CIRCULARLY GENERATED ABELIAN GROUPS

David A. Smith
Duke University, Durham, North Carolina

1. INTRODUCTION

A group will be called n-circularly generated if it has a set of $n(\geq 3)$ generators $x_1, x_2, \cdots, x_n$ such that $x_i x_{i+1} = x_{i+2}$ for all i, where the addition of subscripts is modulo n. This notion was suggested to the author by a problem in the American Mathematical Monthly [1], which can be phrased as follows: Show that a 5-circularly generated group is cyclic of order 11. The problem of determining the structure of circularly generated groups in general appears formidable. They are not all abelian, for the familiar quaternionic group [2, p. 8] clearly has this property for n = 3. Furthermore, if we don't insist that the generators all be distinct, any dicyclic group is 6-circularly generated with generators S, T, ST, S^{m-1}, $S^{2-m}T$, and ST, in the notation of [2, p. 7]. However, the structure of circularly generated abelian groups can be completely determined, as will be shown below.

It should be observed that an n-circularly generated group on $x_1, x_2, \cdots, x_n$ is clearly generated by x_1 and x_2, so if it is abelian, it must either be cyclic or the direct sum of exactly two cyclic subgroups. Furthermore, any circularly generated abelian group is the homomorphic image of an abelian group for which the circular relations are defining relations, so we will confine our attention to that case.

Henceforth (G, +) will denote an abelian group with generators $x_1, x_2, \cdots, x_n$ and defining relations*

$$x_i + x_{i+1} = x_{i+2}, \quad i = 1, 2, \cdots, n . \tag{1}$$

where addition of subscripts is modulo n.

Supported in part by NSF grant Number GP-4473.

*G is isomorphic to F/N, where F is the free abelian group on n generators $t_1, t_2, \cdots, t_n$ and N is the subgroup generated by all elements of the form $t_i + t_{i+1} - t_{i+2}$, under the correspondence $x_i \leftrightarrow t_i + N$. This means simply that all relations in G are consequences of the given relations (1).

The orders of the cyclic summands of G turn out to be various Fibonacci and Lucas numbers. We denote by F_m (respectively, L_m) the m^{th} Fibonacci (Lucas) number, with the usual initial conditions $F_0 = 0$, $L_0 = 2$, $F_1 = L_1 = 1$. Then the results to be proved below may be summarized as follows:

Theorem 1. If $4|n$, then G is the direct sum of two cyclic subgroups, one of order $F_{n/2}$, the other of order $5F_{n/2}$.

Theorem 2. If $2|n$ and $4\nmid n$, then G is the direct sum of two cyclic subgroups, each of order $L_{n/2}$.

Theorem 3. If $2\nmid n$ and $3|n$, then G is the direct sum of two cyclic subgroups, one of order 2, and the other of order $\frac{1}{2}L_n$.

Theorem 4. If $(n, 6) = 1$, then G is cyclic of order L_n.

Note that the direct sum of cyclic groups of orders k and m is itself cyclic of order km if and only if $(k, m) = 1$. It follows that the only cyclic group included among the first three cases is that for $n = 4$, since $F_2 = 1$ (see (10) below). The first eight cases in which G is cyclic are those for which $n = 4, 5, 7, 11, 13, 17, 19, 23$, and the corresponding orders are 5, 11, 29, 199, 521, 3571, 9349, 64079. These numbers are all prime except the last, which is 139 times 451. Thus, the smallest cyclic group G in our list whose order is composite is the one for $n = 23$.

We also observe that every Fibonacci number with even subscript appears among the cyclic summands in Theorem 1. Given any integer $m > 2$, m divides F_k, where k is the period of the Fibonacci sequence modulo m, and k is even [5, Corollary to Theorem 1 and Theorem 4]. Hence a cyclic group of order m is a homomorphic image of at least one of the groups listed above. For $m = 2$, we can take one of the groups of Theorem 3.

Corollary. Every finite cyclic group is n-circularly generated for some n.

2. SOME FIBONACCI AND LUCAS RELATIONS FOR REFERENCE

(2) $$F_{m-2} + F_{m+2} = 3F_m .$$

(3) $$F_{m+3} - F_{m-3} = 4F_m .$$

(4) $$F_{m+3} - F_{m-1} = L_{m+1} .$$

(5) $$F_m + F_{m+2} = L_{m+1} .$$

(6) $$F_{m+3} - F_{m-2} = F_{m+2} + 2F_{m-1} .$$

(7) $$2F_{m+2} - F_{m-3} = 5F_m .$$

(8) $$3F_{m+3} + F_m = 2F_{m+4} .$$

(9) If $3|m$, then $2|F_m$.

(10) If $3|m$, $2\nmid m$, then $4|L_m$.

(11) $$2F_m F_{m-1} + F_{m+2}^2 = L_{2m+1} .$$

(12) $$2F_{m+2}F_{m+1} - F_{m-1}^2 = L_{2m+1} .$$

Relations (2) — (10) are easy, and for the most part well-known, consequences of the definitions. Relations (11) and (12) may be new; their proofs are left as exercises for the reader.

3. A REDUCTION OF THE PROBLEM BY MATRICES

The defining relations for G may be written in matrix form:

$$Ax^t = 0 ,$$

where $x = (x_1, x_2, \cdots, x_n)$ and

$$A = \begin{bmatrix} 1 & 1 & -1 & 0 & \cdots & & 0 \\ 0 & 1 & 1 & -1 & 0 & \cdots & 0 \\ & & & \cdots\cdots & & & \\ 0 & \cdots & 0 & 1 & 1 & & -1 \\ -1 & 0 & \cdots & & 0 & 1 & 1 \\ 1 & -1 & 0 & \cdots & & 0 & 1 \end{bmatrix} .$$

The relation matrix A can be reduced via elementary row and column operations (over the integers) to a form from which one can read off the structure of G as a direct sum of cyclic groups [3, 4]. Rather than apply the standard procedure for this, we make some observations about the matrix A. By adding

suitable multiples of each of the first $n - 2$ rows to the last two rows, we can reduce A to a matrix of the form

$$\left[\begin{array}{c|cc} & B & \\ \hline 0 & a & b \\ & c & d \end{array}\right] , \tag{13}$$

where B is the $(n - 2)$ by n matrix consisting of the first $n - 2$ rows of A. In this form, it is clear that G is generated by x_{n-1} and x_n subject to the relations

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} x_{n-1} \\ x_n \end{pmatrix} = 0 , \tag{14}$$

and that an expression for each of the other x's in terms of these two can be read off from the matrix (13):

$$x_{n-2} = x_n - x_{n-1}, \quad x_{n-3} = x_{n-1} - x_{n-2} = 2x_{n-1} - x_n ,$$

etc. Thus, it suffices to determine the integers a, b, c, d and the structure of an abelian group with relations (14). Observe that row operations involving the first $n - 4$ rows of A do not affect the last two columns.

Lemma 1. After reducing the first k columns of A to zero below the diagonal $(0 \leq k \leq n - 4)$, the last two rows of A have the form:

$$\begin{array}{llll} 0 \cdots 0 & (-1)^{k+1}F_{k+1} & (-1)^{k}F_{k} & 0 \cdots 0\ 1\ 1 \\ \underbrace{0 \cdots 0}_{k} & (-1)^{k}F_{k+2} & (-1)^{k+1}F_{k+1} & \underbrace{0 \cdots 0}_{n-k-4}\ 0\ 1 \end{array} .$$

The proof is by induction on k. Simple induction proofs of this sort will be omitted.

In particular, after $n - 4$ column reductions, the last four rows and columns of (the new) A have the form:

$$\begin{bmatrix} 1 & 1 & -1 & 0 \\ 0 & 1 & 1 & -1 \\ (-1)^{n+1}F_{n-3} & (-1)^{n}F_{n-4} & 1 & 1 \\ (-1)^{n}F_{n-2} & (-1)^{n+1}F_{n-3} & 0 & 1 \end{bmatrix} . \tag{15}$$

Lemma 2. After $n - 2$ column reductions, A is reduced to the form (13), where $a = d = 1 + (-1)^{n+1}F_{n-1}$, $b = 1 + (-1)^{n}F_{n-2}$, and $c = (-1)^{n}F_{n}$.

Proof. Use the obvious row operations to reduce the first and second columns of (15) to zero below the diagonal.

For each of the cases in Theorems 1-4, we will use elementary row operations to reduce the matrix of (14) to one of the forms

$$\begin{pmatrix} p & 0 \\ kr & r \end{pmatrix}, \begin{pmatrix} kr & r \\ p & 0 \end{pmatrix}, \tag{16}$$

where p, r, k are integers. Then it is clear that G is the direct sum of the cyclic groups generated by x_{n-1} and $x_n + kx_{n-1}$, and that these have orders $|p|$ and $|r|$, respectively. In particular, G is cyclic when $|r| = 1$.

4. THE STRUCTURE OF G FOR EVEN n

Henceforth we will write each relation involving x_{n-1} and x_n by writing only the two coefficients. Thus, we have reduced the problem to the pair of defining relations (with the order reversed from that given above):

R 1 $\qquad (-1)^{n}F_{n}, \qquad 1 + (-1)^{n+1}F_{n-1}$

R 2 $\qquad 1 + (-1)^{n+1}F_{n-1}, \qquad 1 + (-1)^{n}F_{n-2}$.

For each $k > 2$, define the relation Rk to be the sum of the relations R(k - 1) and R(k - 2). Then one verifies by induction the general form

Rk $\qquad F_{k-1} + (-1)^{n-k-1}F_{n-k+1}, \; F_{k} + (-1)^{n-k}F_{n-k}$.

Clearly, any two consecutive ones of these relations are defining relations for G.

First, suppose that $n = 4q$, and let $m = 2q$. Then we have the defining relations

$$\begin{array}{ll} R(m-2) & F_{m-3} - F_{m+3}\ ,\ F_{m-2} + F_{m+2} \\ R(m-1) & F_{m-2} + F_{m+2}\ ,\ F_{m-1} + F_{m+1}\ . \end{array}$$

Using (2) and (3), we rewrite these as

$$\begin{array}{ll} R(m-2) & -4F_m\ ,\ 3F_m \\ R(m-1) & 3F_m\ ,\ -F_m\ . \end{array}$$

Add 3 times $R(m-1)$ to $R(m-2)$, and we have the relation matrix

$$\begin{pmatrix} 3F_m & -F_m \\ 5F_m & 0 \end{pmatrix}$$

in the form (16), which completes the proof of Theorem 1.

Now suppose $n = 4q + 2$, and again let $m = 2q$. Referring again to the general form for the relation Rk, we have defining relations

$$\begin{array}{ll} Rm & F_{m-1} - F_{m+3}\ ,\ F_m + F_{m+2} \\ R(m+1) & F_m + F_{m+2}\ ,\ F_{m+1} - F_{m+1}\ . \end{array}$$

Using (4) and (5), we have the relation matrix

$$\begin{pmatrix} -L_{m+1} & L_{m+1} \\ L_{m+1} & 0 \end{pmatrix}$$

in the form (16), which completes the proof of Theorem 2.

5. THE STRUCTURE OF G FOR ODD n

The proofs of Theorems 3 and 4 appear to require separate consideration of six cases, depending on the congruence class of n modulo 12.

Case I. Let $n = 12q + 1$ and $m = 6q$. Referring again to Rk in the previous section, we have the defining relations

$$\begin{array}{ll} R(m-1) & F_{m-2} - F_{m+3}\ ,\ F_{m-1} + F_{m+2} \\ Rm & F_{m-1} + F_{m+2}\ ,\ F_m - F_{m+1}\ . \end{array}$$

Use (3) and (6) to rewrite these as

$$\begin{array}{ll} R(m-1) & -2F_{m-1} - F_{m+2}\ ,\ 5F_{m-1} + F_{m-4} \\ Rm & F_{m-1} + F_{m+2}\ ,\ -F_{m-1}\ . \end{array}$$

We ignore the relations Rk for $k > m$ and define $R(m+1)$ by adding 5 times Rm to $R(m-1)$:

$$R(m+1) \qquad 3F_{m-1} + 4F_{m+2}\ ,\ F_{m-4}\ .$$

For $k > 1$, define $R(m+k)$ by adding 4 times $R(m+k-1)$ to $R(m+k-2)$. One obtains by induction (using (3)) the general form:

$$R(m+k) \qquad F_{3k+1}F_{m-1} + \tfrac{1}{2}F_{3k+3}F_{m+2},\ (-1)^{k+1}F_{m-3k-1}\ .$$

In particular, for $k = 2q - 2$ and $2q - 1$, we have the defining relations

$$\begin{array}{ll} R(8q-2) & F_{m-5}F_{m-1} + \tfrac{1}{2}F_{m-3}F_{m+2}\ ,\ -5 \\ R(8q-1) & F_{m-2}F_{m-1} + \tfrac{1}{2}F_mF_{m+2}\ ,\ \ 1 \end{array}$$

Add 5 times $R(8q-1)$ to $R(8q-2)$ to get a matrix of the form (16) with $r = 1$. Hence G is cyclic of order.

$$\begin{aligned} &(F_{m-5} + 5F_{m-2})F_{m-1} + \tfrac{1}{2}(F_{m-3} + 5F_m)F_{m+2} \\ &\quad = 2F_mF_{m-1} + F_{m+2}^2 \\ &\quad = L_{2m+1} \\ &\quad = L_n\ . \end{aligned}$$

(Formulas (7) and (11) were used here.)

Case II. Let $n = 12q + 5$ and $m = 6q + 2$. This leads to the same equations $R(m - 1)$, Rm, and $R(m + k)$ as in Case I. In particular, for $k = 2q - 1$ and $2q$, we have

$$R(8q + 1) \qquad F_{m-4} F_{m-1} + \tfrac{1}{2} F_{m-2} F_{m+2} \ , \quad 3$$

$$R(8q + 2) \qquad F_{m-1}^2 + \tfrac{1}{2} F_{m+1} F_{m+2} \ , \quad -1$$

As in Case I, this leads to a cyclic group whose order (using (8) and (11)) is

$$\begin{aligned} &(F_{m-4} + 3F_{m-1})F_{m-1} + \tfrac{1}{2}(F_{m-2} + 3F_{m+1})F_{m+2} \\ &\quad = 2F_{m-1}F_m + F_{m+2}^2 \\ &\quad = L_{2m+1} \\ &\quad = L_n \ . \end{aligned}$$

Case III. Let $n = 12q - 5$ and $m = 6q - 3$. From the general form Rk we have relations

$$Rm \qquad F_{m-1} - F_{m+2} \ , \quad F_{m+2}$$

$$R(m + 1) \qquad F_{m+2} \ , \quad F_{m-1} \ .$$

For $k > 1$, $R(m + k)$ is defined to be $R(m + k - 2)$ minus four times $R(m + k - 1)$. Using (3) and induction on k, we have

$$R(m + k) \qquad \frac{(-1)^k}{2} F_{3k-3} F_{m-1} + (-1)^{k+1} F_{3k-1} F_{m+2} \ , \quad F_{m-3k+2} \ .$$

In particular, for $k = 2q - 2$ and $2q - 1$, we have

$$R(8q - 5) \qquad \tfrac{1}{2} F_{m-6} F_{m-1} - F_{m-4} F_{m+2} \ , \quad 5$$

$$R(8q - 4) \qquad -\tfrac{1}{2} F_{m-3} F_{m-1} + F_{m-1} F_{m-2} \ , \quad 1 \ .$$

Again G is cyclic, and the order L_n is computed as in Case I, using (12) instead of (11).

Case IV. Let $n = 12q - 1$ and $m = 6q - 1$. Then relations Rm, R(m + 1), and R(m + k) are as in Case III. For $k = 2q - 1$ and $2q$ we have

$$R(8q-2) \qquad -\tfrac{1}{2}F_{m-5}F_{m-1} + F_{m-3}F_{m+2}, \quad 3$$

$$R(8q-1) \qquad \tfrac{1}{2}F_{m-2}F_{m-1} + F_{m}F_{m+2}, \quad 1 .$$

Again G is cyclic of order L_n, using (8) and (12) as in the previous cases. This completes the proof of Theorem 4.

Case V. Let $n = 12q + 3$ and $m = 6q + 1$. The relations Rm, R(m + 1), and R(m + k) are the same as in Case III. For $k = 2q$ and $2q + 1$, we have

$$R(8q-1) \qquad \tfrac{1}{2}F_{m-4}F_{m-1} - F_{m-2}F_{m+2}, \quad 2$$

$$R(8q+2) \qquad -\tfrac{1}{2}F_{m-1}^2 + F_{m+1}F_{m+2}, \quad 0 .$$

By (9), the first entry in R(8q + 1) is even, hence we have a matrix of the form (16) and G is the direct sum of two cyclic groups, one of order 2, the other (by (12)) of order $\frac{1}{2}L_{2m+1} = \frac{1}{2}L_n$.

Case VI. Let $n = 12q - 3$ and $m = 6q - 2$. Then we have the same relations as in Case I. For $k = 2q - 2$ and $2q - 1$, we have

$$R(8q-4) \qquad F_{m-3}F_{m-1} + \tfrac{1}{2}F_{m-1}F_{m+2}, \quad -2$$

$$R(8q-3) \qquad F_{m}F_{m-1} + \tfrac{1}{2}F_{m+2}^2, \quad 0 .$$

As in Case V, this leads to the direct sum of a cyclic group of order 2 and one of order $\frac{1}{2}L_n$, which completes the proof of Theorem 3.

6. A FURTHER CONSEQUENCE

It is easy to verify that the second entries in each of the relations appearing in each reduction process above are, except for sign, the remainders in the Euclidean Algorithm, applied to the two entries of relation R1. Thus the smallest non-zero entry appearing is their greatest common divisor.

Corollary. If n is even, then

$$(F_n, F_{n-1} - 1) = \begin{cases} F_{n/2}, & \text{if } 4 \mid n \\ L_{n/2}, & \text{otherwise.} \end{cases}$$

If n is odd, then

$$(F_n, F_{n-1} + 1) = \begin{cases} 2, & \text{if } 3 \mid n \\ 1, & \text{otherwise.} \end{cases}$$

REFERENCES

1. J. H. Conway, Problem 5327 (proposed), American Math. Monthly 72(1965) p. 915.
2. H. S. M. Coxeter and W. O. J. Moser, Generators and Relations for Discrete Groups, Springer, Berlin, 1957.
3. N. Jacobson, Lectures in Abstract Algebra, Vol. II, Van Nostrand, Princeton, 1953, pp. 79-83.
4. D. A. Smith, "A Basic Algorithm for Finitely Generated Abelian Groups," Mathematical Algorithms 1 (1966).
5. D. D. Wall, "Fibonacci Series Modulo m," American Math. Monthly, 67, (1960) pp. 525-532.

★ ★ ★ ★ ★