Artin-Schreier Extensions and Generalized Associated Orders

Duc Van Huynh

Department of Mathematics, University of Florida, Gainesville, FL 32611-8105

Abstract

Let k be the local field $\mathbb{F}_q((T))$, where q is a power of a prime number p. Let L be a totally ramified Artin-Schreier extension of degree p over k and G its Galois group, and let v be a valuation of L such that $v(T) = 1$. Define $M_L^r = \{x \in L : v(x) \geq \frac{r}{p}\}$. We give a basis for the O_k-module $A_{r,b}(L/k) = \{x \in k[G] : x \cdot M_L^r \subset M_L^b\}$. Moreover, we determine the conditions for which M_L^r is free over the ring $A_{r,r}$.

1. Introduction and Results

Set $k = \mathbb{F}_q((T))$, where q is a power of a prime p. Let L be an Artin-Schreier extension of degree p over k, and set $G = Gal(L/k)$. Let v be the discrete valuation on L defined by $v(T) = 1$, let O_L denote the valuation ring of L, that is, $O_L = \{x \in L : v(x) \geq 0\}$. Let $M_L^r = \{x \in L | v(x) \geq \frac{r}{p}\}$. Note that $M_L^0 = O_L$. In [1], A. Aiba constructed an explicit basis for $A(L/k) = \{x \in k[G] : x \cdot O_L \subset O_L\}$ over O_k. Furthermore, he showed that O_L is a free A-module under certain conditions. In the same fashion as [1], we will construct an explicit basis for

$$A_{r,b}(L/k) = \{x \in k[G] : x \cdot M_L^r \subset M_L^b\}$$

and determine the conditions for which M_L^r is a free $A_{r,r}$-module. Note that $A_{0,0} = A(L/K)$ above.

When $b = r$, $A_{r,r}$ is a ring with 1, and so M_L^r is a module over $A_{r,r}$. We will describe conditions below for which M_L^r is a free module over $A_{r,r}$. From now on, set $A_r = A_{r,r}$.

Write $r = pf + r_0$, where $0 \leq r_0 \leq p-1$. Then for $x \in A_r$, we have $x \cdot M_L^r \subset M_L^r$ if and only if $x(M_L^{r_0}) \subset M_L^{r_0}$ since $x(M_L^r) = T^f(x \cdot M_L^{r_0})$. Hence, we may assume that $0 \leq r < p$.

In [6], Ferton studies the case of a totally ramified Galois extension K/k of degree p, where k is a local field with characteristic 0. She first constructs θ_r, for $0 \leq r \leq p-1$, such that it generates a normal basis for K/k. She then

Email address: dhuynh@ufl.edu (Duc Van Huynh)

studies $\mathfrak{U}_r = \{x \in k[G] : x\theta_r \in M_K^r\}$. An explicit set of generators for $\mathfrak{U}_r$ is then constructed, which turns out to be very similar to the generators for our O_k-modules A_r. She shows that M_K^r is A_r-free if and only if A_r coincides with $\mathfrak{U}_r$. She then gives the explicit conditions involving the ramification break λ and r for which A_r and $\mathfrak{U}_r$ coincide, which is equivalent to the conditions for which M_K^r is A_r-free. Her results turn out to be exactly the same as the results in this paper in the case when $0 < \lambda < \dfrac{pe}{p-1} - 1$.

Our approach in this paper is different from Ferton's. We will generalize the criterion equivalent to $M_L^0 = O_L$ being A_0-free given by Aiba in [1]. We will study that criterion and extend the techniques of Lettl in [9] to find exactly when M_L^r is A_r-free in terms of λ and r.

In the case when L/k is unramified, we have from Proposition 2.1 of [10] that $A_r = O_k[G]$ and that M_L^r is free over $O_k[G]$. So we will focus on the case when L/k is totally ramified.

Let F be a local field with residue characteristic p. When N is an Artin-Schreier extension of degree p over F, the Galois group G of N/F has a unique ramification break. Recall that an integer i is called a lower ramification break if $G_i \neq G_{i+1}$, where

$$G_i = \{\sigma \in G : \sigma(b) - b \in M_L^{i+1}, \forall b \in O_L\}.$$

By Artin-Schreier Theory we have $N = F(\alpha)$, where α is a root of $X^p - X - \beta$, for some $\beta \in F$. When N/F is totally ramified, by Proposition 2.4, pg. 75 of [4], the element β can be chosen so that $v_F(\beta) = -\lambda$ is relatively prime to p and λ is the unique ramification break of N/F.

Write $L = k(\alpha)$, where α is a root of the equation

$$P(X) = X^p - X - \beta = 0.$$

It follows that $v(\alpha) = \dfrac{-\lambda}{p}$, where $-\lambda = v(\beta)$. As mentioned above, λ is relatively prime to p and is the unique ramification break of the Galois group G of L/k. So we can write $\lambda = pt + s$, where t and s are integers with $1 \leq s \leq p-1$. From elementary Galois theory, we know that $G =< \sigma >$, where $\sigma(\alpha) = \alpha + 1$.

Let $\{x\}$ denote the fractional part of a real number x, that is, $0 \leq \{x\} < 1$ such that $x - \{x\} \in \mathbb{Z}$. We know that $(-x) - \lfloor -x \rfloor = \{-x\}$.

Lemma 1.1.

$$M_L^r = \sum_{u=0}^{p-1} O_k \alpha^u T^{tu+\gamma_r(u)}$$

where $\gamma_r(u) = -\left\lfloor -\left(\frac{su+r}{p}\right)\right\rfloor$, and $\lambda = pt + s$ where $1 \leq s \leq p-1$.

Proof. Note that we have

$$v\left(\alpha^u T^{tu+\gamma_r(u)}\right) = -\frac{pt+s}{p}u + tu + \gamma_r(u) = \left(-\frac{su}{p}\right) - \left\lfloor -\left(\frac{su+r}{p}\right)\right\rfloor.$$

However,

$$\left(-\frac{su}{p}\right) - \left\lfloor -\left(\frac{su+r}{p}\right)\right\rfloor = \left(-\frac{su+r}{p}\right) - \left\lfloor -\left(\frac{su+r}{p}\right)\right\rfloor + \frac{r}{p}$$
$$= \left\{-\frac{us+r}{p}\right\} + \frac{r}{p}$$

We see that the valuations of the p elements $\alpha^u T^{tu+\gamma_r(u)}$ $(0 \le u \le p-1)$ are distinct and lie between $\frac{r}{p}$ and $\frac{p-1+r}{p}$. Hence, we have the desired result. □

For convenience, let

$$N_{u,m,r} = \gamma_r(u) - \frac{us}{p} + \frac{ms}{p} - \gamma_0(m) = -\left\lfloor -\left(\frac{us+r}{p}\right)\right\rfloor - \frac{us}{p} - \left\{\frac{-ms}{p}\right\},$$

where $0 \le m \le u \le p-1$. Set $\gamma'_{r,b}(m) = \gamma_0(m) - \rho_{m,r,b}$, where $\rho_{m,r,b}$ is the smallest integer such that $N_{u,m,r} + \rho_{m,r,b} \ge \frac{b}{p}$ for all u with $0 \le m \le u \le p-1$.

Remark 1.2. For each $m \ge 0$, taking $b = r$, we have $\rho_{m,r,r} = 1$ if there exists u with $m \le u \le p-1$ such that $N_{u,m,r} < \frac{r}{p}$, and $\rho_{m,r,r} = 0$ otherwise. This is due to the fact that $N_{u,m,r}$ is bounded below by $\frac{r+1-p}{p}$ and above by $\frac{p+r-1}{p}$.

Theorem 1.3. Let $L = k(\alpha)$ be a totally ramified cyclic extension of k of degree p, where α is a root of

$$X^p - X - \beta = 0,$$

with $v(\beta) = -\lambda$ and $\lambda = pt + s$ with $(0 < s \le p-1)$.
Then we have the following:

(i)
$$A_{r,b}(L/k) = \sum_{m=0}^{p-1} O_k \varphi_m,$$

where
$$\varphi_m = \frac{1}{T^{mt+\gamma'_{r,b}(m)}}(\sigma - 1)^m.$$

(ii) Let s be fixed. Let n_i be the least positive integer such that $sn_i \equiv i$ (mod p).
If $s < r$, then M_L^r is a free $A_r(L/k)$-module if and only if

$$\frac{p+3}{2} \le r \le p-1, \text{ and } s = 1.$$

If $s \ge r$, then M_L^r is a A_r-free module if and only if r satisfies either of the following conditions:

(a) $r = s$ or $r = s - \left\lfloor \frac{p}{p-n_1} \right\rfloor$ if $n_1 \ge \frac{p}{2}$;

(b) $s - \frac{1}{2}\frac{p}{n_1} \leq r \leq s$ if $n_1 < \frac{p}{2}$.

Corollary 1.4. M_L^0 is A_0-free if and only if $s \mid (p-1)$.

Proof. This is clear if $p = 2$, so we may assume $p > 2$. If M_L^0 is A_0-free, then from Theorem 1.3(ii), either $s = \left\lfloor \frac{p}{p-n_1} \right\rfloor$ or $s \leq \left\lfloor \frac{p}{2n_1} \right\rfloor$. If $s \leq \left\lfloor \frac{p}{2n_1} \right\rfloor$, then $p \geq 2n_1 s$, but this inequality happens only when $s = n_1 = 1$, which, in this case, we have $s \mid p-1$. Now if $s = \left\lfloor \frac{p}{p-n_1} \right\rfloor$, then

$$s \leq \frac{p}{p-n_1} < s+1, \tag{1}$$

which implies

$$p - \frac{p}{s} \leq n_1 < p - \frac{p}{s+1}. \tag{2}$$

Multiply (2) by s and write $sn_1 = 1 + kp$ for some integer k. We obtain the inequalities

$$p(s-1) \leq sn_1 < ps - \frac{ps}{s+1}, \tag{3}$$

which implies $k = s-1$. Then $n_1 = p - \frac{p-1}{s}$, and hence, $s \mid p-1$.

Conversely, suppose that $s \mid p-1$. Then $n_1 = p - \frac{p-1}{s}$. When $s = 1$, we get $n_1 = 1 < \frac{p}{2}$. By Theorem 1.3(ii), M_L^r is A_r-free for all r satisfying

$$s - \frac{p}{2n_1} \leq r \leq s.$$

But $s - \frac{p}{2n_1} < 0$. Hence, M_L^0 is A_0-free. When $s > 1$, we have $n_1 > \frac{p}{2}$. By Theorem 1.3(ii), M_L^r is A_r-free when $r = s - \left\lfloor \frac{p}{p-n_1} \right\rfloor = 0$ since $n_1 = p - \frac{p-1}{s}$. □

Remark 1.5. From the corollary above, we have M_L^0 is A_0-free if and only if $s \mid (p-1)$. This result has already been proven by Aiba and Lettl in [1] and in [9]. The same result was also shown to hold when L has characteristic 0 by Bertrandias and Ferton in [5].

Remark 1.6. Write the fraction $\frac{s}{p}$ as the continued fraction $[0; a_1, a_2, \ldots, a_m]$, that is,

$$\frac{s}{p} = \cfrac{1}{a_1 + \cfrac{1}{a_2 \cfrac{1}{\ddots + \cfrac{1}{a_m}}}}$$

In [6], Ferton studied the case when K/k is cyclic of degree p, where k is a local field of characteristic 0. When $s = 0$, which does not happen in the characteristic p case, she showed that M_L^r is A_r-free for all $0 \leq r \leq p-1$. When $s = 1$ and $\lambda < \dfrac{pe}{p-1} - 1$, she showed that A_r is free if and only if $r \geq \dfrac{p+3}{2}$. When $s \geq 2$ and $\lambda < \dfrac{pe}{p-1} - 1$, she showed that M_L^r is A_r-free if only if r satisfies $r = s$ or $r = s - a_m$ when m is even, and $s - \dfrac{a_m}{2} \leq r \leq s$ when m is odd. We will show below that Ferton's results agree with the results in Theorem 1.3(ii).

Theorem 1.7. Assume the notations of Theorem 1.3 and Remark 1.6. Then

$$a_m = \left\lfloor \frac{p}{p - n_1} \right\rfloor \text{ if } m \text{ is even, and}$$

$$\left\lfloor \frac{a_m}{2} \right\rfloor = \left\lfloor \frac{1}{2} \frac{p}{n_1} \right\rfloor \text{ if } m \text{ is odd.}$$

Furthermore, $n_1 \geq \dfrac{p}{2}$ if and only if m is even.

Proof. (This proof is due to the referee.) We will apply the Extended Euclidean Algorithm. Set $r_{-1} = p, r_0 = s, x_{-1} = 1, y_{-1} = 0, x_0 = 0, y_0 = 1$. For $j \geq 1$, let $r_{j-2} = a_j r_{j-1} + r_j$ with $0 \leq r_j < r_{j-1}$, and for $j \geq 0$, set $x_{j+1} = a_{j+1}x_j + x_{j-1}$ and $y_{j+1} = a_{j+1}y_j + y_{j-1}$, stopping when the decreasing sequence (r_j) of remainders terminates with $r_m = 0$. Then $r_{m-1} = \gcd(p, s) = 1$, and we have the continued fraction expansion $s/p = [0; a_1, \ldots, a_m]$ with $a_m \geq 2$. Moreover, by induction, we have

$$x_j p - y_j s = (-1)^{j+1} r_j \text{ for } -1 \leq j \leq m \tag{4}$$

and

$$x_{j-1}y_j - x_j y_{j-1} = (-1)^j \text{ for } 0 \leq j \leq m. \tag{5}$$

By taking $j = m - 1$ in (4), we obtain the Bezout Identity

$$x_{m-1}p - y_{m-1}s = (-1)^m. \tag{6}$$

And by taking $j = m$ in (4), we get $x_m p = y_m s$. Since $\gcd(x_m, y_m) = 1$ by (5) and clearly $x_m > 0$, we deduce that $x_m = s$ and $y_m = p$.

First suppose that m is even. From (6) we have $y_{m-1}s \equiv p - 1 (\mathrm{mod}\ p)$. Since $0 < y_{m-1} < p$, we have $p - n_1 = n_{p-1} = y_{m-1}$. It follows that

$$\left\lfloor \frac{p}{p - n_1} \right\rfloor = \left\lfloor \frac{y_m}{y_{m-1}} \right\rfloor = a_m.$$

Furthermore, since $p = y_m = a_m y_{m-1} + y_{m-2}$, $a_m \geq 2$ and $n_1 = p - y_{m-1}$, we have

$$n_1 = \frac{p(a_m - 1)}{a_m} + \frac{y_{m-2}}{a_m} \geq \frac{p}{2}.$$

Next suppose that m is odd. Then (6) gives $y_{m-1} = n_1$. Thus,

$$\left\lfloor \frac{1}{2}\frac{p}{n_1} \right\rfloor = \left\lfloor \frac{1}{2}\frac{y_m}{y_{m-1}} \right\rfloor = \left\lfloor \frac{1}{2}\left(a_m + \frac{y_{m-2}}{y_{m-1}}\right) \right\rfloor = \left\lfloor \frac{1}{2}a_m \right\rfloor,$$

where the last equality is due to the fact that $\dfrac{y_{m-2}}{y_{m-1}} < 1$ and a_m is an integer.

Furthermore, since $p = y_m = a_m y_{m-1} + y_{m-2}$, $a_m \geq 2$ and $n_1 = y_{m-1}$, we have

$$n_1 = \frac{p - y_{m-2}}{a_m} < \frac{p}{2}.$$

□

Corollary 1.8. Assume the same notations as the Theorem 1.7. Let $c = \left\lfloor \dfrac{a_m}{2} \right\rfloor$. Then we have

$$p - \frac{p}{a_m} \leq n_1 < p - \frac{p}{a_m + 1} \text{ if } m \text{ is even, and}$$

$$\frac{p}{2(c+1)} < n_1 \leq \frac{p}{2c} \text{ if } m \text{ is odd.}$$

Example. Let $p = 29$. The table below is generated from a double inequality, which will be mentioned in Remark 3.3 and studied carefully Section 4. In Section 3, we will show that a pair (r, s) satisfying the double inequality is equivalent to M_L^r being A_r-free. Each entry in the table below represents a pair (r, s). The entry is 0 if and only if M_L^r is not A_r-free, and the entry is $\sim$ if and only if M_L^r is A_r-free. For instance, when $s = 19$, M_L^{10} is A_{10}-free.

s	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	r
	∼	∼	0	∼	0	0	∼	0	0	0	0	0	0	∼	0	0	0	0	0	0	0	0	0	0	0	0	0	∼	0
	∼	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
	0	∼	∼	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	2
	0	0	∼	0	∼	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	3
	0	0	0	∼	∼	∼	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	4
	0	0	0	0	∼	∼	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	5
	0	0	0	0	0	∼	0	0	0	∼	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	6
	0	0	0	0	0	0	∼	∼	0	∼	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	7
	0	0	0	0	0	0	0	∼	∼	∼	0	0	0	0	∼	0	0	0	0	0	0	0	0	0	0	0	0	0	8
	0	0	0	0	0	0	0	0	∼	∼	0	0	0	0	∼	0	0	0	0	0	0	0	0	0	0	0	0	0	9
	0	0	0	0	0	0	0	0	0	∼	∼	∼	0	0	∼	0	0	0	∼	0	0	0	0	0	0	0	0	0	10
	0	0	0	0	0	0	0	0	0	0	∼	0	0	0	∼	0	0	0	0	0	0	0	0	0	0	0	0	0	11
	0	0	0	0	0	0	0	0	0	0	0	∼	∼	0	∼	0	0	0	0	0	0	0	0	0	0	0	0	0	12
	0	0	0	0	0	0	0	0	0	0	0	0	∼	0	∼	∼	0	0	0	0	0	0	0	0	0	0	0	0	13
	0	0	0	0	0	0	0	0	0	0	0	0	0	∼	∼	0	0	0	0	0	0	0	0	0	0	0	0	0	14
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	∼	0	0	∼	0	0	0	0	0	0	0	0	0	0	15
	∼	0	0	0	0	0	0	0	0	0	0	0	0	0	0	∼	∼	0	0	0	0	0	0	0	0	0	0	0	16
	∼	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	∼	0	0	0	0	0	0	0	0	0	0	0	17
	∼	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	∼	0	∼	0	0	∼	0	0	0	0	0	18
	∼	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	∼	0	∼	∼	0	0	0	0	0	0	19
	∼	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	∼	0	∼	0	∼	0	0	0	0	20
	∼	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	∼	∼	0	0	0	0	0	0	21
	∼	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	∼	0	0	0	0	0	0	22
	∼	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	∼	0	∼	0	0	0	23
	∼	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	∼	∼	∼	0	0	24
	∼	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	∼	0	0	0	25
	∼	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	∼	∼	0	26
	∼	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	∼	0	27
	∼	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	∼	28

2. A Few Lemmas

Lemma 2.1. (Nakayama, Lemma 4.2 of [8]) Let A be a local ring and m its maximal ideal. Let E be a finitely generated A-module, and let F be a submodule of E. If $E = F + mE$, then $E = F$.

Let F be a field of characteristic p. Set F^{alg} to be the algebraic closure of F, and set $\Omega = (F^{alg})^{\times}$, the multiplicative group of F^{alg}. For any finite abelian group B of order relatively prime to p, let $\widehat{B}$ be the set of group homomorphisms from B to μ_B, the group of $|B|$-th roots of unity of Ω. In fact, $\widehat{B}$ is a group. This is the analog to the group of characters with complex values.

Lemma 2.2. (Lemma 2 of [2]) Let $H = H_p \times H_1$ be a finite abelian group, where H_p is the Sylow p-subgroup of H. Let f be a function from H into a field F of characteristic p. Then

$$\det(f(\sigma\tau^{-1}))_{\sigma,\tau\in H} = \prod_{\chi\in\widehat{H_1}} \left(\sum_{\tau\in H_p} \left(\sum_{\sigma\in H_1} \chi(\sigma) f(\sigma\tau) \right) \right)^{|H_p|},$$

where $\widehat{H_1}$ is as defined above.

Remark 2.3. The lemma above is just an application of the Group Determinant Formula (pg. 71 of [11]) and adapting to the case of positive characteristic.

Corollary 2.4. Suppose N is an abelian extension of k such that $H = Gal(N/k)$ is a p-group. Then, for $\alpha \in N$,

$$\det(\alpha^{\sigma\tau^{-1}})_{\sigma,\tau\in H} = \left(Tr_{N/k}(\alpha)\right)^{|H|}.$$

Proof. Set $H = H_p, H_1 = 1$ and $f(\sigma) = \sigma(\alpha)$, and apply the lemma above. □

From now on, put $\det(b) = \det(b^{\sigma\tau^{-1}})_{\sigma,\tau\in H}$, for $b \in M_N^r$. Call an element $a \in M_N^r$ *minimal* if $\det(a)$ divides $\det(b)$ for all $b \in M_N^r$.

Lemma 2.5. Let N be a finite Galois extension of $k, H = Gal(N/k)$ and $A_r = A_r(N/k)$. Suppose that M_N^r is a free A_r-module, which is necessarily of rank one. Then, $A_r \cdot a = M_N^r$ if and only if a is *minimal*.

Proof. Suppose $A_r \cdot a = M_N^r$. Note that since $G \cdot a$ is linearly independent if and only if $\det(a) \neq 0$, and that the rank of $A_r \cdot a$ over O_k is $[N : k]$, we see that the set $H \cdot a$ is linearly independent over O_k, so $\det(a) \neq 0$. Let $b \in M_N^r$. If $\det(b) = 0$, then there is nothing to prove. So, we may assume that $H \cdot b$ is linearly independent over O_k. Then we have

$$\begin{aligned}
[M_N^r : (O_kH)\cdot b] &= [M_N^r : A_r \cdot b][A_r \cdot b : (O_kH)\cdot b] \\
&= [M_N^r : A_r \cdot b][A_r : O_kH] \\
&\text{and} \\
[M_N^r : (O_kH)\cdot b] &= [A_r \cdot a : (O_kH)\cdot a][(O_kH)\cdot a : (O_kH)\cdot b] \\
&= [A_r : O_kH][(O_kH)\cdot a : (O_kH)\cdot b].
\end{aligned}$$

Hence we have the following equality of ideals in O_k (2.4 of [7], pg. 121):

$$\det(a)^2[M_N^r : A_r \cdot b]^2 = \det(a)^2[(O_kH) \cdot a : (O_kH) \cdot b]^2 = \det(b)^2. \qquad (7)$$

So, $\det(a)$ divides $\det(b)$ for all $b \in M_N^r$.

Conversely, suppose a is *minimal*, that is, $\det(a)$ divides $\det(b)$ for all $b \in M_N^r$, and $A_r \cdot c = M_N^r$ for some $c \in M_N^r$. Then, in particular, $\det(a)$ divides $\det(c)$. Since $A_r \cdot a$ is a submodule of M_N^r, we have $\det(c)$ divides $\det(a)$ by (7). Therefore, $A_r \cdot a$ has index 1 in $A_r \cdot c$ and so $A_r \cdot a = A_r \cdot c = M_N^r$. □

Lemma 2.6. (Lemma 3 of [2]) Let $\alpha_1, ..., \alpha_t$ be arbitrary numbers in L. Set $\sigma_n = \sum_{i=1}^{t} \alpha_i^n$, $f(x) = \prod_{i=1}^{t}(1 - \alpha_i x)$ and $g(x) = \sum_{i=1}^{\infty} \sigma_n x^n$. Then

$$g(x) = \frac{-xf'(x)}{f(x)},$$

where $f'(x)$ is the formal derivative of $f(x)$.

Lemma 2.7. Let $\zeta = \alpha^{p-1}T^{t(p-1)+\gamma_r(p-1)} \in M_L^r$. If M_L^r is A_r-free, then $M_L^r = A_r \cdot \zeta$.

Proof. Let $f(x) = X^pP(1/X) = 1 - X^{p-1} - \beta X^p = \prod_{i=0}^{p-1}(1 - \alpha_i X)$, where $\alpha_i = \alpha + i$. By Applying Lemma 2.6, we have

$$Tr_{L/k}(\alpha^i) = \begin{cases} -1 & \text{if } i = p-1 \\ 0 & \text{if } 0 \le i < p-1 \end{cases}$$

By Corollary 2.4, $\det(\zeta) = \left(-T^{t(p-1)+\gamma_r(p-1)}\right)^p$ while for $0 \le u \le p-2$ we have $\det(\alpha^u T^{t(u)+\gamma_r(u)}) = 0$. Linearity of trace and Lemma 2.5 implies $A_r \cdot \zeta = M_L^r$. □

Corollary 2.8. If M_L^r is A_r-free, then $A_r = \{x \in k[G] : x \cdot \zeta \in M_L^r\}$.

Proof. Set $B = \{x \in k[G] : x \cdot \zeta \in M_L^r\}$. Since M_L^r is A_r-free, $M_L^r = A_r \cdot \zeta$ by Lemma 2.7. Hence, $x \in A_r$ if only if $x \cdot \zeta \in M_L^r$ if and only if $x \in B$. □

3. The First Step

Lemma 3.1. For $0 \le u, m \le p-1$,

$$\varphi_m \cdot \alpha^u T^v = \begin{cases} 0 & u < m \\ \dfrac{m!T^v}{T^{mt+\gamma'_{r,b}(m)}} & u = m \end{cases}$$

And for the case $u > m$,

$$\varphi_m \cdot \alpha^u T^v = \frac{T^v}{T^{mt+\gamma'_{r,b}(m)}} \sum_{u_1=m-1}^{u-1} \binom{u}{u_1} \sum_{u_2=m-2}^{u_1-1} \binom{u_1}{u_2} \cdots \sum_{u_m=0}^{u_{m-1}-1} \binom{u_{m-1}}{u_m} \alpha^{u_m}$$

Proof. The cases $u < m$ and $u = m$ are clear. Due to how φ_m is defined and that it acts trivially on T^v for any integer v, it is enough to look at how $(\sigma-1)^m$ acts on α^u. But $(\sigma-1)(\alpha^u) = \binom{u}{0}\alpha^0 + \binom{u}{1}\alpha^1 + \binom{u}{2}\alpha^2 + \cdots + \binom{u}{u-1}\alpha^{u-1}$. If we inductively apply $\sigma - 1$ and use the results for $u < m$ and $u = m$, we get the desired result for $u > m$. □

Theorem 3.2. Let $L = k(\alpha)$ be a wildly ramified cyclic extension of k of degree p, where α is a root of

$$X^p - X - \beta = 0,$$

with $v(\beta) = -\lambda$ and $\lambda = pt + s$ with $0 < s \leq p-1$. Then

$$A_{r,b}(L/k) = \sum_{m=0}^{p-1} O_k \varphi_m,$$

where

$$\varphi_m = \frac{1}{T^{mt+\gamma'_{r,b}(m)}}(\sigma-1)^m.$$

Furthermore, M_L^r is a free $A_r(L/k)$-module if and only if there do not exist integers $0 \leq m \leq n \leq p-1$ such that

$$N_{p-1,m,r} \geq \frac{r}{p} > N_{n,m,r}. \tag{8}$$

Remark 3.3. Note that the first assertion of the theorem above is exactly the assertion in Theorem 1.3(i), and it is a generalization of the main theorem of Aiba in [1]. Rewriting (8) from Theorem 3.2, we have

$$\left\{\frac{s-r}{p}\right\} \geq \left\{\frac{(k+1)s}{p}\right\} > \left\{\frac{(j+1)s-r}{p}\right\},$$

where $n = p-1-j, m = p-1-k$, and $0 \leq j \leq k \leq p-1$. Hence, the second property from Theorem 3.2 can be stated as:
M_L^r is a free $A_r(L/k)$-module if and only if there do not exist integers $1 \leq m \leq n \leq p-1$ such that

$$\left\{\frac{s-r}{p}\right\} \geq \left\{\frac{ns}{p}\right\} > \left\{\frac{ms-r}{p}\right\}. \tag{9}$$

If we let $r = 0$, we have exactly the same property as in [1].

In [1], Aiba showed that $M_L^0 = O_L$ is a free $A_{0,0}$-module if and only if s has the property that there are no integers m, n such that

$$1 \leq m < n \leq p-1 \text{ and } \frac{s}{p} > \left\{\frac{ns}{p}\right\} > \left\{\frac{ms}{p}\right\}.$$

We regret that we have accidentally chosen the variables m, n opposite that of Aiba in [1]. Aiba incorrectly stated the inequality as $1 < m < n < p-1$ and was corrected by Lettl in [9] to $1 \leq m < n \leq p-1$. In [9] Lettl showed that the property above is equivalent to $s \mid p-1$.

Now we will prove Theorem 3.2.

Proof. We will use the Lemma 3.1 to calculate the valuation of $\varphi_m \cdot (\alpha^u T^{tu+\gamma_r(u)})$ for $m \le u \le p-1$. Note that since $v(\alpha) < 0$ and the largest exponent of α in $\varphi_m \cdot (\alpha^u T^{tu+\gamma_r(u)})$ is $u-m$, which happens only once, we have

$$\begin{aligned} v(\varphi_m \cdot (\alpha^u T^{tu+\gamma_r(u)})) &= v\left(\frac{u(u-1)(u-2)\cdots(u-m+1)T^{tu+\gamma_r(u)}\alpha^{u-m}}{T^{mt+\gamma'_{r,b}(m)}}\right) \\ &= tu + \gamma_r(u) - (u-m)\left(\frac{\lambda}{p}\right) - mt - \gamma'_{r,b}(m) \\ &= \gamma_r(u) - \frac{us}{p} + \frac{ms}{p} - \gamma'_{r,b}(m) \\ &= -\left\lfloor -\left(\frac{us+r}{p}\right)\right\rfloor - \frac{us}{p} - \left(\gamma'_{r,b}(m) - \frac{ms}{p}\right) \\ &= N_{u,m,r} + \rho_{m,r,b}. \end{aligned}$$

Note that, for $0 \le u \le p-1$,

$$v(\varphi_m \cdot (\alpha^u T^{tu+\gamma_r(u)})) = N_{u,m,r} + \rho_{m,r,b} \ge \frac{b}{p}$$

by definition of $\rho_{m,r,b}$. Hence, $\varphi_m \in A_{r,b}(L/k)$.

Conversely, we will show that φ_m for $0 \le m \le p-1$, span $A_{r,b}(L/k)$ over O_k. From [1] and [3], it is sufficient to prove that if some linear combination

$$\varphi = \sum_{m=0}^{p-1} a_m \varphi_m \qquad\qquad (a_m \in O_k)$$

has the property that $\varphi \cdot M_L^r \subset TM_L^b$, then $a_m \in TO_k$ for all m. Note that if $\varphi(M_L^r) \subset TM_L^b$, then $v(\varphi(\theta)) \ge 1 + \frac{b}{p}$ for all $\theta \in M_L^r$. Suppose on the contrary that $a_i \notin TO_k$ for some i, that is, $v(a_i) = 0$.

For each m, there exists u such that $\frac{b}{p} \le v(\varphi_m \cdot (\alpha^u T^{tu+\gamma_r(u)})) < 1 + \frac{b}{p}$. Indeed, if

$$v(\varphi_m \cdot (\alpha^u T^{tu+\gamma_r(u)})) = N_{u,m,r} + \rho_{m,r,b} \ge 1 + \frac{b}{p},$$

for all $0 \le u \le p-1$, then $\rho_{m,r,b}$ is not the smallest possible, contradicting the definition of $\rho_{m,r,b}$.

Now, if $v(\varphi_m \cdot (\alpha^u T^{tu+\gamma_r(u)})) \equiv v(\varphi_{m'} \cdot (\alpha^u T^{tu+\gamma_r(u)}))$ mod 1, then $\frac{ms}{p} - \gamma'_{r,b}(m) \equiv \frac{m's}{p} - \gamma'(m')$ mod 1. But that implies $\frac{ms}{p} \equiv \frac{m's}{p}$ mod 1. So, $m = m'$, since $0 \le m, m' \le p-1$. Hence, for $0 \le m \le p-1$, all the elements $\varphi_m \cdot (\alpha^u T^{tu+\gamma_r(u)})$ have distinct valuations. Let u_i be an integer with $1 \le u_i \le$

$p-1$ such that $\frac{b}{p} \leq v(\varphi_i(\alpha^{u_i}T^{tu_i+\gamma_r(u_i)})) < 1+\frac{b}{p}$. It follows that

$$\begin{aligned} v(\varphi \cdot (\alpha^{u_i}T^{tu_i+\gamma_r(u_i)})) &= min\{v(a_m\varphi_m \cdot (\alpha^{u_i}T^{tu_i+\gamma_r(u_i)}))\}_{m=0}^{p-1} \\ &\leq v(a_i\varphi_i(\alpha^{u_i}T^{tu_i+\gamma_r(u_i)})) \\ &< 1+\frac{b}{p}, \end{aligned}$$

a contradiction. Hence, $a_m \in TO_k$. Therefore, we have

$$A_{r,b}(L/k) = \sum_{k=0}^{p-1} \varphi_m O_k.$$

Now we prove the second part of Theorem 3.2. Suppose that M_L^r is a free A_r-module. Assume on the contrary that there do exist integers $0 \leq m \leq n \leq p-1$ such that (8) is satisfied. Recall that $\zeta = \alpha^{p-1}T^{t(p-1)+\gamma_r(p-1)} \in M_L^r$. From Remark 1.2, we have $N_{u,m,r} + \rho_{m,r,r} = N_{u,m,r} + 1$ for all u such that $0 \leq m \leq u \leq p-1$. Then, from the first inequality of (8), we have

$$\text{(a) } v(\varphi_m \cdot \zeta) = N_{p-1,m,r} + \rho_{m,r,r} \geq \frac{r}{p} + 1.$$

From the second inequality of (8), we have

$$\text{(b) } v(\varphi_m \cdot (\alpha^n T^{tn+\gamma_r(n)})) = N_{n,m,r} + \rho_{m,r,r} < \frac{r}{p} + 1.$$

It follows from (a) that $(1/T)\varphi_m \cdot \zeta \in M_L^r$. By Corollary 2.8, $(1/T)\varphi_m \in A_r$. However, from (b), $(1/T)\varphi_m(\alpha^n T^{tn+\gamma_r(n)}) \notin M_L^r$, a contradiction.

Now assume that there do not exist integers $0 \leq m \leq n \leq p-1$ such that (8) is satisfied. It follows that for any $0 \leq m \leq p-1$ such that $N_{p-1,m,r} \geq \frac{r}{p}$, there does not exist an n with $0 \leq m \leq n \leq p-1$ such that $N_{n,m,r} < \frac{r}{p}$. In other words, if $N_{p-1,m,r} \geq \frac{r}{p}$, then $N_{u,m,r} \geq \frac{r}{p}$ for all u such that $0 \leq m \leq u \leq p-1$. So, if $N_{p-1,m,r} \geq \frac{r}{p}$, then $\rho_{m,r,r} = 0$. Hence, we have

$$v(\varphi_m \cdot \zeta) = N_{p-1,m,r} + \rho_{m,r,r} = N_{p-1,m,r} \text{ if } N_{p-1,m,r} \geq \frac{r}{p},$$

and

$$v(\varphi_m \cdot \zeta) = N_{p-1,m,r} + \rho_{m,r,r} = N_{p-1,m,r} + 1 \text{ if } N_{p-1,m,r} < \frac{r}{p}.$$

Furthermore, since

$$N_{p-1,m,r} = \left\{\frac{s-r}{p}\right\} - \left\{-\frac{ms}{p}\right\} + \frac{r}{p},$$

it follows that

$$v(\varphi_m \cdot \zeta) = \left\{\left\{\frac{s-r}{p}\right\} - \left\{-\frac{ms}{p}\right\}\right\} + \frac{r}{p} = \left\{\frac{s-r+ms}{p}\right\} + \frac{r}{p}.$$

Hence, the valuations of the p elements $\varphi_m \cdot \zeta$ for $0 \leq m \leq p-1$ are distinct and lie between $\frac{r}{p}$ and $\frac{p-1+r}{p}$. It follows that

$$(\sum O_k \varphi_m \cdot \zeta) + TM_L^r = M_L^r.$$

Therefore, by Nakayama's Lemma, we have $A_r \cdot \zeta = M_L^r$. □

4. Property A

We will look at the double inequalities (9) given in Remark 3.3 and generalize the works of Lettl in [9]. Let r, s be integers with $0 \leq r \leq p-1$ and $1 \leq s \leq p-1$. We say a pair (r, s) has property A if there do not exist integers $1 \leq m \leq n \leq p-1$ such that

$$\left\{\frac{s-r}{p}\right\} \geq \left\{\frac{ns}{p}\right\} > \left\{\frac{ms-r}{p}\right\}.$$

Hence, for a fixed s, M_L^r is A_r-free if and only if (r, s) has property A.

Since it's clear that any pair of the form (s, s) has property A, we will assume that $r \neq s$. Let $1 \leq n_i \leq p-1$ be the least positive integer such that $n_i s \equiv i \pmod{p}$. Set $I = (n_1, n_2, ..., n_k)$ and $M = max(I)$, where $k = s - r$ if $s > r$ and $k = p + s - r$ if $s < r$. Let R be the least positive integer such that $Rs \equiv r (\text{mod } p)$. In fact, we see that $R = p - n_k + 1$.

Lemma 4.1. Then $M < R$ if and only if $n_i + n_k \leq p$ for all $i \leq k$. Moreover, if these equivalent conditions hold then either

(i) $n_i = in_1$ for all $i \leq k$, or
(ii) $n_i = n_k + (k-i)(p-n_1) = in_1 - (i-1)p$ for all $i \leq k$.

In particular, if $M < R$ then the sequence I is monotone and in arithmetic progression.

Proof. $M < R$ if and only if $n_i < p - n_k + 1$ for all $i \leq k$ if and only if $n_i + n_k \leq p$ for all $i \leq k$.

Both (i) and (ii) clearly holds vacuously when $k = 1$. Suppose $k > 1$. To prove the second statement, note that

$$n_i + n_j \equiv n_{i+j} (\text{mod } p) \text{ for all } i, j \leq k. \tag{10}$$

(i) If $n_1 < n_k$, then we have $2n_1 < n_1 + n_k \leq p$. Since $2n_1 < p$ and $2n_1 \equiv n_2 (\text{mod } p)$ by (10), we have $n_2 = 2n_1$. Similarly, we have $n_3 = 3n_1$. It follows from induction that $n_i = in_1$ for $i \leq k$.

(ii) Now suppose $n_1 > n_k$. Note that $n_k + p - n_1 < n_k + p - n_k = p$. Since $n_k + p - n_1 < p$ and $n_k + p - n_1 \equiv n_{k-1} (\text{mod } p)$ by (10), we have $n_{k-1} = n_k + p - n_1$. Similarly, we have $n_{k-2} = n_k + 2(p - n_1)$. It follows from downward induction that $n_j = n_k + (k-j)(p-n_1)$ for $j \leq k$.

From the first equality of (ii), we obtain $n_1 = n_k + (k-1)(p-n_1)$. Substituting this back into the first equality of (ii), we obtain

$$\begin{aligned} n_i &= n_k + (k-i)(p-n_1) \\ &= n_k + (k-1)(p-n_1) - (i-1)(p-n_1) \\ &= in_1 - (i-1)p \end{aligned}$$

□

Lemma 4.2. The pair (r,s) has property A if and only if

$$\frac{i}{p} \leq \left\{ \frac{ms-r}{p} \right\} \text{ for all } i,m \text{ with } 1 \leq i \leq k, 1 \leq m \leq n_i. \tag{11}$$

Proof. Write $\left\{ \frac{s-r}{p} \right\} = \frac{k}{p}$. Then property A can be restated as: For each $i \leq k$, there do not exist integers $1 \leq m \leq n_i \leq p-1$ such that

$$\frac{k}{p} \geq \frac{i}{p} > \left\{ \frac{ms-r}{p} \right\}. \tag{12}$$

The lemma now follows. □

Lemma 4.3. The pair (r,s) has property A if and only if $M < R$.

Proof. From Lemma 4.2, if the pair (r,s) has property A, then for each $1 \leq i \leq k$, we have $\frac{i}{p} \leq \left\{ \frac{ms-r}{p} \right\}$, for all $m \leq n_i$. By choosing i such that $n_i = M$, then $\frac{i}{p} \leq \left\{ \frac{ms-r}{p} \right\}$, $\forall m \leq M$. If $M \geq R$, then by taking $m = R$, we have

$$\frac{i}{p} \leq \left\{ \frac{ms-r}{p} \right\} = \left\{ \frac{Rs-r}{p} \right\} = 0,$$

a contradiction. Hence, $M < R$.

Recall that $R = p - n_k + 1$. Hence

$$\left\{ \frac{ms-r}{p} \right\} = \left\{ \frac{ms-Rs}{p} \right\} = \left\{ \frac{s(m-R+p)}{p} \right\} = \left\{ \frac{s(n_k-1+m)}{p} \right\}. \tag{13}$$

Combining (11) from Lemma 4.2 with (13), property A can be restated as:

$$\frac{i}{p} \leq \left\{ \frac{s(n_k-1+m)}{p} \right\} \text{ for all } i,m \text{ with } 1 \leq i \leq k, 1 \leq m \leq n_i. \tag{14}$$

Suppose that $M < R$. Then $n_i + n_k \leq p$ for all $i \leq k$ by Lemma 4.1. Let $1 \leq i \leq k$ and $1 \leq m \leq n_i$. We have

$$n_k \leq n_k - 1 + m \leq n_k - 1 + n_i < p. \tag{15}$$

To show (14) is satisfied, we will show that for all z with $1 \leq z < i$, we have $n_z \notin \{m + n_k - 1 : 1 \leq m \leq n_i\}$. Note here that we assume $i > 1$ since (14) is clearly satisfied for $i = 1$.

If I is increasing, then $n_z < n_k$ for all $z < k$. It follows that $n_z \notin \{m+n_k-1 : 1 \leq m \leq n_i\}$ for all $z < i$ by (15). If I is decreasing, then $n_z > n_i$ for all $z < i$, so $p - n_{i-z} = n_z - n_i$ for all $i < z$. Furthermore, $M < R$ implies $n_k + n_{i-z} \leq p$ for all $z < i$. Hence, we get $n_z + n_k \leq n_z$ for all $z < i$, which implies $n_z \notin \{m + n_k - 1 : 1 \leq m \leq n_i\}$ for all $z < i$.

□

Theorem 4.4. Let r, s be integers with $0 \leq r \leq p-1$ and $1 \leq s \leq p-1$ such that the pair (r, s) has property A.

(i) If $r = s$, then (r, s) has property A.

(ii) If $r > s$, then (r, s) has property A if and only if $s = 1$ and $r \geq \dfrac{p+3}{2}$.

Proof.

(i) This case is clear.

(ii) Certainly, for any $r \geq \dfrac{p+3}{2}$, the pair $(r, 1)$ has property A. Conversely, suppose (r, s) has property A with $r > s$. By Lemma 4.2, we have

$$\left\{\frac{n_k s}{p}\right\} \leq \left\{\frac{ms - r}{p}\right\} \text{ for all } m \leq n_k. \tag{16}$$

Putting $m = n_k$ into (16), we see that

$$\frac{k}{p} \leq \left\{\frac{k-r}{p}\right\},$$

so $r > k$ and hence $r > \dfrac{p+s}{2}$.

Note that $k = p - r + s \geq s + 1$. We see that $n_{s+1} > 1$, and $n_{s+1} = 2$ if and only if $s = 1$. Suppose $s > 1$ so that $s + 1 \geq 3$. Then $s(n_{s+1} - 1) \equiv 1 (\text{mod } p)$, which implies $n_1 = n_{s+1} - 1$. Since I is strictly monotonic and $n_1 < n_{s+1}$, we have $n_1 < n_2 < n_3 \leq n_{s+1}$; however, this implies $n_{s+1} - n_1 > 1$. Hence, we must have $s = 1$. Therefore, $r \geq \dfrac{p+3}{2}$.

□

Theorem 4.5. Suppose $r < s$.

(a) The pair (r, s) has property A with decreasing I if and only if

$$r = \left\lceil s - \frac{p}{p - n_1} \right\rceil.$$

(b) The pair (r, s) has property A with increasing I if and only if

$$s - \frac{1}{2}\frac{p}{n_1} \leq r < s.$$

Proof.

(a) Suppose I is decreasing and (r, s) has Property A. By Lemma 4.3, (r, s) has property A if and only if $M < R$. Since $M = n_1$, and $R = p - n_k + 1 = p - kn_1 + (k-1)p + 1$ by (ii) of Lemma 4.1, we see that $M < R$ if and only if

$$r \leq s - \frac{p}{p - n_1} + 1, \tag{17}$$

recalling $k = s - r$. Furthermore, from (ii) of Lemma 4.1, we find that

$$n_1 = \frac{n_k}{k} + \frac{k-1}{k}p,$$

which implies $n_1 > \dfrac{k-1}{k}p$. Solving for r, we have

$$r > s - \frac{p}{p - n_1}. \tag{18}$$

Combining equations (17) and (18), we have

$$r = \left\lceil s - \frac{p}{p - n_1} \right\rceil = s - \left\lfloor \frac{p}{p - n_1} \right\rfloor. \tag{19}$$

Conversely, suppose r satisfies (19). We will first show that I is decreasing. Since equation (19) is satisfied, equation (18) is also satisfied, which implies $n_1 > \dfrac{k-1}{k}p$. Note then that $kn_1 - (k-1)p > 0$. Hence, we have $n_i = in_1 - (i-1)p$ for $i \leq k$, which implies I is decreasing. Furthermore, we also have that equation (17) is satisfied, which implies $M < R$, and by Lemma (4.3), (r, s) has Property A.

(b) Note that I is increasing if and only if

$$n_1 < \frac{p}{s - r}. \tag{20}$$

By Lemma 4.3, (r, s) has property A if and only if $M < R$. Since $M = n_k$, and $R = p - n_k + 1 = p - kn_1 + 1$ by (i) of Lemma 4.1, we see that $M < R$ if and only if

$$n_1 \leq \frac{1}{2}\frac{p}{s - r}. \tag{21}$$

Note that if r satisfies (21), then it will satisfy (20). Furthermore, if r_0 satisfies (21), then any r such that $r_0 < r < s$ will also satisfies (21). Hence, for a fixed s, the pair (r, s) has Property A with increasing I if and only if

$$s - \frac{1}{2}\frac{p}{n_1} \leq r < s. \tag{22}$$

□

5. Proof of Theorem 1.3

Part (i) has already been proven by Theorem 3.2.

For part (ii), we know that for a fixed s, M_L^r is A_r-free if and only if (r, s) has Property A. We already know that M_L^s is A_s-free. When $r > s$, we proved in Theorem 4.4 that M_L^r is A_r-free if and only if $s = 1$ and $r \geq \dfrac{p+3}{2}$. When $r < s$, Theorem 4.5 shows that M_L^r is A_r-free if and only if

$$r = s - \left\lfloor \frac{p}{p - n_1} \right\rfloor \text{ if } I \text{ is decreasing,} \tag{23}$$

or

$$s - \frac{1}{2}\frac{p}{n_1} \leq r < s \text{ if } I \text{ is increasing.} \tag{24}$$

When $n_1 > \dfrac{p}{2}$, equation (23) yields $r = s$ and an r such that $r \leq s - 2$, and equation (24) yields $r = s$. On the other hand, when $n_1 < \dfrac{p}{2}$, equation (24) yields a set of r's with

$$s - \frac{1}{2}\frac{p}{n_1} \leq r \leq s \tag{25}$$

with $s - \dfrac{1}{2}\dfrac{p}{n_1} < s - 1$, while equation (23) yields $r = s$ and $r = s - 1$.

The case $n_1 = \dfrac{p}{2}$ happens only when $p = 2$, in which case $s = 1$. Both equations (23) and (24) yield $r = 0$ and $r = 1$.

6. Acknowledgments

I am grateful to my adviser, Kevin Keating, and the referee for insightful remarks and careful review. Kevin has helped me with every confusion along the way, and it was his suggestion to graph all the pairs of integers (r, s) satisfying Property A. The graph was the spark for this paper. The organizational structure of this paper and a few proofs have been greatly improved due to the referee's suggestions. I would like to thanks the referee again for the simple proof to Theorem 1.7.

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

[2] A. Aiba, Carlitz Modules and Galois Module Structure, J. Number Theory 62 (1997) 213-219

[3] N. P. Byott, Some self-dual local rings of integers not free over their associated orders, Math. Proc. Cambridge Philos. Soc. 110 (1991) 5-10

[4] I.B. Fesenko and S.V. Vostokov, Local Fields and Their Extensions, Translation of Mathematical Monographs V. 121, (AMS, 2002)

[5] F. Bertrandias and M. Ferton, C. R. Acad. Scri. Paris ser. A-B 274 (1972), A1330-A1333

[6] M. Ferton, Sur les id*é*aux d'une extension cyclique de degr*é* premier d'un corps local, C.R. Acad. Sc. Paris, t. 276 (June 4, 1973) S*é*rie A 1483 - 1486

[7] A. Frohlich and M.J. Taylor, Algebraic Number Theory, Cambridge studies in advanced mathematics 27 (Cambridge University Press, 1991)

[8] S. Lang, Algebra, Graduate Texts in Mathematics no. 211 (Springer-Verlag, 2002)

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

[10] L. Thomas, On Galois Module Structure of Extensions of Local Fields, Publications Mathematiques de Besançon, 2010

[11] L. Washington, Cyclotomic Fields, Graduate Texts in Mathematics no. 83 (Springer-Verlag, 1982)