ROCKY MOUNTAIN
JOURNAL OF MATHEMATICS
Volume 41, Number 4, 2011

DEGREE k LINEAR RECURSIONS mod (p) AND NUMBER FIELDS

T. MACHENRY AND KIEH WONG

ABSTRACT. Linear recursions of degree k are determined by evaluating the sequence of generalized Fibonacci polynomials, $\{F_{k,n}(t_1, \dots, t_k)\}$ (isobaric reflects of the complete symmetric polynomials) at the integer vectors $(t_1, \dots, t_k)$. If $F_{k,n}(t_1, \dots, t_k) = f_n$, then

$$f_n - \sum_{j=1}^{k} t_j f_{n-j} = 0,$$

and $\{f_n\}$ is a linear recursion of degree k. On the one hand, the periodic properties of such sequences modulo a prime p are discussed and are shown to be related to the prime structure of certain algebraic number fields; for example, the arithmetic properties of the period are shown to characterize ramification of primes in an extension field. On the other hand, the structure of the semi-local rings associated with the number field is shown to be completely determined by Schur-hook polynomials.

1. Introduction. A sequence $\{f_n\}$ is a *linear recursion of degree* k, denoted by $[t_1, \dots, t_k]$, if, given a sequence of integers $t_1, \dots, t_k$, the following equation is satisfied for all $n \in \mathbf{Z}$:

$$f_n - \sum_{j=1}^{k} t_j f_{n-j} = 0. \tag{1.1}$$

In this paper we shall discuss the periodic nature of such sequences and the periodic nature of such sequences modulo primes. In particular, we characterize those k-linear sequences which are periodic, and those which are periodic modulo a prime. While we believe that these

Keywords and phrases. Symmetric polynomials, Schur polynomials, linear recursions, number fields.
Received by the editors on May 9, 2007, and in revised form on November 6, 2008.
DOI:10.1216/RMJ-2011-41-4-1303

results are new and interesting, it is the setting that they occur in and the applications of these results that we are most interested in. The setting in question is that of the ring of symmetric polynomials, and the applications are to the theory of algebraic number fields on the one hand and to the theory of multiplicative arithmetic functions on the other. It is the first of these applications, the number fields, that will be emphasized in this paper, while the second, the multiplicative arithmetic functions, will be discussed in more detail in a paper to follow shortly.

In Macdonald [**13**], MacHenry [**14, 15**] and MacHenry and Tudose [**16**], the notion of isobaric polynomials was introduced, or rather reintroduced. These are just the symmetric functions written in the elementary symmetric polynomial (ESP) basis. Historically, interest in symmetric polynomials arose because of the relation between the roots of a (say, monic) polynomial and its coefficients (for example, see [**5**]). If, for example, we take our monic polynomial to be

$$X^k - t_1 X^{k-1} - \cdots - t_k$$

with roots

$$\lambda_1, \ldots, \lambda_k,$$

then it is the classical result that the t_j are, up to sign, the ESPs of the λ_i. Regarding the λ_i as indeterminates, the k-degree symmetric polynomials are those polynomials on the λ_i's, which are invariant under the action of the symmetric group of degree k acting on the generators. When we rewrite the symmetric functions in the ESP basis (e.g., see [**13**]), we see that the form of the polynomials no longer emphasizes the symmetry of the generators, but rather it is the partitions of the natural numbers which comes to the fore. After the mapping

$$t_j = (-1)^{j+1}\mathcal{E}_j,$$

where $\mathcal{E}_j$ is the j-th elementary symmetric polynomial in k variables, an *isobaric* polynomial looks like this:

$$P_{k,n} = \sum_{\alpha \vdash n} C_\alpha t_1^{\alpha_1} \ldots t_k^{\alpha_k}$$

where $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_k)$ is an integer vector with $\sum_{j=1}^{k} j\alpha_j = n$; that is, $(1^{\alpha_1}, \ldots, k^{\alpha_k})$ is a partition of n into parts with α_j j's. We shall

say that a symmetric polynomial written in this way, emphasizing the partitions of the integers, has *isobaric degree* n. It can be thought of as a polynomial whose variables are Young diagrams (e.g., see Li [**12**]), or more accurately, the Young diagrams representing partitions of n into parts not larger than k. Note that the coefficients C_α are integers.

Of special interest to us in this paper are the sequences of isobaric polynomials which form linear recursions, that is, sequences for which, given the variables $\mathbf{t} = (t_1, \ldots, t_k)$, we have for each k a sequence of polynomials $\{P_{k,n}\}$ for which

$$P_{k,n} = t_1 P_{k,n-1} + \cdots + t_k P_{k.n-k}.$$

The mapping from the λ-basis to the ESP basis is a ring isomorphism, that is, we can speak of the (k-graded) ring of isobaric polynomials. Letting $t_j = 0$ for $j > k$ yields a projection of the ring onto the k-th level of the grading.

It is proved in [**14**] that such sequences form a free k-graded $\mathbf{Z}$-module with a basis consisting of Schur-hook polynomials (also see [**16**]). In [**15**] this was called the module of *Weighted Isobaric Polynomials* or the WIP-module. It can be thought of as a module of polynomials but is best considered as a module of sequences of polynomials. In Section 3, we suggest a way of looking at this module which is both intuitively transparent and algebraically very useful. But first we discuss two especially important sequences in this setting. They are the generalized Fibonacci sequence (GFP), and the generalized Lucas sequence (GLP) [**14**]. In the λ-basis, they are better known as the sequence of Complete Symmetric Polynomials, and the sequence of Power Symmetric Polynomials.

In the isobaric basis the GFPs are of the form,

$$F_{k,n} = \sum_{\alpha \vdash n} \binom{|\alpha|}{\alpha_1 \ldots \quad \alpha_k} t_1^{\alpha_1} \ldots t_k^{\alpha_k},$$

where $\alpha = (\alpha_1, \ldots, \alpha_k)$, $|\alpha| = \sum_{j=1,\ldots,k} \alpha_j$; and the GLPs, of the form

$$G_{k,n} = \sum_{\alpha \vdash n} \frac{n}{|\alpha|} \binom{|\alpha|}{\alpha_1 \ldots \quad \alpha_k} t_1^{\alpha_1} \ldots t_k^{\alpha_k}.$$

In general, a weighted isobaric polynomial (or WIP-polynomial) is given by the expression:

$$P_{\omega,k,n} = \sum_{\alpha \vdash n} \binom{|\alpha|}{\alpha_1, \dots, \alpha_k} \frac{\sum_j^k \alpha_j \omega_j}{|\alpha|} t_1^{\alpha_1} \dots t_k^{\alpha_k},$$

where $\boldsymbol{\omega} = (\omega_1, \dots, \omega_k)$ is a *weight* vector. Each weight vector determines a k-linear recursion [**14**]. The weight vectors for the generalized Fibonacci sequence and the generalized Lukas sequence are given, respectively, by $\boldsymbol{\omega} = (1, 1, \dots, 1, \dots)$, and by $\boldsymbol{\omega} = (1, 2, \dots, n, \dots)$. It is straightforward to check that $P_{\omega,k,n}$ is a k-linear recursive sequence of isobaric polynomials for each ω and k. And, that we can add two weighted sequences in the WIP-module by adding their weight vectors, thus realizing the abelian group structure of the module and emphasizing that the preferred basic element of the module is a sequence.

For each k we call any weighted sequence of isobaric polynomials a *generic* k-linear recursive sequence, allowing the application of an evaluation map to the indeterminates. The WIP-module, and, indeed, the entire ring of $k-$isobaric polynomials $P_{k,n}$, is determined implicitly by the $k-$degree monic polynomial

$$\mathcal{C}(X) = X^k - t_1 X^{k-1} - \dots - t_k = X^k - \sum_{j=1}^{k} t_j X^{k-j}$$

by virtue of the two fundamental theorems of symmetric functions alluded to above, and the change of basis. Therefore, we call this polynomial

$$\mathcal{C}(X) = X^k - \sum_{j=1}^{k} t_j X^{k-j},$$

the *core polynomial*. Thus given the core polynomial, the whole isobaric structure falls into place. But the core polynomial itself is uniquely given once we have assigned the generic variables $t_1, \dots, t_k$, so we find it convenient to use the notation $[t_1, \dots, t_k]$ to denote the core polynomial. Since we can take k to be arbitrarily large, it is also convenient to give power series the honorary status of core polynomial (with some adjustment necessary to the bracket notation).

These remarks will be more effective when we look not just at the generic core, but also consider evaluation maps on the **t**-vectors, that is, when we look at polynomials of degree k with numerical coefficients. (In Section 3, the unity of these ideas will become especially transparent).

Suppose we choose to evaluate the indeterminates **t** in the ring of integers; then each sequence $\{P_{\omega,k,n}(\mathbf{t})\}$ gives a numerical k-degree linear recursion; and since, in particular, **t** is given, the core is uniquely determined. Moreover, every k-degree linear recursion can be realized in this way. The contents of Section 3 will suggest that choosing to use the GFP as our generic sequence has a great deal of merit. This sequence contains the polynomials

(1) $F_{k,0} = 1$

(2) $F_{k,1} = t_1$

(3) $F_{k,2} = t_1^2 + t_2$

(4) $F_{k,3} = t_1^3 + 2t_1t_2 + t_3$

(5) $F_{k,4} = t_1^3 + 3t_1^2t_2 + t_2^2 + 2t_1t_3 + t_4$

(6) etc.

of isobaric degrees $0, 1, 2, 3, 4, \ldots$.

If we let $k = 2$, that is, use the projection $t_j = 0$ for $j > 2$, and let $[t_1, t_2] = [1, 1]$, we find that the sequence $\{F_{2,n}\}$ is just the Fibonacci sequence. A similar exercise for the GLPs yields the Lucas sequence. In either case, the core polynomial is $X^2 - X - 1$. However, once a core polynomial is chosen, given k and the generic linear recursion, all is determined. So in particular, if we choose a generic k-linear recursion, then for each evaluation of the **t**-vector, exactly one core polynomial is selected. In this way, we get a one-to-one relation between k-cores and all numerical linear recursions. (See Section 4).

A sequence $\{f_n\}$ is periodic if there is a positive integer c such that, for all n, $f_{n+c} = f_n$. The first two questions we ask, then, are:

(1) Which numerical linear recursions are periodic?

While this question is not difficult to answer, its answer seems not to appear in the literature.

(2) What is the length of a period of a numerical linear recursion mod (p)? (see [**6**, Chapter 3]).

(At the end of this paper, we include a Maple algorithm, due to Professor Mike Zabrocki of York University, for computing a tight bound for the period of any k-order linear recursion modulo a prime p.)

2. Periodic linear recursions. We now answer the two questions asked in Section 1, reminding the reader that the generic recursion that we are using is the GFP sequence.

Theorem 2.1. *A linear recursion is periodic if and only if every root of the core polynomial is a complex root of unity. In particular, if the core polynomial is the cyclotomic polynomial $CP(n)$ of degree $\phi(n)$, where ϕ is the Euler totient function. Then its associated linear recursion is periodic with period n, see* [**16**]. (*It is interesting to compare this theorem with the Lech-Mahler theorem, see* [**1**].)

The proof will be discussed in Section 3.

Denote the period, either $\mathrm{mod}\,(p)$ or $\mathrm{mod}\,(1)$, of a linear recursion induced by $[t_1, \ldots, t_k]$ by $c_p[t_1, \ldots, t_k]$ where p is either a rational prime or $p = 1$, and the t_j are the coefficients of the core polynomial.

Theorem 2.2 (Evarest, van Poorten, Shparlinski, Ward [**6**, page 46, Theorem 3.1]). *Every linear recursion is periodic modulo p for every rational prime p. The p-period of a linear recursion induced by $[t_1, \ldots, t_k]$ satisfies $c_p[\mathbf{t}] \leqslant p^k$.*

This follows from simple combinatorial arguments, essentially the pigeonhole principle. We improve this bound to a best bound, $p^k - 1$, in Section 4. We observe that if a sequence is a periodic linear recursion, then

$$F_{k,c_p} = F_{c_p} = 1, F_{c_p-1} = \cdots = F_{c_p-k+1} = 0, F_{c_p+1} = t_1.$$

While there is nothing deep about the proofs of these two theorems, it is of some interest that they occur within the confines of the ring of symmetric functions and become obvious when this particular basis is chosen. However, the particular techniques for studying recursions and

periodic recursions reveal an even deeper connection with symmetric functions framed in the language of isobaric polynomials, which in turn points to a strong connection with combinatorial algebra. In the next section we discuss some not so well-known "well-known" results, and add some new information which we believe not to be well-known. We now discuss our most important tool; namely, the companion matrix of the core polynomial and a rather remarkable structure induced by it.

3. The companion matrix of the core polynomial. With each core polynomial, we associate its rational canonical matrix, the so-called *companion matrix* (for example, see [**6**]). We first consider the companion matrix for the generic core polynomial of degree k.

$$\mathbf{A} = \begin{pmatrix} 0 & 1 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 1 \\ \cdots & \cdots & \cdots & \cdots \\ t_k & t_{k-1} & \cdots & t_1 \end{pmatrix}.$$

Since $\det \mathbf{A} = (-1)^{k+1} t_k$, $\det \mathbf{A^n} = (-1)^{n(k+1)} t_k^n$, $\mathbf{A}$ is singular if and only if $t_k = 0$. But, if $t_k = 0$, the core polynomial is reducible; so we assume $\mathbf{A}$ to be nonsingular. Thus, $\mathbf{A}$ is invertible and generates a cyclic group (finite, if the coefficients of the core polynomial satisfy the conditions of Theorem 2.1; otherwise, infinite). The inverse of $\mathbf{A}$ is

$$\mathbf{A}^{-1} = \begin{pmatrix} -t_{k-1}t_k^{-1} & -t_{k-2}t_k^{-1} & \cdots & t_1 t_k^{-1} & t_k^{-1} \\ 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & 1 & 0 \end{pmatrix}.$$

We record the orbit of the k-th row vector of $\mathbf{A}$ under the action of $\mathbf{A}$, below $\mathbf{A}$, and the orbit of the first row of $\mathbf{A}$ under the action of $\mathbf{A}^{-1}$ on the first row of $\mathbf{A}$ is recorded above $\mathbf{A}$, and consider the $\infty \times k$ matrix whose row vectors are the elements of the doubly infinite orbit of $\mathbf{A}$ acting on any one of them. For $k = 3$, $\mathbf{A}^\infty$ looks like this (we explain

the symbols for the elements below):

$$\mathbf{A}^{\infty} = \begin{pmatrix} \cdots & \cdots & \cdots \\ S_{(-n,1^2)} & -S_{(-n,1)} & S_{(-n)} \\ \cdots & \cdots & \cdots \\ S_{(-3,1^2)} & -S_{(-3,1)} & S_{(-3)} \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ t_3 & t_2 & t_1 \\ \cdots & \cdots & \cdots \\ S_{(n-2,1^2)} & -S_{(n-2,1)} & S_{(n-2)} \\ S_{(n-1,1^2)} & -S_{(n-1,1)} & S_{(n-1)} \\ S_{(n,1^2)} & -S_{(n,1)} & S_{(n)} \\ \cdots & \cdots & \cdots \end{pmatrix}_{\infty\times 3}.$$

This matrix has a number of important features which we summarize in

Theorem 3.1 (cf. [**2, 3, 7, 9, 10**]). (i) *The row vectors consist of the orbit of any row with* $\mathbf{A}$ *acting as a transformation matrix* (*on the right, say*), *and the components of the row vectors are just isobaric reflects of Schur-hook polynomials.*

(ii) *The set of* $k \times k$ *contiguous row vectors of* $\mathbf{A}^{\infty}$, *with the entry in the lower righthand corner being the Schur-hook function* $\mathbf{S}_{(n)}$, *yields a* (*faithful*) *matrix representation of the cyclic group generated by* $\mathbf{A}$:

$$\mathbf{A}^n = \begin{pmatrix} (-1)^{k-1}S_{(n-k+1,1^{k-1})} & \cdots & (-1)^{k-j}S_{(n-k+1,1^{k-j})} & \cdots & S_{(n-k+1)} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ (-1)^{k-1}S_{(n,1^{k-1})} & \cdots & (-1)^{k-j}S_{(n,1^{k-j})} & \cdots & S_{(n)} \end{pmatrix}.$$

Or, more succinctly, we have

$$\mathbf{A}^n = [(-1)^{k-j}S_{(i,1^{k-j})}]_{k\times k},$$

where the entries are isobaric Schur-hook reflects whose Young diagrams have arm length i *and leg length* $k-j$ *in the case of positive* n.

(iii) *The elements in each row of* $\mathbf{A}^{\infty}$ *are the coefficients of a representation of the powers* (*positive and negative*) *of any of the roots of*

the core polynomial–denoted by λ^n–in terms of a basis consisting of the first $k-1$ powers of λ:

$$\lambda^{n+k-1} = \sum_{j=0}^{k-1} (-1)^{k-j-1} S_{(n,1^{k-j-1})} \lambda^j$$

for $n \in \mathbf{Z}$, where λ is a root of the core polynomial (and, as remarked above, the coefficients are Schur-hook reflects whose Young diagrams have arm length n and leg length $k-j$ when n is positive).

(iv) *Each column of $\mathbf{A}^\infty$ is a $\mathbf{k}$-degree linear recursion of Schur-hook polynomials induced by the core polynomial $[t_1, \ldots, t_k]$. In particular, the righthand column is just the (doubly infinite) sequence of generalized Fibonacci polynomials, $\mathbf{F_{k,n}}$, see* [**6**, 1.1.12].

(v) $\operatorname{tr}(\mathbf{A^n}) = \mathbf{G_{k,n}(t)}$ *for $n \in \mathbf{Z}$, where $\mathbf{G_{k,n}}$ is just the sequence of generalized Lucas polynomials, which is also a $\mathbf{t}$-linear recursion.*

Remark. Since we have assumed that, in the core polynomial $t_k \neq 0$, the matrix $\mathbf{A}$ is invertible, and since $\mathbf{A}^\infty$ is generated by $\mathbf{A}$, $\mathbf{A}^\infty$ extends the sequences of Schur-hook polynomials (in particular, the GFP, as well as the GLP) northward to negatively indexed terms, see [**6**, 1.1.3]. It is reasonable to call the negatively indexed entries in the matrix Schur-hook polynomials also. In fact, they can be represented as quotients of two positively-indexed Schur polynomials, which in general are not hooks. It would be interesting to have a combinatorial interpretation of these negatively indexed functions. One might compare this result with the theorem in MacHenry, [**15**], which gives rational convolution roots to all of the elements in the WIP-module (also see [**17**]), i.e., to all of the sequences of symmetric functions in the free $\mathbf{Z}$-module generated by the Schur-hook polynomials.

Proof of Theorem 3.1. (i) The orbit structure is a consequence of the construction of the matrix. The operation of the companion matrix on a k-vector of integers generates a linear recursion with respect to the vector $\mathbf{t}$. They are, in fact, the Schur-hook sequences claimed in the theorem [**16**].

(ii) follows from the arguments in (i).

(iii) follows from the Hamilton-Cayley theorem. A simple induction shows that these coefficients are just the stated Schur-hook functions of the theorem.

(iv) This is discussed in (i).

(v) The traces of the $k \times k$-blocks are the sums of all of the Schur-hook reflects whose Young diagrams partition the same n; but such sums of Schur-hooks are well known to be GLP of isobaric degree n [**16**]. □

The infinite companion matrix is a remarkable summary of all of the features connected with linear recursions (as enumerated in Theorem 3.1). The righthand column consists of GFPs, i.e., the generic kth order linear recursions; it displays the role of Schur-hook functions as both constituents of sequences of kth order linear recursions, one of which is the GFP sequence, and as coefficients for a representation of the powers of the roots of the core polynomial. It contains a matrix representation of the free abelian group generated by the companion matrix, in particular, a matrix representation of the free abelian group generated by any of the roots of the core. It also contains, as traces, the GLPs. Recall that the GFPs and the GLPs are respectively, isobaric versions of the complete symmetric polynomials and the power symmetric polynomials. With this we have shown a connection between the theory of linear recursion and an important submodule of the algebra of symmetric polynomials, the WIP-module. Moreover, we have introduced an extension of the symmetric polynomials to negatively indexed symmetric functions which are related to the reciprocals of powers of the roots of the core polynomial. Thus, we have a striking summary of the connection between the theory of equations and the theory of linear recursions within the ring of symmetric polynomials. We note that, while many of these properties of the extended companion matrix are known to Lascoux and his students (see Chen and Louk [**4**], also see [**6, 9**]), the role of the GFPs and the GLPs, as well as the form of the negative entries, may not be so well known. This matrix will be a useful and important tool in what follows.

Before we state the next result, we must clarify the following point. A linear recursion is specified when (1) the recursion degree and recursion relation are given, and (2) when the initial conditions are also given.

In our case the recursion relation and degree are given when the vector $(t_1, \ldots, t_k)$ is specified, by (1.1). As for (2), we first note that every column of $\mathbf{A}^\infty$ is a linear recursion as a result of the fact that the rows of $\mathbf{A}^\infty$ are the orbits of any row of the companion matrix under the actions of the companion matrix on its rows (righthand or lefthand action), generating an infinite cyclic group. That is, the cyclic action of the companion group is equivalent to columns being linear recursions (of degree k for some fixed k). Since we assume that A is nonsingular, i.e., that $t_k \neq 0$, the recursion goes in both directions (northward as well as southward). The identity matrix is "embedded" in the companion matrix, and we can start the recursion going (in either direction) by letting the columns of the identity matrix be the initial conditions for the column containing it. Since the core polynomial (with a nonzero constant term) uniquely determines $\mathbf{A}^\infty$, each column is uniquely specified as a k-degree recurrence sequence with specified initial conditions. Since the degree k infinite companion matrix is a projection of the degree $k+1$ infinite companion matrix, it is clear how to specify recursions of infinite degree.

Corollary 3.2. *Let $[t_1, \ldots, t_k]$, $t_j \in \mathbf{Z}$, be an irreducible core polynomial with companion matrix $\mathbf{A}$, and denote the cyclic group generated by $\mathbf{A}$ as $\mathbf{H}$. Let $\mathbf{A_p}, \mathbf{A_p^\infty}$ and $\mathbf{H_p}$ denote $\mathbf{A}, \mathbf{A}^\infty$ and $\mathbf{H}$ with elements reduced modulo p. Then $\mathbf{H_p}$ is a finite cyclic group exactly when the columns of $\mathbf{A_p^\infty}$ are periodic linear recursions. The length of the period of each of the column sequences is equal to the order of the cyclic group $\mathbf{H_p}$, which is $\leqslant (p^k - 1)$. Moreover, every root of the core polynomial generates a finite cyclic group whose order is just the order of $\mathbf{H_p}$.*

Proof. That the columns of $\mathbf{A}^\infty$ are linear recursions is justified by Theorem 3.1 (iv), so the effective part of the assumption is that the columns of $\mathbf{A_p^\infty}$ are periodic. Clearly, if $\mathbf{H_p}$ is periodic, then so is each of its columns. On the other hand, since, by Theorems 1.1 and 3.1 in [**6**], these columns (having the same core polynomial) have the same period length, thus $\mathbf{H_p}$ is finite with order the period length of any of the columns of $\mathbf{A_p^\infty}$. That the roots of the irreducible core polynomial when taken modulo p generate a finite cyclic group of order equal to the order of $\mathbf{H_p}$ follows from Theorem 3.1 (iii). □

Remark. Let ${}_1\mathbf{C}, {}_2\mathbf{C}, \ldots, {}_k\mathbf{C}$ denote the columns of $\mathbf{A}_\mathbf{p}^\infty$. Then it is easy to show that a column can be added row-wise to a another column shifted column-wise and yield a sequence which is periodic modulo p, with the same period length as either of the summands. Thus,

$$\sum_{\mathbf{j=1}}^{\mathbf{k}} \mathbf{a_{jj}C_{k,n+i_j}}$$

has the same core polynomial as any of its summands and so is a periodic sequence with same period length as any column. These are just the elements of the WIP-module. In [**16**, Theorems 3.1 and 3.4] it is shown that the elements of the WIP-module are the only possible linearly recursive sequences of symmetric polynomials.

Applying the facts learned above about the companion matrix, we now consider the periodic behavior of linear recursions modulo a prime p.

4. p-periodicity and the companion matrix. We use the notation $[t_1, \ldots, t_k]_p$ to indicate the core polynomial with coefficients taken modulo (p), and, as mentioned above, c_p and $c_p[t_1, \ldots, t_k]$ to denote the period of $\mathbf{A}$ with entries taken modulo (p), which, in turn, we write as $\mathbf{A_p}$. For any matrix $\mathbf{M}$, $\operatorname{tr}\mathbf{M}$ denotes the trace of the $\mathbf{M}$.

Theorem 4.1. (i) $c_p[\mathbf{t}] = c_p[t_1, \ldots, t_k] \leq p^k - 1$.

(ii) *The (cyclic) group generated by* $\mathbf{A_p}$ ($\mathbf{H_p}$) *has order* $c_p[\mathbf{t}]$.

(iii) *The columns of* $\mathbf{A}_\mathbf{p}^\infty$ *have periods dividing* $c_p[\mathbf{t}]$*; and the least common multiple of the periods of the columns of* $\mathbf{A}_\mathbf{p}^\infty$ *is* $c_p[\mathbf{t}]$.

(iv) $\lambda^{c_p}[\mathbf{t}] =_p 1$, *where* λ *is a root of* $\mathcal{C}(X)[\mathbf{t}]$, *and* $c_p[\mathbf{t}]$ *is the least positive integer for which this is true*; *i.e.,* $c_p[\mathbf{t}]$ *is the p-order of* λ.

(v) $\operatorname{tr}\mathbf{A}_\mathbf{p}^\mathbf{n}$ *is linearly recursive with period* $\leqslant c_p[\mathbf{t}]$.

Proof of Theorem 4.1. (i) is a consequence of Corollary 3.2. Clearly $\mathbf{A_p}$ generates a cyclic group of order dividing c_p; on the other hand, since each of the columns of $\mathbf{A}^\infty$ is a linear recursion, and since they generate $\mathbf{H}$, the l.c.m. of their periods must be c_p (also see [**19**]).

(iv) is a direct consequence of Theorem 3.1 (iii), 3.1 (iv) and Theorem 4.1 (iii).

(v) is a consequence of Theorem 3.1 (v). □

Remarks. As pointed out above, Corollary 3.2 accounts for the truth of Theorem 2.1. The core polynomials for the primitive nth roots of unity are the cyclotomic polynomials of degree $\phi(n)$, whose roots have the obvious geometric period of n; that is, $c_p[\mathbf{t}] = n$, where $\mathbf{t}$ is the appropriate vector of coefficients of the cyclotomic polynomial of degree $\phi(n)$. This also affords a geometric interpretation of periodicity for the roots of the core polynomial in the plane of complex numbers with coordinates taken (mod p), which is analogous to the cyclotomic periodicity.

The example of the Fibonacci sequence and the trace sequence associated with its infinite companion matrix shows that Theorem 4.1 (v) cannot be improved: $c_5[1, 1] = 20$ while the period of the sequence $G_{2,n}$ is 8.

5. The number field $\mathfrak{O}[\mathbf{t}]$ and the semi-local ring $\mathfrak{O}_{\mathbf{p}}[\mathbf{t}]$. We are now in a position to give an interesting application of these ideas to algebraic number fields. For this purpose we take the core polynomial to be irreducible and consider the number field $\mathcal{F} = \mathbf{Q}(\lambda) = \mathbf{Q}[X]/\mathrm{id}\langle\mathcal{C}(X)\rangle$. Let us denote the ring of integers (the maximal order) in this field by $\mathfrak{O}[\mathbf{t}]$, and we write $\mathfrak{O}[\mathbf{t}] \otimes \mathbf{Z_p} = \mathfrak{O}_{\mathbf{p}}[\mathbf{t}]$. We can write the elements of the field $\mathcal{F}$ either as a module over the basis $\{1, \lambda, \ldots, \lambda^{k-1}\}$, or uniquely as k-tuples $(m_0, \ldots, m_{k-1})$ with entries from $\mathbf{Q}$ with multiplication determined by the minimal polynomial of the field or, as a result of the Hamilton-Cayley theorem, as a module with the basis $\{\mathbf{I}, \mathbf{A}, \ldots, \mathbf{A^{k-1}}\}$. This gives a matrix representation of the elements in the field. Call it the *standard* representation. We also have the same three options in $\mathfrak{O}_{\mathbf{p}}[\mathbf{t}]$, using these bases modulo (p). Theorem 3.1 (iii) can be regarded as giving a representation of the powers of λ in $\mathcal{F}$, as polynomials in the integral λ-basis where the coefficients are Schur-hook polynomials evaluated at $[\mathbf{t}]$. Note that we have an induced *standard* matrix representation in the ring $\mathfrak{O}_{\mathbf{p}}[\mathbf{t}]$.

One of the concerns of the theory of algebraic number fields is the relation between primes in the extension field $\mathcal{F}$ and the rational primes

in $\mathbf{Z}$ that they sit over. If we let p be a rational prime generating the prime ideal $\mathbf{p}$ in $\mathbf{Q}$ and let $\mathcal{P}$ be the ideal in $\mathfrak{O}[\mathbf{t}]$ extending $\mathbf{p}$, then $\mathcal{P} = \mathcal{P}_1^{\varepsilon_1} \dots \mathcal{P}_s^{\varepsilon_s}$ is the prime decomposition of $\mathcal{P}$ in the Dedekind ring $\mathfrak{O}[\mathbf{t}]$. If f_j is the relative degree of the prime ideal $\mathcal{P}_j$, i.e., the degree of its minimal polynomial, then either $s = 1$ and $\varepsilon_1 = 1$, in which case $\mathcal{P}$ is a prime ideal and p is *inert*; or, $s > 1$ but $\varepsilon_j = 1$ for all j's, in which case $\mathcal{P}$ is the product of distinct prime ideals and p *splits*; or, some $\varepsilon_j > 1$ and p *ramifies*. These properties are reflected in the semi-local ring $\mathfrak{O}_p[\mathbf{t}]$. Moreover, there is a relation between the phenomenon of periodicity of the linear recursion associated with the core polynomial and properties of the primes in the extensions of the core localized at p. This will be discussed in the following sections. It is well known that for each irreducible core polynomial only a finite number of primes ramify; when they do, they divide the discriminant of the field. With few exceptions, the converse is also true, and those exceptions will not occur in our discussion (see, for example, Janusz [**8**]); hence, for the purposes of this paper, p ramifies if and only if $p|\Delta$, where Δ is the discriminant of $\mathcal{F}$. We shall want to use the following well-known fact.

Proposition 5.1 (see [**8**]).

$$\Delta = (-1)^{k(k-1)/2}\mathbf{N}(\mathcal{C}(X))\det \mathcal{C}'(\mathbf{t}).$$

$\mathcal{C}'(\mathbf{t})$ is the derivative of the core polynomial, that is, the *different*.

Noting that $\mathcal{C}'(\mathbf{t})$ can be regarded as an element of $\mathfrak{O}_{\mathbf{p}}[\mathbf{t}]$, and, denoting $\mathcal{C}'(\mathbf{t})$ by $\mathbf{D}[\mathbf{t}]$, we have

Corollary 5.2. $\mathbf{D}_{\mathbf{p}}[\mathbf{t}]$ *generates an ideal in* $\mathfrak{O}_{\mathbf{p}}[\mathbf{t}]$ (*the discriminant ideal*) *if and only if* $p|\Delta$, *that is, if and only if* p *ramifies in* $\mathfrak{O}[\mathbf{t}]$.

Proof. p divides the discriminant of the core polynomial modulo p if and only if p ramifies, which occurs if and only if the different vanishes modulo p at a root of the core polynomial, and this happens if and only if the different generates an ideal in the semi-local ring $\mathfrak{O}_{\mathbf{p}}[\mathbf{t}]$ (the alternative being that the different is a unit in $\mathfrak{O}_{\mathbf{p}}[\mathbf{t}]$). □

In keeping with the notation $\mathbf{A}^{\infty}[\mathbf{t}]$, we let $\mathbf{M}^{\infty}[\mathbf{t}]$ be the $\mathbf{H_p}[\mathbf{t}]$-orbit of any row vector in the matrix $\mathbf{M}[\mathbf{t}]$. Since, by construction, the columns of a standard matrix are $\mathbf{t}$-linear recursions, the following proposition can be proved by induction.

Proposition 5.3. *The righthand column of* $\mathbf{D}^{\infty}[\mathbf{t}]$ *is the sequence of* GLPs; *that is, the righthand column of* $\mathbf{D}^{\infty}[\mathbf{t}]$ *is a list of the traces of the matrices representing* $\mathbf{A^n}[\mathbf{t}]$; *thus, the righthand column of the matrix consists of the terms of the* GLP*-sequence, cf.* (3.15).

Proof. If the core polynomial is $X^k - \sum_{j=1}^{k} t_j X^{k-j}$, then the different $\mathbf{D}$ is the polynomial $\mathbf{D}[\mathbf{t}] = kX^{k-1} - \sum_{j=1}^{k-1} t_j(k-j)X^{k-j-1}$. This is represented by the vector $(-t_{k-1}, \ldots, -(k-1)t_1, k)$ in $\mathfrak{O}[\mathbf{t}]$, and the orbit of this vector under the action of the companion matrix of the core polynomial gives the standard matrix representation. Since acting on a vector in $\mathfrak{O}[\mathbf{t}]$ by $\mathbf{A}[\mathbf{t}]$ automatically generates linearly recursive columns determined by $[t_1, \ldots, t_k]$, it is necessary only to notice that the element in the upper righthand corner of the matrix representing $\mathbf{D}[\mathbf{t}]$ is k. Induction does the rest. □

Remark. There is an interesting connection between the GFP-sequence and the GLP-sequence; namely, they are related by partial differentiation. Precisely,

$$\frac{\partial}{\partial t_j} G_n = nF_{n-j}, \quad j = 1, \ldots, k,$$

cf. this with Lehmer's notion of companion sequences (see [**11**]).

Remark. It follows from Proposition 5.3 that the period of the different $\mathbf{D_p}[\mathbf{t}]$ is the same as $c_p(\mathfrak{O}_\mathbf{p}[\mathbf{t}])$ if p does not ramify. If p splits (recall that in this paper 'splits' mean factors but does not ramify), then $\mathbf{D_p}[\mathbf{t}]$ is in the group of units $\mathbf{G_p}[\mathbf{t}]$ and is a coset of $\mathbf{A_p}[\mathbf{t}]$, possibly identical with $\mathbf{A_p}[\mathbf{t}]$. If p ramifies, then $\mathbf{D}[\mathbf{t}]$ is a maximal ideal in $\mathfrak{O}_\mathbf{p}[\mathbf{t}]$. Theorem 5.3 and the remark above give the rather pretty set of connections among the GFP-sequence, the core polynomial, the derivative of the core, and the GLP-sequences: GFP determines the core, the derivative of the core yields GLP, the derivative (any first partial) of GLP yields the GFP.

6. Structure of the semi-local ring $\mathfrak{O}_{\mathbf{p}}[\mathbf{t}] = \mathfrak{O}[\mathbf{t}] \bigotimes \mathbf{Z_p}$. $\mathfrak{O}_{\mathbf{p}}[\mathbf{t}]$ is a finite, commutative ring; it is, therefore, a semi-local ring. The structure of semi-local rings is well known (for example, see [**18**]). We restate the structure theorem here (Theorem 6.4) for easy reference. $\mathfrak{O}_{\mathbf{p}}[\mathbf{t}]$ also has an orbit structure under the action of the group generated by $\mathbf{A_p}[\mathbf{t}]$, which, while not mysterious, is not readily found in the literature, and plays an integral role in our results. We shall first discuss this orbit structure and then exploit the semi-local nature of $\mathfrak{O}_{\mathbf{p}}[\mathbf{t}]$.

If $t_k \not\equiv 0 \pmod{p}$, then $\mathbf{A_p}[\mathbf{t}]$ is nonsingular, and, hence, is a unit in $\mathfrak{O}_{\mathbf{p}}[\mathbf{t}]$. The units in $\mathfrak{O}_{\mathbf{p}}[\mathbf{t}]$ are exactly those elements with norms different from 0, that is, having a standard matrix with nonzero determinant. An element with zero norm, then, either is zero or belongs to a proper ideal. Denote the group of units of $\mathfrak{O}_{\mathbf{p}}[\mathbf{t}]$ by $\mathbf{G_p}[\mathbf{t}]$ and its subgroup $\mathrm{gp}\langle \mathbf{A_p}[\mathbf{t}] \rangle$ by $\mathbf{H_p}[\mathbf{t}]$, the *period subgroup*. Then $\mathfrak{O}_{\mathbf{p}}[\mathbf{t}]$ is a $\mathbf{Z_p}(\mathbf{H_p}[\mathbf{t}])$-module, or more conveniently, a right $\mathbf{H_p}[\mathbf{t}]$-module. Clearly, $\mathfrak{O}_{\mathbf{p}}[\mathbf{t}]$ is the disjoint union of its orbits under the action of $\mathbf{A_p}[\mathbf{t}]$. A number of observations follow from these facts. It will be useful to list them for future reference:

(1) The orbit of zero is a singleton.

(2) An ideal consists of the disjoint union of orbits, each of which has orbit length dividing $c_p[\mathbf{t}]$. (Clearly, two orbits are either disjoint or identical, up to cyclic permutation.)

(3) Two distinct orbits in the same maximal ideal differ from one another by a coset representative of $\mathbf{H_p}$, i.e., if O_1 and O_2 are distinct orbits in the maximal ideal I, then there is a coset representative g of $\mathbf{H_p}$ in $\mathbf{G_p}$ such that $O_1 g = O_2$. (Of course, a coset representative may belong to the stabilizer of $\mathbf{H_p}$. O_1 and O_2 need not be bijective.)

(4) The orbits of $\mathbf{G_p}$ are the cosets of $\mathbf{H_p}$.

(5) The columns of an orbit are $\mathbf{t}$-linearly recursive, with a period dividing $c_p[\mathbf{t}]$.

(6) The (standard) matrix representation of $\mathfrak{O}_{\mathbf{p}}[\mathbf{t}]$ is implicit in the orbit structure of $\mathfrak{O}_{\mathbf{p}}[\mathbf{t}]$.

If $\mathbf{m} \in \mathfrak{O}_{\mathbf{p}}[\mathbf{t}]$, and if $m_{i,j}$ is the (i,j)th component of the standard matrix representation $\mathbf{M_p}$ of $\mathbf{m}$, the row vectors $\mathbf{m_i}$ of $\mathbf{M_p}$ are just the elements of the $\mathbf{A_p}$-orbit of $\mathbf{m}$.

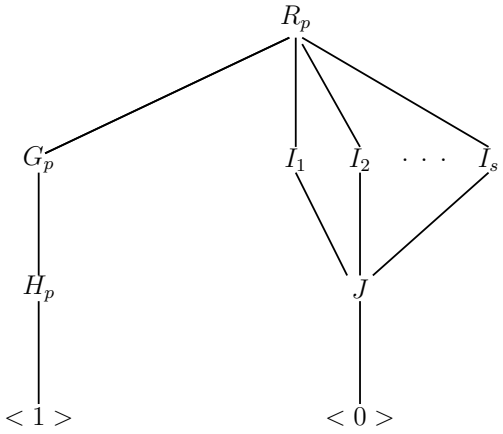

FIGURE 1. Lattice diagram of semi-local ring.

A pseudo-Hasse diagram that illustrates the construction of a typical finite ring $\mathfrak{O}_{\mathbf{p}}[\mathbf{t}]$ is given in Figure 1.

In Figure 1, $\mathbf{G_p}$ is the group of units in the finite ring $\mathfrak{O}_{\mathbf{p}}[\mathbf{t}]$, $\mathbf{H_p} = \text{gp}\langle \mathbf{A_p} \rangle$, $|\mathbf{H_p}| = c_p$ is the period of the associated k-linear recursion $F_{k,n}(t_1, \ldots, t_k) \pmod p$, the $\mathbf{I_j}$ are the maximal ideals in this ring and $\mathbf{J}$ is the radical. The "pseudo" in pseudo-Hasse refers to the fact that we show the lattice structure of the group of units in this ring in the same diagram. For an example, see Figure 2.

$\mathbf{e_1} = (-1, 1, -1)$, $\mathbf{e_2} = (-1, -1, 1)$, $\mathbf{e_1}$ and $\mathbf{e_2}$ are idempotents, $|\mathfrak{O}_{\mathbf{3}}| = 27$, $|\mathbf{G_3}| = 16$, $|\mathbf{H_3}| = 8$, $|\mathbf{G_3} : \mathbf{H_3}| = 2$.

$$\mathbf{A_3} = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & -1 & 0 \end{pmatrix}.$$

We record the following well-known fact:

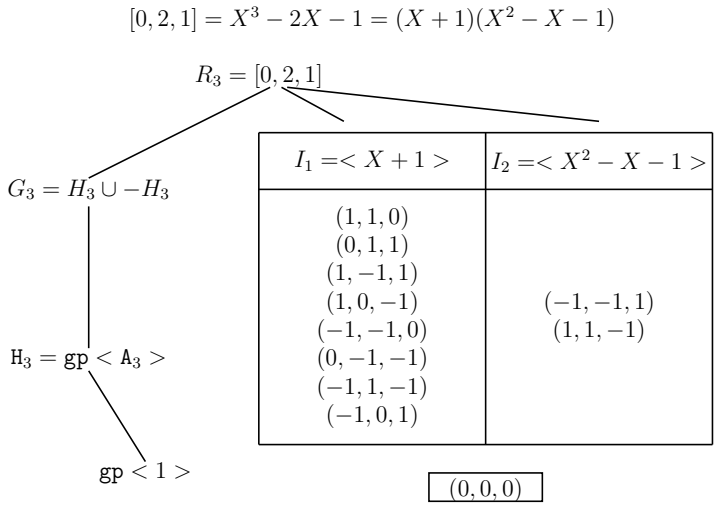

FIGURE 2. Lattice diagram of [0,2,1].

Proposition 6.1. *There is a one-to-one correspondence between maximal ideals of* $\mathfrak{O}_{\mathbf{p}}$ *and irreducible factors of* $\mathcal{C}(X) \pmod p$. □

Proposition 6.2 (Traces). *Let* $\mathbf{m} = (m_0, \dots, m_{k-1}) \in \mathfrak{O}_{\mathbf{p}}[\mathbf{t}]$. $\mathrm{tr}\,(\mathbf{m}) = m_0\mathbf{G_{k,0}} + \cdots + m_{k-1}\mathbf{G_{k,k-1}}$, *where* $\{\mathbf{G_{k,n}}\}$ *is the sequence of generalized Lucas polynomials, i.e., the isobaric reflect of the complete symmetric polynomials.*

Proof. Express $\mathbf{m}$ as $(m_0, m_1, \dots, m_{k-1})$ and note that the rows of $\mathbf{M}$ are vectors $\mathbf{mA^i}$. Writing $\mathbf{A^i_j}$ for the jth column of $\mathbf{A^i}$, we have that the trace of $\mathbf{m}$ is

$$(\mathbf{mA^0})\mathbf{A^0_1} + (\mathbf{mA^1})\mathbf{A^1_2} + \cdots + (\mathbf{mA^{k-1}})\mathbf{A^{k-1}_k}.$$

But a suitable rearrangement of this sum is just

$$m_0 \mathrm{tr}\,\mathbf{A^0} + m_1 \mathrm{tr}\,\mathbf{A^1} + \cdots + m_{k-1} \mathrm{tr}\,\mathbf{A^{k-1}},$$

which, by Theorem 3.1 (v), yields Proposition 6.2. □

Also note that, since each component of a vector in an orbit is in exactly one trace computation, the sum of the components of vectors in an orbit is equal to the sum of the traces of the vectors in the orbit. That is,

Proposition 6.3. (i) *The sum of the elements of the* $\mathbf{A_p[t]}$*-orbit of the vector* $\mathbf{m}$ *is the sum of the traces of the row vectors,* $\mathbf{m_i}$*, i.e.,*

$$\sum_{i,j} m_{i,j} = \sum_{i} \operatorname{tr} \mathbf{m_i}.$$

(ii) *If* $\mathbf{m} \in \mathfrak{O}_\mathbf{p}$*, i.e., if* $\det(\mathbf{m}) = 0$*, then*

$$\sum_{\text{orbits of } I} \sum_{i} \operatorname{tr}(\mathbf{m_i}) = 0.$$

Theorem 6.4 (cf., [**18**, VI.2], [**8**]). $\mathfrak{O}_\mathbf{p}[\mathbf{t}]$ *is a semi-local ring. In particular, letting* $\mathbf{J}(\mathfrak{O}_\mathbf{p}[\mathbf{t}]) = \operatorname{Rad}(\mathfrak{O}_\mathbf{p}[\mathbf{t}]) = \mathbf{I_1} \cap \cdots \cap \mathbf{I_s} = \mathbf{I_1} \cdots \mathbf{I_s}$*,* $\mathbf{I_1}, \ldots, \mathbf{I_s}$ *a complete set of maximal ideals in* $\mathfrak{O}_\mathbf{p}[\mathbf{t}]$*, there is a smallest integer* m *such that* $\mathbf{J^m} = \mathbf{I_1^m} \cdots \mathbf{I_s^m} = 0$*, and* $\mathfrak{O}_\mathbf{p}[\mathbf{t}] = \oplus_j \mathfrak{O}_\mathbf{p}[\mathbf{t}]/\mathbf{I_j^m}$*, where each factor is a local ring.*

Remark. For finite, commutative, semi-simple rings, several of the radical operators coalesce. The radical mentioned in the theorem can be taken, for example, to be the intersection of maximal ideals, or as the nilpotent radical.

As pointed out above, we use the term 'p splits' to mean that the core polynomial factors modulo (p), but that it does not ramify.

Theorem 6.5. (i) *If* p *is inert, then* $\mathfrak{O}_\mathbf{p}[\mathbf{t}]$ *is a field.*

(ii) *If* p *splits, then* $\mathfrak{O}_\mathbf{p}[\mathbf{t}]$ *has a trivial radical and thus is semi-simple, i.e., it is the direct sum of* s *simple rings* (*fields in this case*)*, where* s *is the number of prime ideals in the factorization of* $\mathfrak{O}_\mathbf{p}[\mathbf{t}]$*.*

(iii) *If* p *ramifies, then* $\mathfrak{O}_\mathbf{p}[\mathbf{t}]$ *has a nontrivial radical and is a direct sum of* s (*nontrivial*) *local rings.*

Proof. Theorem 6.5 is a direct consequence of the structure theorem, Theorem 6.4. The m in Theorem 6.4 is the l.c.m. of the ramification indices. □

Remark. An ideal element $\mathbf{m}$ outside of the radical is cyclic, i.e., satisfies $\mathbf{m}^n = \mathbf{m}$ for some natural number n. If $\mathbf{m} = \mathbf{e}$ is an idempotent, then the powers of $\mathbf{eA}$ coincide with the orbit of $\mathbf{e}$. This is because $(\mathbf{eA})^n = \mathbf{eA}^n$; thus, $\mathbf{eA}$ generates a cyclic group of order dividing $c_p[\mathbf{t}]$. Using the standard matrix representation of elements in $\mathfrak{O}[\mathbf{t}]$ or in $\mathfrak{O}_\mathbf{p}[\mathbf{t}]$, we can assign to each element a *rank* by letting $r(\mathbf{m}) = \operatorname{rank}(\mathbf{M})$, where $\mathbf{M}$ is the standard matrix representation of $\mathbf{m}$. We then observe that all elements in the same orbit have the same rank; that the rank of a unit is k, the degree of the core polynomial; and that the rank of an ideal element is at most the co-degree of the ideal , i.e., $k-d$, where d is the degree of the minimal polynomial of the ideal. (The rank of the representing matrix cannot exceed the degree of the minimal polynomial.)

Theorem 6.6. *Suppose that p splits and that $\{\mathbf{e_1}, \ldots, \mathbf{e_s}\}$ is a complete set of distinct primitive idempotents in $\mathfrak{O}_\mathbf{p}[\mathbf{t}]$.*

$$r\left(\sum_1^s \mathbf{e_j}\right) = \sum_1^s r(\mathbf{e_j}) = k.$$

Proof. By Theorem 6.5 (ii), $\mathfrak{O}_\mathbf{p}[\mathbf{t}]$ is semi-simple. We observe that: $1 \leq r(\mathbf{e_j}) < k$, and since $\sum_1^s \mathbf{e_j} = 1$, $r(\sum_1^s \mathbf{e_j}) = k$. The proof will then be a consequence of the following lemma and corollaries.

Lemma. *If we let $\mathbf{e}$ be the sum of the elements in any subset of the set of primitive idempotents $\{\mathbf{e_i}\}$ and let $\overline{\mathbf{e}}$ be the complementary sum, then*

$$r(\mathbf{e}) + r(\overline{\mathbf{e}}) \leqslant k.$$

Proof. If $\mathbf{E_1}$ and $\mathbf{E_2}$ are $k \times k$-matrices such that $\mathbf{E_1E_2} = \mathbf{0}$, then $r(\mathbf{E_1}) + r(\mathbf{E_2}) \leqslant k$. Since $\mathbf{E_1E_2} = \mathbf{0}$, we have that $r(\mathbf{E_1}) \leqslant \nu(\mathbf{E_2}) \leqslant k - r(\mathbf{E_2})$, where ν is the nullity of $\mathbf{E_2}$, and the lemma follows. □

Corollary 6.7.

$$r(\mathbf{e}) + r(\overline{\mathbf{e}}) = k.$$

Proof. Using the above Lemma and the remark at the beginning of the proof of the theorem, we have $k = r(\mathbf{e}+\overline{\mathbf{e}}) \leqslant r(\mathbf{e})+r(\overline{\mathbf{e}}) = k$. □

Corollary 6.8.

$$r(\mathbf{e_i} + \mathbf{e_j}) = r(\mathbf{e_i}) + r(\mathbf{e_j}).$$

Proof. From Corollary 6.7, we have that $r(\mathbf{e_1}) + r(\overline{\mathbf{e}}_\mathbf{1}) = k$, so that we can apply the above arguments to $r(\overline{\mathbf{e}}_\mathbf{1}) = k - r(\mathbf{e_1})$ to deduce that $r(\sum_2^s \mathbf{e_i}) = \sum_2^s r(\mathbf{e_i})$; hence, Corollary 6.8 holds. □

Theorem 6.6 follows now from the proof of Corollary 6.8. □

Corollary 6.9. *If we let* $\mathbf{B_1}, \ldots, \mathbf{B_s}$ *be the ideals* $\mathfrak{O}_\mathbf{p}[\mathbf{t}]\mathbf{e_1}, \ldots, \mathfrak{O}_\mathbf{p}[\mathbf{t}]\mathbf{e_s}$ *in* $\mathfrak{O}_\mathbf{p}[\mathbf{t}]$, *and let* $\mathbf{B_j^*} = \mathbf{B_j} - \{\mathbf{0}\}$, *then*

$$\mathbf{B_1^*} \times \cdots \times \mathbf{B_s^*} = \mathbf{G_p}[\mathbf{t}],$$

where $\mathbf{G_p}[\mathbf{t}]$ *is the group of units of* $\mathfrak{O}_\mathbf{p}[\mathbf{t}]$. *If* p *does not ramify, the* $\mathbf{B_j}$ *are finite fields.*

Proof. This follows from Theorem 6.5, Theorem 6.6, the fact that the ranks of nonzero elements of $\mathfrak{O}_\mathbf{p}[\mathbf{t}]$ are positive integers and that an element of $\mathfrak{O}_\mathbf{p}[\mathbf{t}]$ is a unit if and only if its norm is not zero (see [**18**]). □

Corollary 6.10.

$$|\mathbf{G_p}[\mathbf{t}]| = |\mathbf{B_1^*}| \cdots |\mathbf{B_s^*}| = (p^{r_1} - 1) \cdots (p^{r_s} - 1),$$

where p^{r_i} *is the order of* $\mathbf{B_i}$ *and* r_i *is the rank of* $\mathbf{e_i}$.

Corollary 6.11. *If* p *splits, the period* $c_p[t_1, \ldots, t_k] = \operatorname{lcm}\{c_p(\mathbf{min-poly}\,(\mathbf{e_i}))\}_1^s$.

Lemma. *If* $\mathbf{e}$ *is an idempotent in an ideal of* $\mathfrak{O}_\mathbf{p}[\mathbf{t}]$*, then the* $\mathbf{H_p}$*-orbit of* $\mathbf{e}$ *consists of the powers of* $\mathbf{eA}$*, a multiplicative cyclic group. In particular, the order of* $\mathbf{eA}$ *divides* $c_p[\mathbf{t}]$*.*

Proof. All of this follows easily from the fact that $(\mathbf{eA})^n = \mathbf{e}^n\mathbf{A}^\mathbf{n} = \mathbf{eA}^\mathbf{n}$, that $\mathbf{eA}^{\mathbf{c_P}} = \mathbf{e}$, and that the length of any orbit divides the period. □

The following result gives a remarkable connection between the p-periodicity of a linear recursion and the splitting properties of primes in associated rational number fields.

Theorem 6.7. *p divides $c_p[\mathbf{t}]$ if and only if p ramifies.*

Proof. First, we assume that $p \mid c_p[\mathbf{t}]$ and that p does not ramify; but then, by Theorem 6.5, $\mathfrak{O}_\mathbf{p}[\mathbf{t}]$ is semi-simple, and, so by Corollary 6.10, $p \mid (p^{r_i} - 1)$ for some i. A contradiction. In particular, if p does not ramify, $|\mathbf{G_p}[\mathbf{t}]|$ and p are relatively prime. To prove the converse, we observe that, if p ramifies, then each of the direct factors in $\mathfrak{O}_\mathbf{p}[\mathbf{t}]$ is a nontrivial local ring, say $\mathbf{B_j}$, where $\mathbf{B_j} = \mathbf{I_j}/\mathbf{I_j}^m$. If $\mathbf{B_j}^*$ is the group of units in $\mathbf{B_j}$, then there is an idempotent $\mathbf{e_j}$ in $\mathbf{I_j}$ and $\mathbf{e_j} + \mathbf{m}$ is a unit in the local ring $\mathbf{B_j}$, that is, is in $\mathbf{B_j}^*$, whenever $\mathbf{m} \in \mathbf{I_j}^m$, i.e., whenever $\mathbf{m} \in \mathbf{J}$. Moreover, there is a bijective correspondence between such $\mathbf{m}$s in $\mathbf{I_j}$ and the elements in the orbit of $\mathbf{e_j}$, so that by the Lemma, p divides c_p. Thus, p divides $|\mathbf{H_p}[\mathbf{t}]|$ and, hence, the order of $\mathbf{G_p}[\mathbf{t}]$. □

Remark. The well-known fact that a rational prime p ramifies with respect to a cyclotomic extension over $CP(n)$ only if p divides n now follows immediately from Theorems 2.1, 4.1 (iv) and 6.7.

Remark. Note that our notation $c_p[\mathbf{t}]$ for period of $\mathbf{A_p}$ determined by the core polynomial $[t_1, \ldots, t_k]$, for $p = 1$ or p prime, could as well be written $c_p(\mathfrak{O}_\mathbf{p}[\mathbf{t}])$, where, of course, $\mathfrak{O}_\mathbf{p}[\mathbf{e}] = \mathfrak{O}$ if $p = 1$. (Here it really doesn't matter whether the core is irreducible or not, that is, whether $\mathfrak{O}$ is a number field, or merely a commutative ring.) Since each maximal ideal in $\mathfrak{O}_\mathbf{p}[\mathbf{t}]$ is determined by and determines its minimal polynomial, which in turn determines the periods of the p-factors of the core polynomial of $\mathfrak{O}$, the notation $c_p(\mathbf{I})$ can be used to denote the

period of $\mathbf{A_p}$ determined by a factor of the original core polynomial. We use this notation in the statement of the next theorem.

Theorem 6.8. *Suppose that the semi-local ring $\mathfrak{O}_\mathbf{p}[\mathbf{t}]$ has maximal ideals $\mathbf{I_1}, \ldots, \mathbf{I_s}$, that is, suppose that the core polynomial has s irreducible factors, denoting the radical of $\mathfrak{O}_\mathbf{p}[\mathbf{t}]$ by $\mathbf{J}$. Then*

(1)
$$|\mathbf{G_p}(\mathfrak{O}_\mathbf{p}[\mathbf{t}])| = |\mathbf{B_{1^*}}| \cdot \cdots \cdot |\mathbf{B_s^*}| \cdot |\mathbf{J}|,$$

(2)
$$c_p(\mathfrak{O}_\mathbf{p}[\mathbf{t}]) = \operatorname{lcm}\{c_p(\mathbf{I_1}), \ldots, c_p(\mathbf{I_s})\} \cdot |\mathbf{J}|,$$

where $\mathbf{B_j^*} = \mathbf{I_j}/\mathbf{J}$, $j = 1, \ldots, s$ and $p = 1$ or p is prime.

Proof. Consider the exact sequence

$$\mathbf{J} \rightarrowtail \mathfrak{O}_\mathbf{p}[\mathbf{t}] \twoheadrightarrow \frac{\mathfrak{O}_\mathbf{p}[\mathbf{t}]}{\mathbf{J}}$$

where $\mathbf{J}$ is the radical of the ring. Since $\mathfrak{O}_\mathbf{p}[\mathbf{t}]/\mathbf{J}$ is semi-simple, by Corollary 6.11, $c_p(\mathfrak{O}_\mathbf{p}[\mathbf{t}]/\mathbf{J}) = \operatorname{lcm}\{c_p(\mathbf{minpoly}\,(\mathbf{B_{j^*}}))\}_1^s$. If $\mathfrak{O}_\mathbf{p}[\mathbf{t}]$ splits, that is, if the radical is $\mathbf{0}$, then we are done. In any case, by Corollary 6.10, $|\mathbf{G_p}(\mathfrak{O}_\mathbf{p}[\mathbf{t}]/\mathbf{J})| = |\mathbf{B_1^*}| \times \cdots \times |\mathbf{B_s^*}| \times |\mathbf{J}|$. It is clear that units in $\mathfrak{O}_\mathbf{p}[\mathbf{t}]$ are mapped homomorphically onto the units of $\mathfrak{O}_\mathbf{p}[\mathbf{t}]/\mathbf{J}$ and, since $\mathbf{u} \to \mathbf{u} + \mathbf{J}, \mathbf{u} \in \mathbf{G_p}$, part (1) of the theorem follows.

As for part (2) of the theorem, we have by Corollary 6.11 that $c_p(\mathfrak{O}_\mathbf{p}[\mathbf{t}]/\mathbf{J}) = \operatorname{lcm}\{|\mathbf{B_1^*}|, \ldots, |\mathbf{B_s^*}|\} = \operatorname{lcm}\{(p_1^{r_1} - 1), \ldots, (p_1^{r_s} - 1)\} = \operatorname{lcm}\{c_p(\mathbf{I_j})\}$, that is, the least common multiple of the periods of the irreducible factors of the core polynomial of $\mathfrak{O}_\mathbf{p}[\mathbf{t}]/\mathbf{J}$. But this number is just the order of the period group $(\mathbf{H_p} + \mathbf{J})/\mathbf{J}$ in $\mathfrak{O}/\mathbf{J}$, which accounts for the factor $|\mathbf{J}|$ in part (2) of the theorem. □

Theorem 6.8 now enables us to prove:

Corollary 6.12. *Suppose the core polynomial (reducible or not) factors* (mod p) *into s irreducible factors. Then the p-core polynomial is the least common multiple of the periods of the irreducible factors times the order of the radical of the semi-simple ring $\mathfrak{O}_\mathbf{p}[\mathbf{t}]$. Furthermore, $\mathbf{J}$ is nontrivial exactly when p divides the period. In terms of algebraic number fields, this is just the case when p ramifies, i.e., when p divides the discriminant of the field.*

Figure 3 with $p = 3$ and $[\mathbf{t}] = [4, -5, 2]$, illustrates the situation in the case of a nontrivial radical:

$$[4, -5, 2] = X^3 - 4X^2 + 5X - 2 = (X - 1)^2(X - 2)$$

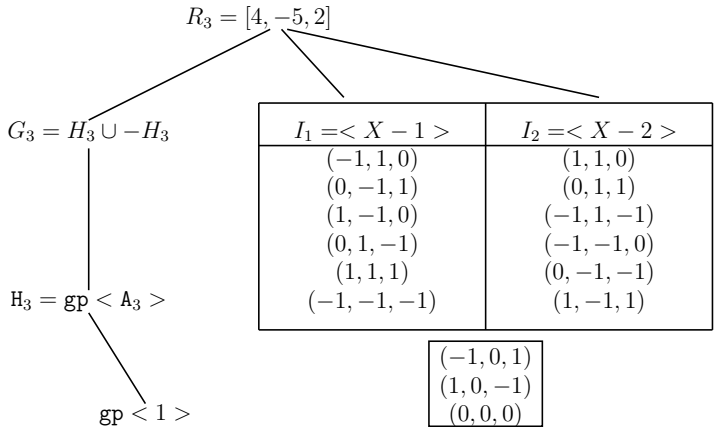

FIGURE 3.

Note that $(0, -1, -1)$ is a unit in $\mathbf{I_2}$ and that $\mathbf{I_2} - \mathbf{J}$ is a multiplicative group in which this unit acts as the identity. In this example $|\mathbf{G_3}| = 12$ and the *period subgroup* is $\mathrm{gp}\langle\mathbf{A}\rangle = \mathbf{H_3}$ has order 6, $|\mathbf{H_3}| = 6$.

In the case of number fields, it is a trivial fact that only finitely many primes ramify. There are examples, however, when, for every p, p divides the period; for instance, the following is such a case. Consider the core polynomial $[2, -1]$. The 2-linear sequence $\{F_n[2, -1]\}$ for this core is just $\{1, 2, 3, \ldots, n, \ldots\}$. It is easy to see that $c(\mathfrak{O}_\mathbf{p}[\mathbf{t}]) = p$ for every p.

REFERENCES

1. J.W.S. Cassels, *Local fields*, Cambridge University Press, Cambridge, 1986.

2. Umberto Cerruti and Francesco Vaccarino, *Matrices, recurrent sequences and arithmetic*, in *Applications of Fibonacci numbers*, Vol. 6, Kluwer Academic Publishers, Dordrecht, 1996.

3. ———, *Vector linear recurrence sequences in commutative rings*, in *Applications of Fibonacci numbers*, Vol. 6 Kluwer Academic Publishers, Dordrecht, 1996.

4. Y.C. Chen and James D. Louck, *The combinatorial power of the companion matrix*, Linear Algebra Appl. **232** (1996), 261–268.

5. Harold M. Edwards, *Galois theory*, Springer, New York, 1984.

6. Graham Everest, Alf van der Poorten, Igor Schlarinski and Thomas Ward, *Recurrence sequences*, AMS Math. Mono. Surv. **104** (2003), 45–49.

7. Qing-hu Hou and Yang-ping Mu, *Recurrent sequences and Schur functions*, Adv. Appl. Math. **31** (2003), 150–162.

8. Gerald L. Janusz, *Algebraic number fields*, Academic Press, New York, 1973.

9. A. Lascoux, *Suites récurrentes linéaires*, Adv. Appl. Math. **7** (1986), 228–235.

10. ———, *Symmetric functions*, Nankai University, 2001, http://www.combinatorics.net/teach.

11. D.H. Lehmer, *An extended theory of Lucas' functions*, Ann. Math. **31** (1930), 419–448.

12. Hua-Chieh Li, *Complete and reduced residue systems of second order recurrences modulo p*, Fibonacci Quart. **38** (2000), 272–381.

13. I.G. Macdonald, *Symmetric functions and Hall polynomials*, Clarendon Press, Oxford, 1995.

14. T. MacHenry, *A subgroup of the group of units in the ring of arithmetic functions*, Rocky Mountain J. Math. **29** (1999), 1055–1065.

15. ———, *Generalized Fibonacci and Lucas polynomials and multiplicative arithmetic functions*, Fibonacci Quart. **38** (2000), 17–24.

16. Trueman MacHenry and Geanina Tudose, *Reflections on isobaric polynomials and arithmetic functions*, Rocky Mountain J. Math. **35** (2005), 901–928.

17. ———, *Differential operators and weighted isobaric polynomials*, Rocky Mountain J. Math. **36** (2006), 1957–1976.

18. Bernard R. McDonald, *Finite rings with identities*, Marcel Dekker, New York, 1974.

19. I. Niven, *Fermat theorem for matrices*, Duke Math. J. **15** (1948), 823–826.

20. Piotr Pragascz, *Architectonique des formules préférées d'Alain Lascoux*, Sém. Lotharingien Combinatoire **52** (2005), 1–39.

York University, Toronto, Canada
Email address: machenry@mathstat.yorku.ca

Centennial College, Toronto, Canada
Email address: kkwong@centennialcollege.ca