MATH. SCAND. 32 (1973), 165–168

PERIODICITY OF RECURRING SEQUENCES IN RINGS

TORLEIV KLØVE

1.

In this paper all rings are commutative (not necessarily containing a unit). A *recurring sequence* in a ring R is a sequence $x_0, x_1, \ldots$ of elements from R satisfying.

$$(1.1) \qquad x_n = P(x_{n-1}, \ldots, x_{n-\varrho}) + r_0 \quad \text{for all } n \geqq \varrho ,$$

where P is a polynomial without constant term and with coefficients $r_1, r_2, \ldots, r_m$ in R. We call $r_0 \in R$ "the *constant term* of the recurring sequence". When P is a polynomial of first degree the sequence is called a linear recurring sequence.

A sequence $x_0, x_1, \ldots$ in R is called *periodic* if there exist integers $\mu > 0$ and $N \geqq 0$ such that

$$x_{n+\mu} = x_n \quad \text{for all } n \geqq N ;$$

μ is then a *period* for the sequence.

We shall prove the following theorem.

THEOREM 1. *If the linear recurring sequence defined by* $x_0 = 0, x_n = x_{n-1} + r_0$ (that is $x_n = nr_0$) *is periodic and the linear recurring sequences defined by* $x_0 = r, x_n = rx_{n-1}$ (that is $x_n = r^{n+1}$) *are periodic for each* $r \in R$ *then every recurring sequence in* R *with constant term* r_0 *is periodic.*

2.

For each $r \in R$ let $S(r)$ be the least positive integer such that $S(r)r = 0$. If no such integer exists we put $S(r) = \infty$. We shall need the following lemmas.

LEMMA 1. *The following two conditions are equivalent*:

(i) *For each* $r \in R$ *the linear recurring sequence defined by* $x_0 = r, x_n = rx_{n-1}$ *is periodic.*

Received May 16, 1972.

(ii) *For each* $r \in R$ *there exist two positive integers* $k(r), l(r)$ *such that* $r^{k(r)+l(r)} = r^{l(r)}$.

LEMMA 2. *Let* $r_0 \in R$. *The following two conditions are equivalent:*

(i) *The linear recurring sequence defined by* $x_0 = 0, x_n = x_{n-1} + r_0$ *is periodic.*

(ii) $S(r_0)$ *is finite.*

LEMMA 3. *Let* R *be a ring satisfying condition* (ii) *of lemma* 1.

(i) *For each* $r \in R$ *there exists a positive integer* $\lambda(r)$ *such that* $S(r^{\lambda(r)})$ *is finite.*

(ii) *If* $S(a)$ *is finite for some* $a \in R$, *then* $S(ar)$ *is finite and divides* $S(a)$ *for all* $r \in R$.

Lemmas 1 and 2 are immediate consequences of the definition of periodicity. To prove lemma 3 we first note that if $r^{k+l} = r^l$, then $r^{\alpha k + \lambda} = r^\lambda$ for all integers $\alpha \geqq 0$ and $\lambda \geqq l$. Let $\lambda = \lambda(r) = \max(l(r), l(2r))$, $k = k(r)$ and $\varkappa = k(2r)$. Then

$$2^\lambda r^\lambda = (2r)^\lambda = (2r)^{k\varkappa + \lambda} = 2^{k\varkappa + \lambda} r^{\varkappa k + \lambda} = 2^{k\varkappa + \lambda} r^\lambda .$$

Hence

$$(2^{k\varkappa + \lambda} - 2^\lambda) r^\lambda = 0 ,$$

which proves (i). To prove (ii) we note that

$$S(a)ar = (S(a)a)r = 0 .$$

Hence $S(ar) \leqq S(a)$. Put $S(a) = pS(ar) + q$ where $0 \leqq q < S(ar)$. Then

$$qar = S(a)ar - pS(ar)ar = 0$$

and hence $q = 0$ by the minimality of $S(ar)$.

We note that if R of lemma 3 is a ring with unit e, then $S(r)$ is finite for all $r \in R$. This is a consequence of lemma 3 since $e^{\lambda(e)} = e$, hence $S(e)$ is finite and so $S(r) = S(er)$ is finite. In particular, the two equivalent conditions of lemma 2 are satisfied for such rings.

3.

We now turn to the proof of theorem 1. Suppose conditions (i) (and hence conditions (ii)) of lemma 1 and 2 are satisfied and let $x_0, x_1, \ldots$ be any recurring sequence satisfying (1.1). Applying (1.1) repeatedly we get

$$x_n = Q_n(x_0, \ldots, x_{\varrho-1}) + r_0 Q_n^*(x_0, \ldots, x_{\varrho-1}) , \tag{3.1}$$

where Q_n is a polynomial whose coefficients are polynomials q_{nj}, $j=1,2,\ldots,J(n)$, in $r_1,r_2,\ldots,r_m$ with integral coefficients, $r_1,r_2,\ldots,r_m$ being the coefficients of P, and $Q_n{}^*$ is a polynomial whose coefficients are polynomials $q_{nj}{}^*, j=1,2,\ldots,J^*(n)$, in $r_0,r_1,\ldots,r_m$.

The polynomials Q_n are given recursively by

$$Q_n(x_0,\ldots,x_{\varrho-1}) = x_n \quad \text{if } 0 \leqq n \leqq \varrho-1\,, \tag{3.2}$$

$$Q_n(x_0,\ldots,x_{\varrho-1}) = P(Q_{n-1}(\ldots),\ldots,Q_{n-\varrho}(\ldots)) \quad \text{if } n \geqq \varrho. \tag{3.3}$$

Let $d(n)$ be the degree of the term in the polynomials q_{nj} of least degree. By (3.2) and (3.3)

$$d(n) = 0 \quad \text{if } 0 \leqq n \leqq \varrho-1\,,$$
$$d(n) \geqq \min_{1\leqq i\leqq \varrho}\{d(n-i)+1\} \quad \text{if } n \geqq \varrho\,.$$

By induction on n we get

$$d(n) \geqq [n/\varrho] \tag{3.4}$$

where $[x]$ denotes the greatest integer $\leqq x$. Put $S=$least common multiple of $S(r_i{}^{\lambda(r_i)})$, $i=1,2,\ldots,m$. Then

$$Sr_1{}^{\alpha_1}\ldots r_m{}^{\alpha_m} = 0$$

if $\alpha_i \geqq \lambda(r_i)$ for at least one i by lemma 3. Hence, if

$$n \geqq \varrho\{\lambda(r_1)+\ldots+\lambda(r_m)-m+1\}$$

then, by (3.4), q_{nj} is a polynomial with coefficients $<S$. Since q_{nj} is of degree $<k(r_i)+\lambda(r_i)$ in r_i, there are only a finite number of such polynomials. Further Q_n is a polynomial of degree $<k(x_i)+l(x_i)$ in x_i, hence there are only a finite number of different Q_n's.

As to the polynomials $r_0Q_n{}^*$ we note that the coefficients of $r_0q_{nj}{}^*$ are $<S(r_0)$, hence there are only a finite number of different $r_0Q_n{}^*$. Finally, by (3.1), there are only a finite number of different x_n's and so there are only a finite number of different arrays $x_n,x_{n+1},\ldots,x_{n+\varrho-1}$. Hence there exist integers $N\geqq 0$ and $\mu>0$ such that

$$x_{n+\mu} = x_n \quad \text{for } n = N,N+1,\ldots,N+\varrho-1\,.$$

By (1.1), $x_{n+\mu}=x_n$ for all $n\geqq N$.

4.

Ward [1] defined periodicity modulo an ideal A in R as follows:

The sequence $x_0,x_1,\ldots$ is periodic modulo A if $x_{n+\mu}-x_n \in A$ for all $n\geqq N$.

This, however, is the same as periodicity of the sequence x_0+A, $x_1+A, \ldots$ in the ring R/A. Thus the first part of Ward's theorem 6.1 is a corollary of our theorem 1.

5.

We may define recurrence somewhat more generally and prove an analogous theorem in the general case.

Let C be a set containing R, in which there is defined a multiplication

(i) which extends the multiplication in R,

(ii) which is commutative, assosiative, and distributive over addition in R,

(iii) such that $cr \in R$ for all $c \in C$, $r \in R$.

A *recurring sequence* in R with *coefficients* in C is a sequence $x_0, x_1, \ldots$ of elements from R satisfying (1.1) where now P is a polynominal with coefficients in C; the r_0 in (1.1) is still an element of R.

A possible choice of C is $C = R \cup \mathsf{Z}$, Z being the set of integers. The multiplication in C is defined in the natural way. This choice of C covers all recurrences with integral coefficients, these would not be otherwise covered if R is a ring without unit.

Another choice is C being a ring having R as an ideal.

We get the following theorem (which reduces to theorem 1 if $C = R$).

THEOREM 2. *If the linear recurring sequence defined by* $x_0 = 0, x_n = x_{n-1} + r_0$ (that is $x_n = nr_0$) *is periodic and the linear recurring sequences defined by* $x_0 = r, x_n = cx_{n-1}$ (that is $x_n = c^n r$) *are periodic for each* $r \in R$ and $c \in C$ *then every recurring sequence in R with coefficients in C and constant term* r_0 *(in R) is periodic.*

With minor alterations the proof of theorem 1 also applies to theorem 2.

REFERENCE

1. M. Ward, *Arithmetical properties of sequences in ring*, Ann. of Math. (2), 39 (1938), 210–219.

UNIVERSITY OF BERGEN,
BERGEN, NORWAY