurs when $n = L - k + 2$. Thus $s = L - k + 2$. Clearly $x^j - 1$ divides $x^L - 1$, which gives the second part of the theorem. $\square$

In particular, in the notation of Theorem 4.2, γ is periodic if and only if $x^j - 1$ divides $x^L - 1$ for each $j \in \{j_1, \dots, j_k\}$.

Corollary 4.2.1. *If the coefficients of the defining polynomials are restricted to the rational field, then the completely multiplicative locally periodic functions are just those determined by the linear polynomials $x - 1$ and $x + 1$. The quadratic polynomials which determine locally periodic functions are $CP(3)$, $CP(4)$, $CP(6)$ and $CP(1)$ times $CP(2)$ where $CP(m)$ is the mth cyclotomic polynomial.*

The arithmetic functions determined by the quadratic polynomials mentioned in Corollary 4.1.3 are, in the order cited, the functions with 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