Local Galois module structure in positive characteristic and continued fractions

Smit, B.; Thomas, L.

Arch. Math. 88 (2007), 207–219
© 2007 Birkhäuser Verlag Basel/Switzerland
1422-6928/030207-13, *published online* 2007-02-19
DOI 10.1007/s00013-006-1939-8

Archiv der Mathematik

Local Galois module structure in positive characteristic and continued fractions

Bart de Smit and Lara Thomas

Abstract. For a Galois extension of degree p of local fields of characteristic p, we express the Galois action on the ring of integers in terms of a combinatorial object: a balanced $\{0,1\}$-valued sequence that only depends on the discriminant and p. We show that the embedding dimension $\mathrm{edim}(R)$ of the associated order R is tightly related to the minimal number d of R-module generators of the ring of integers. Moreover, we show how to compute d and $\mathrm{edim}(R)$ from p and the discriminant with a continued fraction expansion.

Mathematics Subject Classification (2000). Primary: 11R33; Secondary: 11J70, 68R15.

Keywords. Galois module structure, local fields, Artin-Schreier extensions, associated orders, embedding dimension, continued fractions.

1. Main results. By a local field we mean a field which is complete with respect to a discrete valuation. Let $K \subset L$ be a Galois extension of local fields of characteristic $p > 0$, whose Galois group G is cyclic of order p. Let A and B be the rings of integers of K and L. Let $\mathfrak{p}$ be the maximal ideal of A and $k = A/\mathfrak{p}$ its residue field.

Define the *multiplier ring*, or associated order, of the Galois module B to be the subring $R = \{x \in K[G] : xB \subset B\}$ of the group ring $K[G]$. This ring R is a local ring with residue field k which is free of rank p as an A-module, and which contains $A[G]$. We denote its maximal ideal by $\mathfrak{m}$.

The goal of this paper is to study the ring R and the structure of B as an R-module. Let d be the minimal number of R-module generators of B, and let $\delta_{L/K}$ be the integer for which $\mathfrak{p}^{\delta_{L/K}}$ is the discriminant of B over A. Our first theorem

We thank Bruno Anglès, Wieb Bosma and Rob Tijdeman for their bibliographic assistance.

says that d is closely related to the *embedding dimension* $\operatorname{edim}(R) = \dim_k(\mathfrak{m}/\mathfrak{m}^2)$ of R. In Theorem 3 below we show how to compute d.

Theorem 1. *If $p \mid \delta_{L/K}$ then R is isomorphic as an A-algebra to $A[X]/(X^p)$ and B is free of rank 1 as an R-module. If $p \nmid \delta_{L/K}$ then* $\operatorname{edim}(R) = 2d + 1$.

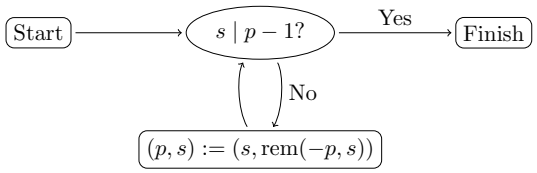
Theorem 1 implies that $d = 1$ and $\operatorname{edim}(R) = 2$ if $p \mid \delta_{L/K}$. This case includes the unramified case, the case that the residue field extension is inseparable, and also certain cases where the ramification index is p. We have $R = A[G]$ if and only if L is unramified over K; see Proposition 3.

The proof has two basic ingredients: graded rings and balanced sequences. In Section 3 we will give R the structure of a *graded ring*, and B the structure of a *graded module* over R. We will use an Artin-Schreier equation $x^p - x = y$ for L over K where $y \in K$ has valuation $-t$ with $t \geq 0$ as small as possible. If the ramification index is p then $p \nmid t$ and $\delta_{L/K} = (p-1)(t+1)$, and otherwise $p \mid t$ and $\delta_{L/K} = (p-1)t$; see Section 3 for details. Define the *remainder* $s = \operatorname{rem}(t, p)$ of t when dividing by p to be the unique integer s that satisfies $0 \leq s < p$ and $t \equiv s \bmod p$.

We will give an explicit combinatorial description of the gradings on R and B in terms of the *balanced sequence* associated to the fraction s/p. This sequence and its basic properties are introduced in Section 2. The proof of Theorem 1, which is given in Section 4, exploits some slightly subtle combinatorial properties of this sequence.

The combinatorial description also gives rise to a method to compute d.

Theorem 2. *If $s = 0$ then $d = 1$. Otherwise, d is the number of times we pass through the middle oval in the following flow chart.*



It follows from the two theorems that for $s \neq 0$ we have

$$d = 1 \iff \operatorname{edim}(R) \leq 3 \iff s \mid p - 1;$$
$$d \leq 2 \iff \operatorname{edim}(R) \leq 5 \iff s - \operatorname{rem}(p, s) \mid s - 1.$$

The equivalence $d = 1 \iff s \mid p - 1$ is essentially the result of Aiba [1], as pointed out by Byott [5] and Lettl [9]. We include an independent proof of this in Section 3, which does not rely on the combinatorial arguments of Section 4. See [2, 3] for a characteristic zero analog.

We can compute d more efficiently in terms of the continued fraction expansion of $-s/p$. If $s \neq 0$ then we can write

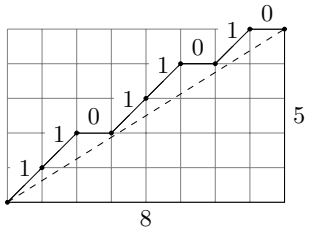
$$-\frac{s}{p} = x_0 + \cfrac{1}{x_1 + \cfrac{1}{\ddots \cfrac{\ddots}{x_{m-1} + \cfrac{1}{x_m}}}}$$

for unique integers $x_0, \ldots, x_m \in \mathbb{Z}$ satisfying $x_1, \ldots, x_{m-1} \geq 1$ and $x_m \geq 2$.

Theorem 3. *If $s = 0$ or $s = p - 1$ then $d = 1$. Otherwise d is the sum of all x_i with i odd and $i < m$.*

We give the proof in Section 4. Since the continued fraction expansion can be computed quickly, this gives rise to an algorithm that given p and s computes d in polynomial time, i.e., in time bounded by a polynomial in $\log(p)$. When $p > 2$ and $s = p - 2$ we have $m = 2$ and $x_1 = (p-1)/2$, so we immediately get $d = (p-1)/2$ by Theorem 3, while the flow chart does not finish in polynomial time.

2. Balanced sequences. Suppose x is a real number with $0 \leq x < 1$. For $i \in \mathbb{Z}$ let $a_i = \lceil ix \rceil = \inf\{n \in \mathbb{Z} : n \geq ix\}$ and put $\epsilon_i = a_i - a_{i-1} \in \{0, 1\}$. This means that the point (i, a_i) is on or above the line through the origin with slope x, and $(i, a_i - 1)$ is below it. In the picture below, we give the sequences ϵ_i, a_i and m_i (defined below) for $x = 5/8$.



$$\begin{aligned} \epsilon_1, \ldots, \epsilon_7 &= 1, 1, 0, 1, 1, 0, 1 \\ a_1, \ldots, a_7 &= 1, 2, 2, 3, 4, 4, 5 \\ m_1, \ldots, m_7 &= 0, 1, 2, 2, 3, 4, 5. \end{aligned}$$

The sequence $(\epsilon_i)_{i \in \mathbb{Z}}$ is *balanced*, i.e., any two finite blocks in the sequence of the same length have sums that differ by at most one. Moreover, blocks starting with ϵ_1 have maximal sum. This is phrased more precisely in the next lemma.

Lemma 1. *For all $i, j, n \in \mathbb{Z}$ with $n \geq 0$ we have*

$$|(\epsilon_{i+1} + \epsilon_{i+2} + \ldots + \epsilon_{i+n}) - (\epsilon_{j+1} + \epsilon_{j+2} + \ldots + \epsilon_{j+n})| \leq 1.$$

For all $n \geq 0$ we have

$$a_n = \epsilon_1 + \epsilon_2 + \cdots + \epsilon_n = \sup\{\epsilon_{i+1} + \epsilon_{i+2} + \ldots + \epsilon_{i+n} \colon\ i \in \mathbb{Z}\}.$$

We leave the easy proof to the reader. See [10, Sec. 2.1.2] for further properties. When x is not rational the balanced sequence is often called a *Sturmian sequence*.

In this paper we are only interested in the case that x is rational, so from now on let us assume that $x \in \mathbb{Q}$. Then the sequence ϵ is *periodic* that is, there is an integer $p \geq 1$ so that $\epsilon_i = \epsilon_j$ for all $i, j \in \mathbb{Z}$ with $i \equiv j \bmod p$. Let us take p minimal with this property. Then p is the denominator of x. In our main application, p will be the characteristic of K, but we will need balanced sequences whose period is not prime as well. Write s for the numerator of x.

Lemma 2. *The sequence $\epsilon_2, \epsilon_3, \ldots, \epsilon_{p-1}$ is a palindrome.*

This lemma follows immediately from the fact that $a_i + a_{p-i} = s+1$ when $0 < i < p$.

We define a third sequence $m_0, m_1, m_2, \ldots, m_{p-1}$ by

$$m_n = \inf\{\epsilon_{i+1} + \epsilon_{i+2} + \ldots + \epsilon_{i+n} \colon\ 0 \leq i < p - n\}.$$

The range over which we take this infimum is restricted: m_n is the smallest sum of a block of length n *within* $\epsilon_1, \ldots, \epsilon_{p-1}$.

Lemma 3. *For $n \in \{1, \ldots, p-1\}$ we have $a_n = m_n$ if and only if for all $i, j \in \{1, \ldots, p-1\}$ with $i \equiv j \bmod n$ we have $\epsilon_i = \epsilon_j$.*

This lemma follows easily from Lemma 1. If $n \in \{1, \ldots, p-1\}$ has the property in Lemma 3 then we say that n is a *sub-period* of ϵ. In our example with $x = 5/8$ we see that 3, 6 and 7 are sub-periods.

3. Graded rings. Let the notation be as in the introduction. See [4, Chap. II §11] for basic concepts of graded rings and modules. Our gradings will be indexed by the non-negative integers.

For each $g \in G = \mathrm{Gal}(L/K)$ we have the identity $(g-1)^p = g^p - 1 = 0$ in $K[G]$. This implies that the group ring $K[G]$ is a local ring with residue field K. If we choose a generator σ for G, and write $X = \sigma - 1 \in K[G]$, then $K[G]$ is the truncated polynomial ring $K[X]/(X^p)$. Thus, $K[G]$ becomes a *graded ring* whose homogeneous part of degree i is non-trivial only if $i = 0, \ldots, p-1$, in which case it is the 1-dimensional K-vector space KX^i. For each $i \geq 0$ the elements of degree at least i form an ideal, which coincides with the i-th power of the maximal ideal of $K[G]$. Thus, the grading depends on the choice of a generator of G, but the induced filtration of $K[G]$ by a chain of ideals is canonical. Note that $A[G] = \bigoplus_i AX^i$ is a graded subring of $K[G]$.

For $x \in L$ write $\wp(x) = x^p - x$. By Artin-Schreier theory, we have $L = K(\alpha)$ for some $\alpha \in L$ with $\wp(\alpha) \in K$. We use the generator σ of G with $\sigma\alpha = \alpha + 1$ to define a grading on $K[G]$ so that $\sigma - 1$ is homogeneous of degree 1. For $i < p$ the element $\binom{\alpha}{i}$ is the binomial polynomial $\alpha(\alpha-1)\cdots(\alpha-i+1)/i!$ where $\binom{\alpha}{0} = 1$ and $\binom{\alpha}{i} = 0$ for $i < 0$. For $i < p$ we have $(\sigma - 1)\binom{\alpha}{i} = \binom{\alpha}{i-1}$. This implies that we can equip L with the structure of a *graded module* over $K[G]$: its homogeneous

piece of degree i is 0 for $i = 0$ and $i > p$, and it is the 1-dimensional K-vector space $L_i = K\binom{\alpha}{p-i}$ for $i = 1, \ldots, p$. Note that L is free over $K[G]$ on one homogeneous generator $\binom{\alpha}{p-1}$ in degree 1.

We now refine our choice of Artin-Schreier equation to obtain a description of B, and to show that B is a graded $A[G]$-submodule of L. Thus, we need a better choice of $\alpha \in S = \{\alpha' \in L \text{ with } \wp(\alpha') \in K \text{ and } \alpha' \notin K\}$. Let $f_{L/K}$ be the degree of the residue field extension of L over K. The following proposition partly goes back to Hasse [6]. We include a proof below for convenience.

Proposition 1. *The supremum* $\sup\{\mathrm{ord}_{\mathfrak{p}}(\wp(\alpha')) : \alpha' \in S\}$ *is an integer* $-t$ *with* $t \geq 0$. *If* $p \mid t$ *then* $f_{L/K} = p$ *and* $\delta_{L/K} = (p-1)t$. *If* $p \nmid t$ *then* $f_{L/K} = 1$ *and* $\delta_{L/K} = (p-1)(t+1)$.

We now choose $\alpha \in S$ so that the supremum in the Proposition is attained at α. Again, the generator σ of G with $\sigma\alpha = \alpha + 1$ gives rise to a grading on $K[G]$ for which $\sigma - 1$ is homogeneous of degree 1.

Proposition 2. *The ring* B *is a graded* $A[G]$*-submodule of* L. *For* $i = 1, \ldots, p$ *its homogeneous part of degree* i *is the free* A*-module of rank* 1

$$B_i = \mathfrak{p}^{\lceil t(p-i)/p \rceil} \binom{\alpha}{p-i}.$$

Proof of Propositions 1 *and* 2. For $y \in K$ consider the polynomial $f = T^p - T - y \in K[T]$. If $y \in A$ then $(f \bmod \mathfrak{p}) \in k[T]$ is separable, which by Hensel's lemma implies that f has a zero in K if $(y \bmod \mathfrak{p}) \in \wp(k)$, and that otherwise a zero of f generates an unramified degree p extension of K. By applying this to $y = \wp(\alpha')$ with $\alpha' \in S$, we deduce two things. First, we then have $(y \bmod \mathfrak{p}) \notin \wp(k)$, and in particular $y \notin \mathfrak{p}$, so $\mathrm{ord}_{\mathfrak{p}}(\wp(\alpha')) \leq 0$. Thus, the supremum in Proposition 1 is a finite number $-t$ with $t \geq 0$. Secondly, we have $t = 0$ if L is unramified over K.

Write v_K and v_L for the valuations on K and L, and let $\pi \in K$ with $v_K(\pi) = 1$. Thus, $\mathfrak{p} = \pi A$ and $v_L(\pi)$ is the ramification index of L over K.

Suppose that $p \nmid t$. Then $v_L(\alpha) < 0$, and by the strong triangle inequality we have $pv_L(\alpha) = v_L(\alpha^p) = v_L(\wp(\alpha))$. It follows that $p \mid v_L(\wp(\alpha)) = -tv_L(\pi)$, so $v_L(\pi) = p$ and $v_L(\alpha) = -t$, which implies that $v_L(\binom{\alpha}{i}) = -it$. Moreover, v_L assumes the values $\{0, 1, \ldots, p-1\}$ on the set $\{\pi^{\lceil it/p \rceil}\binom{\alpha}{i} \colon\ 0 \leq i < p\}$. With Nakayama's Lemma it follows that this set is an A-basis for B, as required.

Now suppose that $p \mid t > 0$. Then the image u of $\pi^{t/p}\alpha \in B$ in the residue field of L satisfies $u^p \in k$. If $u^p = v^p$ for some $v \in k$, then $\alpha' = \alpha - \pi^{-t/p}z \in S$, for any lift z of v to A, would satisfy $v_K(\wp(\alpha')) > -t$ which is a contradiction. Thus, u generates an inseparable degree p extension of k. Again by Nakayama's lemma, the set $\{\pi^{it/p}\alpha^i \colon\ 0 \leq i < p\}$ is an A-basis of B. It follows that $\{\pi^{it/p}\binom{\alpha}{i} \colon\ 0 \leq i < p\}$ is an A-basis of B as well. This proves Proposition 2.

In order to compute the discriminant in terms of t, first note that

$$\delta_{L/K} = v_K(\Delta_{L/K}) = (p-1) f_{L/K} v_L(\sigma x - x)$$

when x is an A-algebra generator of B; see [11, Ch. IV §1 Prop. 4, Ch. II §2 Cor. 4]. If in addition $x \in A\binom{\alpha}{i}$ with $0 \le i < p$ then $\sigma x - x = xi/\alpha$, so $v_L(\sigma x - x) = v_L(x) - v_L(\alpha) = v_L(x) + t/f_{L/K}$. In the case $p \mid t$ we found such an x with $v_L(x) = 0$. In the case $p \nmid t$ we have such an x in our A-basis of B with $v_L(x) = 1$. This gives the discriminant formulas in Proposition 1. □

We write $t = pk + s$ with $k, s \in \mathbb{Z}$ and $0 \le s < p$. Let $\epsilon_1, \epsilon_2, \dots$ be the balanced sequence associated to the fraction s/p. Define the integers $m_1, m_2, \dots, m_{p-1}$ and $a_0, a_1, \dots$ as in Section 2.

Let π be a prime element of K and consider the element $\varphi = (\sigma - 1)/\pi^k \in K[G]$, which is homogeneous of degree 1.

Proposition 3. *For $i = 1, \dots, p$ we have*

$$B_i = \mathfrak{p}^{k(p-i)+a_{p-i}} \binom{\alpha}{p-i}, \qquad \varphi B_i = \mathfrak{p}^{\epsilon_{p-i}} B_{i+1}.$$

The ring R is a graded subring of $K[G]$ with $R_i = \mathfrak{p}^{-m_i}\varphi^i$ when $0 \le i < p$.

Proof. We have $\varphi\binom{\alpha}{p-i} = \binom{\alpha}{p-i-1}\pi^{-k}$, and $\lceil t(p-i)/p \rceil = \lceil t(p-i-1)/p \rceil + k + \epsilon_{p-i}$. Combining this with the previous Proposition the first statement follows.

The endomorphism ring of a finitely generated graded module over a graded ring is itself graded [4, Ch. II §11.6]. In our case, we have a canonical isomorphism of graded rings $K[G] \to \mathrm{End}_{K[G]}(L)$ that maps R bijectively to $\mathrm{End}_{A[G]}(B)$. It follows that R is a graded subring of $K[G]$, and that its homogeneous part of degree i is given by

$$R_i = \{\psi \in K\varphi^i : \ \psi B_j \subset B_{j+i} \text{ for all } j \text{ with } 1 \le j \le p-i\}.$$

To compute this we apply the first statement: for $i, j \ge 1$ with $i + j \le p$ we have $\varphi^i B_j = \mathfrak{p}^w B_{i+j}$ with $w = \epsilon_{p-i-j+1} + \cdots + \epsilon_{p-j}$. As j varies with i fixed, this number w runs over the sums of blocks of length i in the sequence $\epsilon_1, \dots, \epsilon_{p-1}$. The minimal such w is m_i. □

Corollary. *If $s = 0$ or $s = p - 1$ then $d = 1$ and* $\mathrm{edim}(R) = 2$.

To see this, note that $R = A[\varphi]$ if $s = 0$ and $R = A[\varphi/\pi]$ if $s = p - 1$, and that in both cases B_1 generates B as an R-module.

We now formulate the main result of this Section. We define the following two sets:

$$\mathcal{D} = \{i : \ 0 < i < p \text{ and } a_j + m_{i-j} < a_i \text{ for all } j \text{ with } 0 < j < i\};$$
$$\mathcal{E} = \{i : \ 0 \le i < p \text{ and } m_j + m_{i-j} < m_i \text{ for all } j \text{ with } 0 < j < i\}.$$

Theorem 4. *We have $d = \#\mathcal{D}$ and $\operatorname{edim}(R) = \#\mathcal{E}$. Moreover, a set of homogeneous elements in B (resp. $\mathfrak{m}$) forms a set of R-module generators of B (resp. $\mathfrak{m}$) if and only if for each i in $\mathcal{D}$ (resp $\mathcal{E}$) it contains an A-module generator of B_i (resp $\mathfrak{m}_i$).*

Proof. The maximal ideal $\mathfrak{m}$ of R is homogeneous: $\mathfrak{m} = \bigoplus_{i=0}^{p-1} \mathfrak{m}_i$ with $\mathfrak{m}_0 = \mathfrak{p}$ and $\mathfrak{m}_i = R_i$ for $i > 0$. This implies that $\mathfrak{m}B$ is a graded submodule of B. For each i with $1 \leq i \leq p$ we have

$$(\mathfrak{m}B)_i = \sum_{j=1}^{i} \mathfrak{m}_{i-j} B_j.$$

It follows that $(\mathfrak{m}B)_i = B_i$ if and only if $a_{p-j} - m_{i-j} = a_{p-i}$ for some j with $1 \leq j < i$. Taking $i = p$ and $j = 1$ we see that $a_{p-1} - m_{p-1} = 0 = a_0$, so $(\mathfrak{m}B)_p = B_p$. If $1 \leq j < i < p$ then we have $a_i + a_{p-i} = s + 1 = a_j + a_{p-j}$, so the condition $a_{p-j} - m_{i-j} = a_{p-i}$ is equivalent to $a_j + m_{i-j} = a_i$. It follows that we have $(\mathfrak{m}B)_i = B_i$ if and only if $i \notin \mathcal{D}$.

By Nakayama's lemma, a subset of B generates B as an R-module if and only if it generates $B/\mathfrak{m}B$ as a k-vector space. In particular, the minimal number of such elements is the k-dimension of $B/\mathfrak{m}B$, which is the number of integers i with $B_i \neq (\mathfrak{m}B)_i$. The last statement for B also follows.

Similarly, the ideal $\mathfrak{m}^2$ is homogeneous. We have

$$\mathfrak{m}^2 = \bigoplus_{i=0}^{p-1} (\mathfrak{m}^2)_i \text{ with } (\mathfrak{m}^2)_i = \sum_{j=0}^{i} \mathfrak{m}_j \mathfrak{m}_{i-j}.$$

Since $\mathfrak{m}_0 \neq A$ it follows that $(\mathfrak{m}^2)_i = \mathfrak{m}_i$ if and only if $m_j + m_{i-j} = m_i$ for some j with $0 < j < i$, which in turn is equivalent to $i \notin \mathcal{E}$. The result now follows as in the first case with Nakayama's lemma. □

The next result also follows Theorem 2, but since it is easy to prove without much combinatorics we include a separate proof. The equivalence of the first and third condition also follows from work of Aiba [1, 5, 9].

Corollary. *When $s \neq 0$ the following are equivalent:*

(1) $d = 1$;
(2) $\epsilon_1, \ldots, \epsilon_{p-1}$ *is an s-fold repetition of a sequence* $1, 0, 0, \ldots, 0$;
(3) $s \mid p - 1$.

Proof. Clearly, (2) implies (3). Suppose (3) holds, so that $p - 1 = sk$ for an integer k. Then it is easy to see that (2) holds and that $m_{i-1} = a_i - 1$ for each i with $0 < i < p$. If $i > k$ then we get $a_{i-k} + m_k = a_{i-k} + 1 = a_i$, so $i \notin \mathcal{D}$. If $2 \leq i \leq k$ then we have $a_1 + m_{i-1} = 1 + 0 = a_i$, so again $i \notin \mathcal{D}$. We deduce that $\mathcal{D} = \{1\}$ so that (1) holds. Note that $R = A[\varphi, \varphi^k/\pi]$.

Now suppose that (1) holds and that $0 < s < p-1$. Then we have $\mathcal{D} = \{1\}$ and $m_1 = 0$. The smallest l with $m_l = 1$ satisfies $2 \leq l \leq p-1$. For each i with $1 \leq i < l$ we have $1 = m_i + 1 \geq a_i \geq \epsilon_1 = 1$, so $a_i = 1$. Since $l \notin \mathcal{D}$ there is an integer i with $0 < i < l$ and $a_l = a_i + m_{l-i} = 1 + 0 = 1 = m_l$. By Lemma 3 we see that l is a sub-period. Thus, the sequence $\epsilon_1, \epsilon_2, \ldots, \epsilon_{p-1}$ satisfies $\epsilon_i = 1$ exactly when $i \equiv 1 \bmod l$. Using Lemma 2 we see that the sequence ends with $l-1$ zeroes, so (2) follows. □

4. Combinatorial results. In this section we prove the results in Section 1 by analyzing the sets $\mathcal{D}$ and $\mathcal{E}$ for balanced sequences in a slightly more general setting.

Let $x \in \mathbb{Q}$ with $0 < x < 1$, and write $x = s/p$ with s and p positive coprime integers. We do not assume that p is prime. We use the notation from Section 2. In particular we have the sequences (ϵ_i), (a_i) and (m_i). We define the sets $\mathcal{D}$ and $\mathcal{E}$ as in Section 3. We first look at the set of sub-periods

$$\mathcal{P} = \{n : 0 < n < p \text{ and } a_n = m_n\}.$$

By Lemma 3 these are the $n < p$ for which we have a commutative diagram

$$\begin{array}{ccc} \{1, 2, \ldots, p-1\} & \xrightarrow{\quad i \mapsto \epsilon_i \quad} & \{0, 1\}. \\ & \searrow \quad \nearrow & \\ & \mathbb{Z}/n\mathbb{Z} & \end{array}$$

Clearly, $p-1$ always lies in $\mathcal{P}$, and any multiple below p of an element of $\mathcal{P}$ again lies in $\mathcal{P}$. We define $\mathcal{M} = \mathcal{M}(x)$ to be the set of *minimal sub-periods*, that is, the sub-periods for which no proper divisor is a sub-period.

Lemma 4. *Suppose $i, j \in \mathcal{P}$ with $i + j \leq p$. Then $\gcd(i, j) \in \mathcal{P}$. If $i + j = p$ then $1 \in \mathcal{P}$.*

Proof. Suppose first that $i + j = p$. We may assume that $j > 1$. By Lemma 2 and the fact that $i \in \mathcal{P}$ we get $\epsilon_j = \epsilon_{p-j+1} = \epsilon_{i+1} = \epsilon_1 = 1$. Using $j \in \mathcal{P}$ and Lemma 1 one sees that for each l with $0 \leq l < i$ we have

$$\epsilon_{l+1} + a_l = a_{l+1} \geq \epsilon_j + \cdots + \epsilon_{j+l} = \epsilon_j + (\epsilon_1 + \cdots + \epsilon_l) = 1 + a_l,$$

so that $\epsilon_{l+1} = 1$. Since $i \in \mathcal{P}$ this implies that $s = p - 1$ and $1 \in \mathcal{P}$.

Next, suppose that $i + j < p$ and assume that $j < i$. Suppose $i \equiv r \mod j$ with $0 \leq r < j$. For each k with $1 \leq k \leq j$ we then have $\epsilon_{r+k} = \epsilon_{i+k} = \epsilon_k$, since $j \in \mathcal{P}$ and $i \in \mathcal{P}$. For each l with $0 < l < p - r$ there is an integer k with $1 \leq k \leq j$ so that $l \equiv k \mod j$ and $\epsilon_{l+r} = \epsilon_{k+r} = \epsilon_k = \epsilon_l$. Thus, $r \in \mathcal{P}$. We can repeat the argument with j and r instead of i and j, and by the Euclidean algorithm it follows that $\gcd(i, j) \in \mathcal{P}$. □

Theorem 5. *If $s = p-1$ then $\mathcal{D} = \{1\}$ and $\mathcal{E} = \{0, 1\}$. Otherwise the map $f\colon \mathcal{M} \to \mathcal{D}$ given by $f(i) = \operatorname{rem}(p, i)$ is a bijection, and $\mathcal{E}$ is the disjoint union $\{0\} \cup \mathcal{M} \cup \mathcal{D}$.*

Proof. If $s = p-1$ we have $\epsilon_1 = \cdots = \epsilon_{p-1} = 1$, and the result is obvious. So assume $0 < s < p-1$.

Suppose that $i \in \mathcal{M}$. If $i \mid p$ then $i, p-i \in \mathcal{P}$, and $s = p-1$ by Lemma 4, contradicting our assumption. It follows that $f(i) > 0$. By Lemma 4, and minimality of $i \in \mathcal{P}$ we see that there is no $j \in \mathcal{P}$ with $j \leq f(i)$. This implies that $a_j = m_j + 1$ for all j with $0 < j \leq f(i)$. Using $i \in \mathcal{P}$ again, and Lemma 2 we see that for each j with $0 < j < f(i)$ we have $\epsilon_j = \epsilon_{p-f(i)+j} = \epsilon_{f(i)-j+1}$, so $\epsilon_1, \ldots, \epsilon_{f(i)}$ is a palindrome. This implies that for each j with $0 < j < f(i)$ we have

$$a_{f(i)} = a_j + a_{f(i)-j} = a_j + 1 + m_{f(i)-j} > a_j + m_{f(i)-j},$$

which implies that $f(i) \in \mathcal{D}$. Secondly, this gives

$$m_{f(i)} = a_{f(i)} - 1 > a_j + m_{f(i)-j} - 1 = m_j + m_{f(i)-j},$$

which shows that $f(i) \in \mathcal{E}$. This proves that $f(\mathcal{M}) \subset \mathcal{D}$ and $f(\mathcal{M}) \subset \mathcal{E}$.

Now suppose that $i \in \mathcal{D}$. Then for each j with $0 < j < i$ we have

$$a_j + m_{i-j} < a_i \leq a_j + a_{i-j} \leq a_j + m_{i-j} + 1,$$

so $a_{i-j} = m_{i-j} + 1$ and $a_i = a_j + a_{i-j}$. It follows from the first equality that we have $j \notin \mathcal{P}$ for each j with $0 < j < i$. The second equality implies that $\epsilon_1, \ldots, \epsilon_i$ is a palindrome, so for each j with $0 < j < i$ we have $\epsilon_j = \epsilon_{i-j+1} = \epsilon_{p-i+j}$, and it follows that $p-i \in \mathcal{P}$. There is an element $k \in \mathcal{M}$ with $k \mid p-i$, and we know that $k \geq i$. If $k = i$ then $1 \in \mathcal{P}$ by Lemma 4, and $s = p-1$. So $k > i$ and $i = \mathrm{rem}(p, k)$. This shows that $\mathcal{D} \subset f(\mathcal{M})$.

We now show that f is injective. Suppose that $k = \mathrm{rem}(p, i) = \mathrm{rem}(p, j)$ for $i, j \in \mathcal{M}$ with $i \neq j$. Then $\mathrm{lcm}(i, j) \mid p - k$ so $i + j < \mathrm{lcm}(i, j) \leq p - k \leq p$. With Lemma 4 it follows that $\gcd(i, j) \in \mathcal{P}$, which contradicts minimality of the periods i and j. This shows that f is a bijection from $\mathcal{M}$ to $\mathcal{D}$.

In order to show that $\mathcal{M} \subset \mathcal{E}$, let $i \in \mathcal{M}$ and $0 < j < i$. We have

$$m_i = a_i \geq a_j + m_{i-j} \geq m_j + m_{i-j};$$
$$m_i = a_i \geq a_{i-j} + m_j \geq m_j + m_{i-j}.$$

If $m_i = m_j + m_{i-j}$ then $a_j = m_j$ and $a_{i-j} = m_{i-j}$, so $j, i-j \in \mathcal{P}$. By Lemma 4 the strict divisor $\gcd(j, i-j)$ of i then lies in $\mathcal{P}$, contradicting minimality of i. We deduce that $i \in \mathcal{E}$.

We have proved that $\mathcal{M} \cup \mathcal{D} \subset \mathcal{E} \backslash \{0\}$, and we now prove the other inclusion. Suppose $i \in \mathcal{E}$ with $i \neq 0$ and $i \notin \mathcal{D}$. We will show that $i \in \mathcal{M}$. Since $i \notin \mathcal{D}$, there is an integer j with $0 < j < i$ and $a_i = m_j + a_{i-j}$. Since $i \in \mathcal{E}$ we also have

$$m_j \leq m_i - m_{i-j} - 1 \leq m_i - a_{i-j} \leq a_i - a_{i-j} = m_j,$$

so all inequalities are equalities. It follows that $a_i = m_i$, and $i \in \mathcal{P}$. If i has a strict divisor $l \in \mathcal{P}$, we have $m_i = m_l + m_{i-l}$, which contradicts that $i \in \mathcal{E}$. Therefore we have $i \in \mathcal{M}$.

Finally, if the union $\{0\} \cup \mathcal{M} \cup \mathcal{D}$ is not disjoint, then there is an integer $i \in \mathcal{M} \cap \mathcal{D}$ with $i, p-i \in \mathcal{P}$, so $s = p-1$ by Lemma 4. □

Proof of Theorem 1. See the Corollary to Proposition 3 for the case $s = 0$ and $s = p-1$. In the other cases Theorems 4 and 5 give $d = \#\mathcal{D} = \#\mathcal{M}$, and $\operatorname{edim}(R) = \#\mathcal{E} = 1 + \#\mathcal{M} + \#\mathcal{D} = 1 + 2d$. □

In order to prove Theorems 2 and 3 we give an inductive procedure to break down our balanced sequence.

Define $g\colon\ \mathbb{Z} \to \mathbb{Z}$ by $g(i) \mapsto \lfloor i/x \rfloor$. Then for each $i \in \mathbb{Z}$ the point $(g(i), i)$ is on or above the line through the origin with slope $x = s/p$, and $(g(i)+1, i)$ is below this line. This implies that

$$\{1 + g(i)\colon\ i \in \mathbb{Z}\} = \{j \in \mathbb{Z} : \epsilon_j = 1\},$$

so for $i \geq 0$ the $(i+1)$th occurrence of a 1 in the sequence $\epsilon_1, \epsilon_2, \ldots$ is at $\epsilon_{1+g(i)}$.

Let us now write $y = T(x) = \lceil 1/x \rceil - 1/x$, and put $k = \lceil 1/x \rceil$. Then $x = 1/(k-y)$ with $k \in \mathbb{Z}$ and $0 \leq y < 1$. We will see below that this is the beginning of a continued fraction expansion of x.

The distance between the $(i+1)$th and the ith occurrence of the number 1 in $\epsilon_1, \epsilon_2, \ldots$ is

$$\begin{aligned} g(i) - g(i-1) &= \lfloor i(k-y) \rfloor - \lfloor (i-1)(k-y) \rfloor \\ &= k - (\lceil iy \rceil - \lceil (i-1)y \rceil) = k - \epsilon'_i, \end{aligned}$$

where $(\epsilon'_i)_i$ is the balanced sequence for the rational number y.

In the following example we give $\epsilon_1, \ldots, \epsilon_{19}$ for $x = 8/19$. We have $T(x) = 5/8$ and $k = 3$. For $i = 0, \ldots 7$ the number ϵ'_{1+i} is written below $\epsilon_{1+g(i)} = 1$.

1	0	1	0	1	0	0	1	0	1	0	1	0	0	1	0	1	0	0
1		1		0			1		1		0			1		0		

The next Proposition tells us how to express the set of minimal sub-periods $\mathcal{M}(x)$ of $\epsilon_1, \ldots, \epsilon_{p-1}$, in terms of the set of minimal sub-periods $\mathcal{M}(y)$ of $\epsilon'_1, \ldots, \epsilon'_{s-1}$.

Proposition 4. *If $p \equiv 1 \bmod s$ then $\mathcal{M}(x) = \{(p-1)/s\}$. Otherwise, we have $p-1 \in \mathcal{M}(x)$ and we have a bijection $\mathcal{M}(y) \to \mathcal{M}(x) \backslash \{p-1\}$ given by $i \mapsto g(i)$.*

Proof. The first statement is clear: if $p = us + 1$ then $\epsilon_1, \ldots, \epsilon_{p-1}$ consists of s consecutive blocks of a 1 followed by $u-1$ zeroes, so $\mathcal{P} = \{i \in u\mathbb{Z}\colon\ 1 \leq i < p\}$, and $\mathcal{M}(x) = \{u\}$.

For the rest of the proof, assume that $p \not\equiv 1 \bmod s$. Therefore $s \neq 1$ and $0 < y < 1$. We have $\epsilon'_s = 0$ and $g(s-1) = p - k$.

We first show that $g(\mathcal{P}(y)) \subset \mathcal{P}(x)$. Suppose that $i \in \mathcal{P}(y)$. All blocks in $\epsilon'_1, \ldots, \epsilon'_{s-1}$ of length i have the same sum, so all blocks in $\epsilon_1 \ldots, \epsilon_{g(s-1)}$ of sum i starting with a 1 which are not followed by a 0, have the same length, and this length is $g(i)$. We get the sequence $\epsilon_1 \ldots, \epsilon_{p-1}$ by adding a 1, and $k-2$ zeroes. It is not hard to see that in this longer sequence each block of length $g(i)$ has sum i, so that $g(i) \in \mathcal{P}(x)$. This shows that $g(\mathcal{P}(y)) \subset \mathcal{P}(x)\backslash\{p-1\}$.

Now suppose that $j \in \mathcal{P}(x)$ with $1 \leq j < p-1$. Then $\epsilon_{j+1} = \epsilon_1 = 1$ so $j = g(i)$ for some i with $1 \leq i < s$. For l with $1 \leq l < s$ the symbol ϵ'_l is determined by the distance between the l-th and the $(l+1)$th occurrence of the number 1 in the sequence $\epsilon_1, \ldots, \epsilon_{p-1}$. Since this sequence is obtained by repeating a block containing i symbols 1, this distance depends only on l mod i. Thus, $i \in \mathcal{P}(y)$.

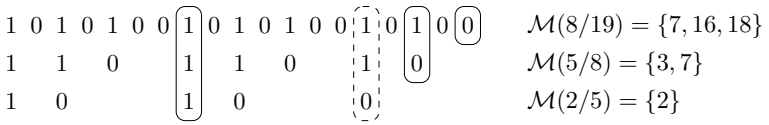
This shows that g gives a bijection $\mathcal{P}(y) \to \mathcal{P}(x)\backslash\{p-1\}$. If i is in $\mathcal{P}(y)$, then for $j \geq 1$ with $i + j < s$ the distance from the $(i+j+1)$th number 1 to the $(i+1)$th is equal to the distance between the $(j+1)$th and the first, so we have $g(i+j) = g(i) + g(j)$. This implies that the bijection $g\colon \mathcal{P}(y) \to \mathcal{P}(x)\backslash\{p-1\}$ preserves the divisibilities, so that we obtain a bijection $\mathcal{M}(y) \to \mathcal{M}(x)\backslash\{p-1\}$.

It remains to show that $p-1 \in \mathcal{M}(x)$. Assume this is false. We have $p-1 \in \mathcal{P}(x)$, so $l \in \mathcal{M}(x)$ for a strict divisor l of $p-1$. Writing $jl = p-1$, we see that j is a strict divisor of s and that $l = g(s/j)$. By applying Lemma 4 to $s/j, s - s/j \in \mathcal{P}(y)$ it follows that $1 \in \mathcal{P}(y)$, which in turn implies that $p \equiv 1 \bmod s$, contradicting our assumption. □

Iterating the operator T computes the Hirzebruch continued fraction of $-x$; see [7]. For instance, if we start with $x = 8/19$ then $T(x) = 5/8$ and $T(T(x)) = 2/5$, and we get

$$-\frac{8}{19} = -\cfrac{1}{3-\frac{5}{8}} = -\cfrac{1}{3-\cfrac{1}{2-\frac{2}{5}}} = -\cfrac{1}{3-\cfrac{1}{2-\cfrac{1}{3-\frac{1}{2}}}}\,.$$

The proposition above implies that we can count $\mathcal{M}(x)$ by iterating T on our rational number x until we have a number a/b with $a \mid b-1$. In the picture below we outline $\{\epsilon_{i+1} : i \in \mathcal{M}(x)\}$ for the values x we encounter starting from 8/19. We outlined ϵ_{i+1} for the non-minimal $i \in \mathcal{P}$ with a dashed line.



Proof of Theorems 2 *and* 3. In Proposition 4 we have $y = T(s/p)$ satisfies $y = \mathrm{rem}(-p, s)/s$, so Theorem 2 follows from Proposition 4 and Theorem 5.

In order to deduce Theorem 3, recall first that the Hirzebruch continued fraction expansion of $-x$ is

$$-x = -\frac{s}{p} = -\cfrac{1}{y_1 - \cfrac{1}{\ddots \quad \cfrac{\ddots}{y_{n-1} - \cfrac{1}{y_n}}}}$$

for integers $n \geq 1$ and $y_1, \ldots, y_n \geq 2$, which are given by $y_i = \lceil 1/T^{i-1}(x) \rceil$ and $T^n(x) = 0$.

We have the following rewriting rule [8, (19) p. 215] between the usual continued fraction and the Hirzebruch continued fraction. For integers u, v with $v \geq 1$ and a rational number $w > 1$ we have

$$u + \cfrac{1}{v + \cfrac{1}{w}} = u + 1 - \cfrac{1}{2 - \cfrac{1}{\ddots \quad \cfrac{\ddots}{2 - \cfrac{1}{w+1}}}},$$

where the number of symbols 2 on the right is $v - 1$.

The rule also holds when $w = \infty$, that is, when we replace $1/w$ and $1/(w+1)$ by 0. This implies that we have $s = p-1$ if and only if $y_1 = y_2 = \ldots = y_n = 2$, and we have $s \mid p-1$ if and only if $y_2 = y_3 = \ldots = y_n = 2$. Thus, Proposition 4 implies that if $s \neq p-1$, the number d is the largest $i \leq n$ with $y_i \neq 2$. Starting with the continued fraction in Theorem 3 we can apply the rewriting rule repeatedly to find the Hirzebruch continued fraction expansion of $-x$. Then we find that the largest $i \leq n$ with $y_i \neq 2$ is the sum of all odd x_i with $i < m$. □

References

[1] A. AIBA, Artin-Schreier extensions and Galois module structure. J. Number Theory, **102**, 118–124 (2003).

[2] F. BERTRANDIAS AND M.-J. FERTON, Sur l'anneau des entiers d'une extension cyclique de degré premier d'un corps local. C. R. Acad. Sci. Paris Sér. A **274**, 1330–1333 (1972).

[3] F. BERTRANDIAS, J.-P. BERTRANDIAS AND M.-J. FERTON, Sur l'anneau des entiers d'une extension cyclique de degré premier d'un corps local. C. R. Acad. Sci. Paris Sér. A **274**, 1388–1391 (1972).

[4] N. BOURBAKI, Algèbre I, Hermann, Paris, 1970 [English translation: Algebra I, Addison Wesley, Reading, 1974].

[5] N. P. Byott, Review of [1] in Mathematical Reviews, MR1994476 (2004f:11127). American Mathematical Society, 2004.

[6] H. Hasse, Theorie der relativ-zyklischen algebraischen Funktionenkörper, insbesondere bei endlichem Konstantenkörper. J. Reine Angew. Math. **172**, 37–54 (1934).

[7] F. Hirzebruch, Über vierdimensionale Riemannsche Flächen mehrdeutiger analytischer Funktionen von zwei komplexen Veränderlichen. Math. Ann. **126**, 1–22 (1953).

[8] F. Hirzebruch, Hilbert modular surfaces. Ens. Math. **19**, 183–281 (1973).

[9] G. Lettl, Note on a theorem of A. Aiba. J. Number Theory **115**, 87–88 (2005).

[10] M. Lothaire, Algebraic combinatorics on words. Encyclopedia of Mathematics and its Applications **90**, Cambridge University Press, 2002.

[11] J-P. Serre, Corps locaux, Hermann, Paris, 1962 [English translation: Local fields. Springer-Verlag GTM 67, New York, 1979].

Bart de Smit, Mathematisch Instituut, Universiteit Leiden, Postbus 9512, NL-2300 RA Leiden, Netherlands
e-mail: desmit@math.leidenuniv.nl

Lara Thomas, Chaire de Structures Algébriques et Géométriques, Ecole Polytechnique Fédérale de Lausanne, CH-1015 Lausanne, Switzerland
e-mail: lara.thomas@epfl.ch

Received: 19 March 2006