PACIFIC JOURNAL OF MATHEMATICS
Vol. 32, No. 1, 1970

ON GROUPS OF LINEAR RECURRENCES II. ELEMENTS OF FINITE ORDER

R. R. LAXTON

For each quadratic polynomial $f(x) \in Z[x]$, whose ratio of roots is not ± 1, a group $G(f)$ of equivalence classes of certain linear recurrences with companion polynomial $f(x)$ has been constructed by the author. Its structure was shown to be connected with the structure of the sets of prime divisors of the linear recurrences. The group $G(f)$ is infinite but its torsion subgroup is finite and usually, but not always, consists of just two elements; the class of the Lucas sequence $\mathscr{S} = [0, 1]$ of $f(x)$ and the class of the recurrence $\mathscr{E} = [2, P]$ associated with $f(x)$. This subgroup is completely determined here for each polynomial $f(x)$. In 1961 M. Ward raised the question whether $(\mathscr{S})$ and $(\mathscr{E})$ are the only classes whose sets of prime divisors can be characterized globally. It is shown in this article that there are groups $G(f)$ with elements of finite order, other than $(\mathscr{S})$ and $(\mathscr{E})$, whose prime divisors can be similarly characterized.

We shall use the notation and results of [1]. Part of the object of defining the group structure $G(f)$, where $f(x) = x^2 - Px + Q \in \boldsymbol{Z}[x]$ and $(P, Q) = 1$, is to determine those recurrences among the set of all recurrences with companion polynomial $f(x)$ which are in some sense special. Probably the true sense of special would mean those recurrences which have peculiar arithmetical properties not shared by the remaining ones.[1] For example, the Lucas sequence $\mathscr{S} = [0, 1]$ of $f(x)$ is such a recurrence and so to all intents and purposes is the sequence $\mathscr{E} = [2, P]$ of $f(x)$. Both $(\mathscr{S})$ and $(\mathscr{E})$ are of finite order in $G(f)$; here we interpret 'special' as meaning of finite order in $G(f)$. There are only a finite number of such elements in $G(f)$; furthermore if $(\mathscr{W}) \in G(f)$ and $(\mathscr{W})^k = (\mathscr{S})$ it would seem that the arithmetical properties of $\mathscr{W}$ are fairly closely related to those of $\mathscr{S}$. This is so for $(\mathscr{E})$ and for the other elements $(\mathscr{A})$ and $(\mathscr{B})$ of order two in $G(f)$ (when they exist); for example see Theorem 4.6 of [1] and the final paragraph of that paper. Also some properties of recurrences of finite order are readily deducible which, although they may be true for most or even all recurrences, are not so easily proved in full generality (see for example [1], 3.9.1). Here we determine the structure of the subgroup of elements of finite order. Then we shall show by means of examples that the prime divisors of

[1] An article "On groups of Linear Recurrences III. Arithmetic properties" is in preparation.

some elements of finite order (other than $\mathscr{T}$ and $\mathscr{E}$) can be characterized globally—thus some elements of finite order are even special in the arithmetical sense. Finally we add a few words concerning elements of the group which are locally finite everywhere.

1. **The elements of finite order in $G(f)$.** We shall carry out the computations only when $f(x)$ is irreducible over $\boldsymbol{Q}$; The results remain valid when $f(x)$ is reducible but involve slightly longer calculations. Let $\mathscr{W} \in F(f)$ be given by

$$w_n = (A\theta_1^n - B\theta_2^n)/(\theta_1 - \theta_2)\ , \tag{1.1}$$

for all $n \in \boldsymbol{Z}$, with $A = w_1 - w_0\theta_2$, $B = w_1 - w_0\theta_1$, $w_0, w_1 \in \boldsymbol{Z}$ and $(w_0, w_1) = (Q, w_1) = 1$. Thus $\mathscr{W}$ is a reduced recurrence (see beginning of § 3 of [1]).

We denote the subgroup of elements of finite order in $G(f)$ by $H(f)$. Thus $(\mathscr{W}) \in H(f)$ if and only if $\mathscr{W}^m \equiv \mathscr{T}$ in $F(f)$ for some positive integer m. But this holds exactly when

$$(w_1 - w_0\theta_2)^m = d\theta_1^n \tag{1.2}$$

for some $n, d \in \boldsymbol{Z}$. We conclude that $(AB)^m = d^2Q^n$ and as $\mathscr{W}$ is reduced that $(d, Q) = 1$. Thus both d^2 and Q^n are m-th powers in $\boldsymbol{Z}$; put $d^2 = g^m$, $g \in \boldsymbol{Z}$, and on squaring both sides of (1.2) obtain

$$(w_1 - w_0\theta_2)^{2m} = g^m\theta_1^{2n}\ . \tag{1.3}$$

It follows that if $\mathscr{W}^m \equiv \mathscr{T}$, then some m-th root of θ_1^{2n} lies in $\boldsymbol{Q}(\theta_1)$ and if we denote this root by $\sqrt[m]{\theta_1^{2n}}$ we get

$$(w_1 - w_0\theta_2)^2 = g\zeta\sqrt[m]{\theta_1^{2n}} \tag{1.4}$$

for some $n, g \in \boldsymbol{Z}$ and some m-th root of unity $\zeta \in \boldsymbol{Q}(\theta_1)$.

We remark that if ζ, m, n are fixed, the solutions $(\mathscr{W}) \in G(f)$ obtained from (1.4) are independent of g.

Now we do have a solution to (1.4) when $n = m$ and $\zeta = 1$, namely $(\mathscr{T})$ and $(\mathscr{E})$ (see § 4 of [1]). So we may take n/m to be the least positive number for which (1.4) has a solution with $w_0, w_1, g \in \boldsymbol{Z}$ and some root of unity $\zeta \in \boldsymbol{Q}(\theta_1)$. It follows that $0 < n \leqq m$ and that n divides m. The latter is clear since if we put $t - 1 \leqq m/n < t$, then $m = tn - s$, $0 \leqq s < n$ and on substituting in (1.4) with both sides raised to the power t we obtain $((w_1 - w_0\theta_2)^t)^2 = g^t\zeta^t\theta_1^{2s}\sqrt[m]{\theta_1^{2s}}$. Hence if (1.4) has a solution so does this equation, but $s/m < n/m$ so that $s = 0$. If we put $kn = m$, $k \in \boldsymbol{Z}$, then $1/k$ is the least positive number for which there exists a solution w_0, w_1, g, ζ to (1.4); if another solution exists for some $m = m'$ and $n = n'$, then $n'/m' = t/k$ for some $t \in \boldsymbol{Z}$, $0 < t \leqq k$. Therefore all elements of $H(f)$

are obtained by solving the k equations

$$(1.5.t) \qquad (w_1 - w_0\theta_2)^2 = g\zeta \sqrt[k]{\theta_1^{2t}}\,, \qquad t = 1, 2, \cdots, k$$

for some $w_0, w_1, g \in \boldsymbol{Z}$ and some root of unity $\zeta \in \boldsymbol{Q}(\theta_1)$.

The solutions obtained from the equation (1.5.k) are $(\mathscr{S})$ and $(\mathscr{E})$ and if $(\mathscr{W})$ is one solution of (1.5.t), the other is $(\mathscr{W}\mathscr{E})$. Since $\zeta \in \boldsymbol{Q}(\theta_1)$ it can only take the value ± 1, $\pm i$ and $\pm w$, $\pm w^2$, where w is a complex cube root of unity. So we have three cases.

Case 1. Here we assume that $\boldsymbol{Q}(\theta_1)$ contains no complex root of unity. We are left with solving (1.5.t) with $\zeta = 1$. Let $(\mathscr{W})$, $(\mathscr{W}\mathscr{E}) \in H(f)$ be the solutions derived from (1.5.1); then $(\mathscr{W})^2 = (\mathscr{W}\mathscr{E})^2$ and so provide one solution of (1.5.2), $(\mathscr{W})^3 \neq (\mathscr{W}\mathscr{E})^3$ are the two solutions derived from (1.5.3), and similarly up to the solutions $(\mathscr{W})^k$ and $(\mathscr{W}\mathscr{E})^k$ obtained from (1.5.k) the solutions of which are, as mentioned above, $(\mathscr{S})$ and $(\mathscr{E})$. If k is odd then $(\mathscr{W})^k \neq (\mathscr{W}\mathscr{E})^k$ and so one of them is $(\mathscr{E})$, say $(\mathscr{W})^k = (\mathscr{E})$. Then clearly $H(f) = \langle(\mathscr{W})\rangle \cong \boldsymbol{Z}_{2k}$, a cyclic group of order $2k$. If k is even and $(\mathscr{X})^2 = (\mathscr{E})$ has a solution in $G(f)$ (see § 4 of [1]), then necessarily $(\mathscr{W})^k = (\mathscr{W}\mathscr{E})^k = (\mathscr{E})$ and again $H(f) = \langle(\mathscr{W})\rangle \cong \boldsymbol{Z}_{2k}$. On the other hand, if $(\mathscr{X})^2 = (\mathscr{E})$ has no solution in $G(f)$, then $(\mathscr{W})^k = (\mathscr{W}\mathscr{E})^k = (\mathscr{S})$ and it follows that $H(f) = \langle(\mathscr{W})\rangle \times \langle(\mathscr{E})\rangle \cong \boldsymbol{Z}_k \times \boldsymbol{Z}_2$ (direct product).

If $f(x)$ is reducible over $\boldsymbol{Q}$, then we have to solve simultaneously $(w_1 - w_0\theta_2)^{2m} = g^m\theta_1^{2n}$ and $(w_1 - w_0\theta_1)^{2m} = g^m\theta_2^{2n}$ and consequently $(w_1 - w_0\theta_2)^2 = f\sqrt[m]{\theta_1^{2n}}$ and $(w_1 - w_0\theta_1)^2 = g\sqrt[m]{\theta_2^{2n}}$ or $(w_1 - w_0\theta_1)^2 = -g\sqrt[m]{\theta_2^{2n}}$. We have proved

THEOREM 1. *Let $\boldsymbol{Q}(\theta_1) \neq \boldsymbol{Q}(i)$ or $\boldsymbol{Q}(w)$ and k be the maximal positive integer such that $(w_1 - w_0\theta_2)^2 = g\zeta_1\sqrt[k]{\theta_1^2}$ and $(w_1 - w_0\theta_1)^2 = g\zeta_2\sqrt[k]{\theta_2^2}$ have simultaneous solutions with $w_1, w_0, g \in \boldsymbol{Z}$ and $\zeta_1, \zeta_2 = \pm 1$ (which are identical if $\boldsymbol{Q}(\theta_1) \neq \boldsymbol{Q}$). Then the subgroup $H(f)$ of elements of finite order in $G(f)$ is isomorphic to $\boldsymbol{Z}_{2k}$ when k is odd or when k is even and $(\mathscr{X})^2 = (\mathscr{E})$ has a solution in $G(f)$ and is isomorphic to $\boldsymbol{Z}_k \times \boldsymbol{Z}_2$ when k is even and $(\mathscr{X})^2 = (\mathscr{E})$ has no solution in $G(f)$.*

The condition of the theorem implies that Q is a unit times a k-th power in $\boldsymbol{Z}$. By Theorem 4.5 of [1], $(X)^2 = (E)$ has a solution in $G(f)$ when and only when $-(P^2 - 4Q)$ or $-Q(P^2 - 4Q)$ is a square in Z. Since $\boldsymbol{Q}(\theta_1) \neq Q(i)$ this can only happen when Q is the negative of a square and $P^2 - 4Q$ is a square, i.e., $f(x)$ is reducible over $\boldsymbol{Q}$.

EXAMPLE. $f(x) = (x - 4)(x + 9)$ so that $Q = -6^2$, k is even and $H(f) \cong \boldsymbol{Z}_4$. Direct calculation shows that $H(f) = \{[5, -19], [2, -5], [1, -35], [0, 1]\}$ and is obtained by solving $(w_1 + w_0 9)^2 = f(4)$ and $(w_1 - w_0 4)^2 = -f(-9)$ simultaneously.

Case 2. $\boldsymbol{Q}(\theta_1) = Q(i)$. The equation $(\mathrm{w}_1 - w_2\theta_2)^2 = ei$ has a solution $w_0, w_1, e \in \boldsymbol{Z}$; let us denote the resulting solution in $G(f)$ by $(\mathscr{Y}\hat{})$. Then $(\mathscr{I})$, $(\mathscr{Y}\hat{})$, $(\mathscr{Y}\hat{})^2$ and $(\mathscr{Y}\hat{})^3$ are all distinct and $(\mathscr{Y}\hat{})^4 = (\mathscr{I})$. Furthermore $(\mathscr{Y}\hat{})^2$ is derived from a solution of $(t_1 - t_0\theta_2)^2 = g \in \boldsymbol{Z}$ and so must be $(\mathscr{E})$. It follows that if we obtain all the solutions of the equation (1.5.t) with $\zeta = 1$ we get all elements of $H(f)$ combining these with the powers of $(\mathscr{Y}\hat{})$.

Let $(\mathscr{W}\hat{})$ and $(\mathscr{W}\hat{}\mathscr{E})$ be solutions of (1.5.1) with $\zeta = 1$; then all solutions of (1.5.1) for all ζ are $(\mathscr{W}\hat{})$, $(\mathscr{W}\hat{}\mathscr{E})$, $(\mathscr{W}\hat{}\mathscr{Y}\hat{})$ and $(\mathscr{W}\hat{}\mathscr{Y}\hat{}\mathscr{E})$. Then two solutions of (1.5.2) are $(\mathscr{W}\hat{})^2 = (\mathscr{W}\hat{}\mathscr{E})^2$ and $(\mathscr{W}\hat{}\mathscr{Y}\hat{})^2 = (\mathscr{W}\hat{}\mathscr{Y}\hat{}\mathscr{E})^2 = (\mathscr{W}\hat{})^2(\mathscr{E})$, all four solutions of (1.5.3) are $(\mathscr{W}\hat{})^3$, $(\mathscr{W}\hat{}\mathscr{E})^3$, $(\mathscr{W}\hat{}\mathscr{Y}\hat{})^3$ and $(\mathscr{W}\hat{}\mathscr{Y}\hat{}\mathscr{E})^3$ and similarly up to the solutions $(\mathscr{W}\hat{})^k$, $(\mathscr{W}\hat{}\mathscr{E})^k$ $(\mathscr{W}\hat{}\mathscr{Y}\hat{})^k$ and $(\mathscr{W}\hat{}\mathscr{Y}\hat{}\mathscr{E})^k$ obtained for (1.5.k) (the solutions of which are $(\mathscr{I})$, $(\mathscr{E})$, $(\mathscr{Y}\hat{})$ and $(\mathscr{Y}\hat{}\mathscr{E})$, for all possible values of ζ). If k is odd then the four solutions obtained are all distinct and so one is $(\mathscr{I})$—say $(\mathscr{W}\hat{})^k = (\mathscr{I})$. Then $H(f) = \langle(\mathscr{W}\hat{})\rangle \times \langle(\mathscr{Y}\hat{})\rangle \cong \boldsymbol{Z}_k \times \boldsymbol{Z}_4$ (direct product). If $k = 2 \pmod 4$, then the distinct solutions obtained are $(\mathscr{W}\hat{})^k$ and $(\mathscr{W}\hat{})^k(\mathscr{E})$ one of which must be $(\mathscr{I})$. So we have the same result. If $k = 0 \pmod 4$ all our solutions in $G(f)$ obtained for (1.5.k) are identical to $(\mathscr{W}\hat{})^k$. Now we already have two solutions of the equations $(\mathscr{X}\hat{})^2 = (\mathscr{E})$, namely $(\mathscr{X}\hat{}) = (\mathscr{Y}\hat{})$ and $(\mathscr{Y}\hat{}\mathscr{E})$. Such an equation can have no, two or four solutions in $G(f)$ (see [1] 4.5). If then only two solutions exist, $(\mathscr{W}\hat{})^k = (\mathscr{I})$ and again our group $H(f) = \langle(\mathscr{W}\hat{})\rangle \times \langle(\mathscr{Y}\hat{})\rangle \cong \boldsymbol{Z}_k \times \boldsymbol{Z}_4$; if four solutions exist we have $(\mathscr{W}\hat{})^k = (\mathscr{E})$ and $H(f) = \langle(\mathscr{W}\hat{})\rangle \times \langle(\mathscr{W}\hat{}\mathscr{Y}\hat{})\rangle \cong \boldsymbol{Z}_k \times \boldsymbol{Z}_k$. Thus

THEOREM 2. *Let* $\boldsymbol{Q}(\theta_1) = \boldsymbol{Q}(i)$ *and* k *be the maximal positive integer such that* $(w_1 - w_0\theta_2)^2 = g\zeta\sqrt[k]{\theta_1^2}$ *has a solution* $w_1, w_0, g \in \boldsymbol{Z}$ *and* ζ *a fourth root of unity. Then* $H(f)$ *is isomorphic to* $\boldsymbol{Z}_{4k}$ *if* k *is odd, to* $\boldsymbol{Z}_k \times \boldsymbol{Z}_4$ *if* $k = 2 \pmod 4$ *or if* $k = 0 \pmod 4$ *when* $(\mathscr{X}\hat{})^2 = (\mathscr{E})$ *has only two solutions in* $G(f)$ *and to* $\boldsymbol{Z}_k \times \boldsymbol{Z}_k$ *when* $k = 0 \pmod 4$ *and* $(\mathscr{X}\hat{})^2 = (\mathscr{E})$ *has four solutions in* $G(f)$.

Again the condition of the theorem implies that Q is a unit times a k-th power in $\boldsymbol{Z}$. Since $P^2 - 4Q$ is the negative of a square, the invariant $\Delta(\mathscr{E}) = -(P^2 - 4Q)$ is a square and so $(\mathscr{X}\hat{})^2 = (\mathscr{E})$ has four solutions in $G(f)$ only when Q is also a square in $\boldsymbol{Z}$ and then $G(f)$ has three elements of order two (see [1], 4.6).

Case 3. $\boldsymbol{Q}(\theta_1) = \boldsymbol{Q}(w)$. The equation $(w_1 - w_0\theta_2)^2 = ew$ has a solution $w_0, w_1, e \in \boldsymbol{Z}$; denote the resulting solution in $G(f)$ by $(\mathscr{Y})$. Then $(\mathscr{F})$, $(\mathscr{Y})$, $(\mathscr{Y})^2$, $(\mathscr{Y})^3$, $(\mathscr{Y})^4$, $(\mathscr{Y})^5$ are all distinct and $(\mathscr{Y})^6 = (\mathscr{F})$, Furthermore $(\mathscr{Y})^3 = (\mathscr{E})$; the equation $(\mathscr{X})^2 = (\mathscr{E})$ has no solution in $G(f)$ (since $-(P^2 - 4Q) = 3$ times a square in $\boldsymbol{Z}$ and so is not a square, and $-Q(P^2 - 4Q)$ cannot be a square in $\boldsymbol{Z}$ also). If $(\mathscr{W})$ is one solution in $G(f)$ derived from (1.5.1) with $\zeta = 1$, then all solutions derived from (1.5.1) for all ζ are $(\mathscr{W})$, $(\mathscr{W}\mathscr{Y})$, $(\mathscr{W}\mathscr{Y}^2)$, $(\mathscr{W}\mathscr{E})$, $(\mathscr{W}\mathscr{Y}\mathscr{E})$, $(\mathscr{W}\mathscr{Y}^2\mathscr{E})$. Among the solutions derived from (1.5.k) are $(\mathscr{W})^k$, $(\mathscr{W}\mathscr{Y})^k$, $(\mathscr{W}\mathscr{Y}^2)^k$, $(\mathscr{W}\mathscr{E})^k$, $(\mathscr{W}\mathscr{Y}\mathscr{E})^k$ and $(\mathscr{W}\mathscr{Y}^2\mathscr{E})^k$. If k is odd, then $(\mathscr{W})^k$ and $(\mathscr{W}\mathscr{E})^k$ provide the two distinct solutions obtained from (1.5.k) with $\zeta = 1$ and so at least one of them is $(\mathscr{F})$; say $(\mathscr{W})^k = (\mathscr{F})$, then $H(f) = \langle(\mathscr{W})\rangle \times \langle(\mathscr{Y})\rangle \cong \boldsymbol{Z}_k \times \boldsymbol{Z}_6$. If k is even, neither $(\mathscr{W})^k$ nor $(\mathscr{W}\mathscr{E})^k$ can be $(\mathscr{E})$ (since otherwise $(\mathscr{X})^2 = (\mathscr{E})$ would have a solution in $G(f)$) and so both must be $(\mathscr{F})$, Hence again $H(f) = \langle(\mathscr{W})\rangle \times \langle(\mathscr{Y})\rangle \cong \boldsymbol{Z}_k \times \boldsymbol{Z}_6$. Therefore

THEOREM 3. *Let* $\boldsymbol{Q}(\theta_1) = \boldsymbol{Q}(w)$ *and* k *be the maximal positive integer such that* $(w_1 - w_0\theta_2)^2 = g\zeta\sqrt[k]{\theta_1^2}$ *has a solution* $w_1, w_0, g \in \boldsymbol{Z}$ *and* ζ *a cube root of unity. Then* $H(f) \cong \boldsymbol{Z}_k \times \boldsymbol{Z}_6$.

2. **Prime divisors of elements of finite order.** At present the only known way to determine if a prime p, $(p, Q) = 1$, divides a general linear recurrence $\mathscr{W}$ is to examine any $p + 1$ consecutive terms of $\mathscr{W}$; p is a divisor of $\mathscr{W}$ if and only if it divides one of these terms. Such a characterization we shall call *local*. On the other hand every prime divides $(\mathscr{F})$ and a prime divides the element $(\mathscr{E})$ of order two in $G(f)$ if and only if its rank of apparition in $\mathscr{F}$ is even. M. Ward in [3] termed this a *global* characterization of the prime divisors of $(\mathscr{F})$ and $(\mathscr{E})$ and raised the question whether these are the only two recurrences (for a given companion polynomial $f(x)$, or in our terminology, in $G(f)$) for which the prime divisors can be so characterized. Here we show that there are other elements of finite order besides $(\mathscr{F})$ and $(\mathscr{E})$ where prime divisors can be globally characterized. Although we have not made an exhaustive study we suspect that there are other elements of finite order whose prime divisors are globally characterized. But it is not clear that every element of finite order has this property, for example, we know that an odd prime of odd rank of apparition in $\mathscr{F}$ is a divisor of one and only one of the two linear recurrences $(\mathscr{A})$, $(\mathscr{B})$ of order two in $G(f)$ (when they exist) but we cannot at present say which recurrence of the two such a prime divides. Nevertheless, we are tempted to conjecture that if an element of $G(f)$ has its prime

divisors globally characterized, then it is of finite order.

We consider the example of an element of order four considered previously; here $H(f) = \{(\mathscr{V}), (\mathscr{V})^2 = (\mathscr{E}), (\mathscr{V})^3 = (\mathscr{V}\mathscr{E}), (\mathscr{V})^4 = (\mathscr{J})\}$, where $\mathscr{V} = [5, -19]$ and $\mathscr{V}\mathscr{E} = [1, -35]$. Since both $(\mathscr{V})$ and $(\mathscr{V}\mathscr{E})$ generate $H(f)$ they have precisely the same prime divisors; by Theorem 4.3 of [1] there is a labelling of the terms of $\mathscr{V}$ and $\mathscr{W} = \mathscr{V}\mathscr{E}$, say v_n and w_n, such that $v_n w_n = de_{2n+k}$ for all $n \in \boldsymbol{Z}$, some $d \in \boldsymbol{Z}$ and $k = 0$ or 1. Comparing the first two products we see that $v_n w_n = -e_{2n+1}$, where $v_0 = 5$, $v_1 = -19$, $w_0 = 1$, $w_1 = -35$, $e_0 = 2$ and $e_1 = -5$. Since $i_{2n} = i_n e_n$ for nonnegative integers, where $\mathscr{J} = [0, 1]$, $i_0 = 0$, $i_1 = 1$ is the Lucas sequence of $G(f)$, it follows that the odd prime divisors of both $(\mathscr{V})$ and $(\mathscr{W})$ are precisely those of rank $4n + 2$, $n = 0, 1, \cdots$. Thus the prime divisors of $(\mathscr{V})$ and $(\mathscr{V}\mathscr{E})$ have been characterized globally.

Now consider the group $G(f)$, where $f(x) = x^2 - 5x + 7$. The group has two elements $(\mathscr{V}) = ([1, 3])$ and $(W) = (V^2) = ([1, 2])$ of order three. Since these two elements generate the same subgroup of $G(f)$ they have the same prime divisors. If we put $v_0 = 1$, $v_1 = 3$, $w_0 = 1$, $w_1 = 2$, $i_0 = 0$, $i_1 = 1$, then we deduce that $3v_n w_n i_n = i_{3n}$ for all n and consequently it follows that the prime divisors of $(\mathscr{V})$ are precisely those of rank $3n$, $n = 1, 2, \cdots$. Again the prime divisors of $(\mathscr{V})$ and $(\mathscr{V})^2$ have been characterized globally.

Both these examples admit of some generalization.

3. Elements which are locally finite everywhere. To say that an element $(\mathscr{W})$ of $G(f)$ is locally finite everywhere means that $(\mathscr{W})$ is of finite order modulo $G(f, p)$ for all primes p, i.e., $(\mathscr{W}) \in H(f, p)$ for all p (see after Corollary 3.4.1 of [1]). Now $H(f, p) \supseteq K(f, p)$ with equality for all p, which are coprime to $Q(P^2 - 4Q)$. Here we discuss only the case when $Q = \pm 1$. Then $(\mathscr{W}) \in K(f) = \bigcap_p K(f, p)$ if and only if the *reduced* elements of (W) have invariant ± 1. It can be shown that $\Delta(\mathscr{W}) = \pm 1$ implies $(\mathscr{W}) = (I)$ except in the following two situations: when $f(x) = x^2 - 3x + 1$ with $\mathscr{W} = [1, 1]$ and $f(x) = x^2 + 3x + 1$ with $\mathscr{W} = [-1, 1]$. Referring to the remark after Theorem 4.4 of [1], we see that both these exceptional sequences are of order two; $K(x^2 - 3x + 1) = ((\mathscr{B}))$, $K(x^2 + 3x + 1) = ((\mathscr{A}))$ and $K(x^2 - Px \pm 1) = ((\mathscr{J}))$ in all other cases. Now if $(\mathscr{W}) \in \bigcap_p H(f, p)$, when $(\mathscr{W})^k \in K(f)$ for some $K \in \boldsymbol{Z}$ and so we may conclude by means of Theorem 3.7 of [1] that the elements which are locally finite everywhere are precisely the elements of finite order in $G(f)$.

REMARKS. (a) The sequence $\mathscr{B}$ given above is a sequence of alternate terms of the Fibonacci sequence, the sequence $\mathscr{A}$ is similarly

related apart from signs, and the two exceptional groups $G(x^2 - 3x + 1)$ and $G(x^2 + 3x + 1)$ are isomorphic.

(b) If Q is not a unit the situation is quite different. To begin with things are complicated by the fact that one cannot use reduced elements alone in discussing the subgroup K. The above result that an element which is locally finite everywhere is of finite order is not true in general.

(c) We can generalize a result of A. Schinzel given in [2] to show that if $(\mathscr{W}) \in G(f, p)$ for all primes p with at most a finite number of exceptions, then $(\mathscr{W}) = (\mathscr{S})$.

REFERENCES

1. R. R. Laxton, *On groups of linear recurrences, I*, Duke Math. J. (forthcoming article)

2. A. Schinzel, *On the congruence* $a^x \equiv b \pmod{p}$, Polonaise des Sciences, Serie des Sci. Math., Astr. et Phys. **8** (1960), 307-309.

3. M. Ward, *The prime divisors of Fibonacci numbers*, Pacific J. Math. **11** (1961), 379-386.

Received December 11, 1968, and in revised form July 22, 1969.

UNIVERSITY OF NOTTINGHAM