# ON GROUPS OF LINEAR RECURRENCES. I.

By R. R. Laxton

**Introduction.** A linear recurrence $\mathcal{W} = \{w_n, n \in \mathbf{Z}\}$ of degree $m$ with $f(x) = x^m - a_{m-1}x^{m-1} - \cdots - a_0$ as companion polynomial is given by a set $w_0$, $w_1, \cdots, w_{m-1}$ of numbers together with the relation $w_{n+m} = a_{m-1}w_{n+m-1} + \cdots + a_0 w_n$ for all $n \in \mathbf{Z}$ (we assume that not all the $a_i$ are zero). The early interest in linear recurrences was in those of degree two with $f(x) = x^2 - Px + Q \in \mathbf{Z}[x]$ and $w_0$, $w_1 \in \mathbf{Z}$. Furthermore, the interest was in special sequences; the most frequently considered one was the Lucas sequence $\mathcal{I}$ of $f(x)$ with $i_0 = w_0 = 0$ and $i_1 = w_1 = 1$, and occasionally the sequence $\mathcal{E}$ with $e_0 = w_0 = 2$ and $e_1 = w_1 = P$ was studied for its connection with the Lucas sequence. Very occasionally a few other special types of recurrences have been studied (see for example [3]). The recent study of general integral linear recurrences of degree two is largely the work of M. Ward in a whole series of papers (see later references). Besides this, there is the study of general linear recurrences defined over finite fields (see E. Selmer's [8] which also contains an extensive bibliography on the subject). In connection with this class of recurrences a ring structure has been constructed for those with a fixed companion polynomial.

One problem of perennial interest is that of prime divisors of a recurrence. A prime is a divisor of an integer linear recurrence $\mathcal{W} = \{w_n, n \in \mathbf{Z}, n \geq 0\}$ if it divides some $w_n$ of $\mathcal{W}$. K. Mahler [5] and M. Ward [11] proved that, with the usual exceptions, every linear recurrence of degree two has an infinity of prime divisors (in fact, Mahler proves much more; also the above mentioned result can be generalized for recurrences of degree greater than two). Of course since $i_0 = 0$ in $\mathcal{I}$ every prime is a divisor of a Lucas sequence. However, more can be said; if a prime $p$ does not divide the constant coefficient $Q$, then $p$ divides the terms of $\mathcal{I}$ with a certain periodicity and similarly if $p$ is a divisor of $\mathcal{W}$ it divides the terms of $\mathcal{W}$ with the same periodicity. One of Ward's main concerns was to obtain general criteria to determine if a prime is a divisor of a recurrence $\mathcal{W}$ or not. No really satisfactory criteria is known at present. The divisor problem is the chief interest in this article.

Here we begin a systematic study of linear recurrences of degree two by introducing a commutative group structure $G(f)$ on (essentially) all linear recurrences which have $f(x)$ as companion polynomial. The main feature is that we no longer regard a recurrence as 'starting' from a fixed pair of integers $w_0$, $w_1$, rather we regard it as a doubly infinite sequence of terms, though now not all the terms need be integers (they are from some point onwards). By this means we identify two linear recurrences $\mathcal{W} = \{w_n, n \in \mathbf{Z}\}$ and $V = \{v_n, n \in \mathbf{Z}\}$ with the same companion polynomial $f(x)$ if there exists non-zero integers $k$, $l$ and

Received February 10, 1968.