Journal de Théorie des Nombres de Bordeaux **17** (2005), 801–823

On coefficient valuations of Eisenstein polynomials

par Matthias KÜNZER et Eduard WIRSING

Résumé. Soit $p \geq 3$ un nombre premier et soient $n > m \geq 1$. Soit π_n la norme de $\zeta_{p^n} - 1$ sous C_{p-1}. Ainsi $\mathbf{Z}_{(p)}[\pi_n]|\mathbf{Z}_{(p)}$ est une extension purement ramifiée d'anneaux de valuation discrète de degré p^{n-1}. Le polynôme minimal de π_n sur $\mathbf{Q}(\pi_m)$ est un polynôme de Eisenstein; nous donnons des bornes inférieures pour les π_m-valuations de ses coefficients. L'analogue dans le cas d'un corps de fonctions, comme introduit par Carlitz et Hayes, est etudié de même.

Abstract. Let $p \geq 3$ be a prime, let $n > m \geq 1$. Let π_n be the norm of $\zeta_{p^n} - 1$ under C_{p-1}, so that $\mathbf{Z}_{(p)}[\pi_n]|\mathbf{Z}_{(p)}$ is a purely ramified extension of discrete valuation rings of degree p^{n-1}. The minimal polynomial of π_n over $\mathbf{Q}(\pi_m)$ is an Eisenstein polynomial; we give lower bounds for its coefficient valuations at π_m. The function field analogue, as introduced by Carlitz and Hayes, is studied as well.

Contents

Manuscrit reçu le 1er février 2004.

0. Introduction

0.1. Problem and methods. Consider a primitive p^nth root of unity ζ_{p^n} over $\mathbf{Q}$, where p is a prime and $n \geq 2$. One has $\mathrm{Gal}(\mathbf{Q}(\zeta_{p^n})|\mathbf{Q}) \simeq C_{p^{n-1}} \times C_{p-1}$. To isolate the p-part of this extension, let π_n be the norm of $\zeta_{p^n} - 1$ under C_{p-1}; that is, the product of the Galois conjugates $(\zeta_{p^n} - 1)^\sigma$, where σ runs over the subgroup C_{p-1}. Then

$$\begin{tikzcd}
 & \mathbf{Q}(\zeta_{p^n}) \arrow[dd, dash, "p^{n-1}"] \\
\mathbf{Q}(\pi_n) \arrow[ur, dash, "p-1"] \arrow[dd, dash, "p^{n-1}"'] & \\
 & \mathbf{Q}(\zeta_p) \\
\mathbf{Q} \arrow[ur, dash, "p-1"] &
\end{tikzcd}$$

We ask for the minimal polynomial $\mu_{\pi_n,\mathbf{Q}}(X) = \sum_{j\in[0,p^{n-1}]} a_j X^j \in \mathbf{Z}[X]$ of π_n over $\mathbf{Q}$. By construction, it is an Eisenstein polynomial; that is, $v_p(a_j) \geq 1$ for $j \in [0, p^{n-1} - 1]$, and $v_p(a_0) = 1$, where v_p denotes the valuation at p.

More is true, though. Our basic objective is to give lower bounds bigger than 1 for these p-values $v_p(a_j)$, except, of course, for $v_p(a_0)$. As a byproduct of our method of proof, we shall also obtain congruences between certain coefficients for varying n.

A consideration of the trace $\mathrm{Tr}_{\mathbf{Q}(\pi_n)|\mathbf{Q}}(\pi_n)$ yields additional information on the second coefficient of $\mu_{\pi_n,\mathbf{Q}}(X)$. By the congruences just mentioned, this also gives additional information for certain coefficients of the minimal polynomials $\mu_{\pi_l,\mathbf{Q}}(X)$ with $l > n$; these coefficients no longer appear as traces.

Finally, a comparison with the different ideal

$$\mathfrak{D}_{\mathbf{Z}_{(p)}[\pi_n]|\mathbf{Z}_{(p)}} = \mathbf{Z}_{(p)}[\pi_n]\, \mu'_{\pi_n,\mathbf{Q}}(\pi_n)$$

then yields some exact coefficient valuations, not just lower bounds.

Actually, we consider the analogous question for the coefficients of the slightly more general relative minimal polynomial $\mu_{\pi_n,\mathbf{Q}(\pi_m)}(X)$, where $n > m \geq 1$, which can be treated using essentially the same arguments. Note that $\pi_1 = p$.

Except for the trace considerations, the whole investigation carries over mutatis mutandis to the case of cyclotomic function field extensions, as introduced by Carlitz [1] and Hayes [5].

As an application, we mention the Wedderburn embedding of the twisted group ring (with trivial 2-cocycle)

$$\mathbf{Z}_{(p)}[\pi_n] \wr C_{p^{n-1}} \quad \xhookrightarrow{\omega} \quad \mathrm{End}_{\mathbf{Z}_{(p)}}\mathbf{Z}_{(p)}[\pi_n] \ \simeq \ \mathbf{Z}_{(p)}^{p^{n-1}\times p^{n-1}} ,$$

to which we may reduce the problem of calculating $\mathbf{Z}_{(p)}[\zeta_{p^n}]\wr(C_{p^{n-1}}\times C_{p-1})$ by means of Nebe decomposition. The image $\omega(\pi_n)$ is the companion matrix of $\mu_{\pi_n,\mathbf{Q}}(X)$. To describe the image $\omega(\mathbf{Z}_{(p)}[\pi_n] \wr C_{p^{n-1}})$ of the whole ring, we may replace this matrix modulo a certain ideal. To do so, we need to know the valuations of its entries, i.e. of the coefficients of $\mu_{\pi_n,\mathbf{Q}}(X)$, or at least a lower bound for them. So far, this could be carried through only for $n = 2$ [10].

In this article, however, we restrict our attention to the minimal polynomial itself.

0.2. Results.

0.2.1. *The number field case.* Let $p \geq 3$ be a prime, and let ζ_{p^n} denote a primitive p^nth root of unity over $\mathbf{Q}$ in such a way that $\zeta_{p^{n+1}}^p = \zeta_{p^n}$ for all $n \geq 1$. Put

$$\begin{aligned} F_n &= \mathbf{Q}(\zeta_{p^n}) \\ E_n &= \mathrm{Fix}_{C_{p-1}} F_n \ , \end{aligned}$$

so $[E_n : \mathbf{Q}] = p^n$. Letting

$$\pi_n \ = \ \mathrm{N}_{F_n|E_n}(\zeta_{p_n} - 1) \ = \ \prod_{j\in[1,p-1]} (\zeta_{p^n}^{jp^{n-1}} - 1) \ ,$$

we have $E_n = \mathbf{Q}(\pi_n)$. In particular, $E_{m+i} = E_m(\pi_{m+i})$ for $m, i \geq 1$. We fix m and write

$$\begin{aligned} \mu_{\pi_{m+i},\,E_m}(X) \ &= \ \sum_{j\in[0,p^i]} a_{i,j}X^j \\ &= \ X^{p^i} + \Big(\sum_{j\in[1,p^i-1]} a_{i,j}X^j\Big) - \pi_m \ \in \ \mathbf{Z}_{(p)}[\pi_m][X] \ . \end{aligned}$$

Theorem (5.3, 5.5, 5.8).

(i) *We have* $p^i \mid ja_{i,j}$ *for* $j \in [0, p^i]$.
(i′) *If* $j < p^i(p-2)/(p-1)$, *then* $p^i\pi_m \mid ja_{i,j}$.
(ii) *We have* $a_{i,j} \equiv_{p^{i+1}} a_{i+\beta,p^\beta j}$ *for* $j \in [0, p^i]$ *and* $\beta \geq 1$.
(ii′) *If* $j < p^i(p-2)/(p-1)$, *then* $a_{i,j} \equiv_{p^{i+1}\pi_m} a_{i+\beta,p^\beta j}$ *for* $\beta \geq 1$.
(iii) *The element* $p^{i-\beta}$ *exactly divides* $a_{i,p^i-(p^i-p^\beta)/(p-1)}$ *for* $\beta \in [0, i-1]$.
(iv) *We have* $\mu_{\pi_n,\mathbf{Q}}(X) \equiv_{p^2} X^{p^{n-1}} + pX^{(p-1)p^{n-2}} - p$ *for* $n \geq 2$.

Assertion (iv) requires the computation of a trace, which can be reformulated in terms of sums of $(p-1)$th roots of unity in $\mathbf{Q}_p$ (5.6). Essentially, one has to count the number of subsets of $\boldsymbol{\mu}_{p-1} \subseteq \mathbf{Q}_p$ of a given cardinality whose sum is of a given valuation at p. We have not been able to go much beyond this reformulation, and this seems to be a problem in its own right — see e.g. (5.9).

To prove (i, i′, ii, ii′), we proceed by induction. Assertions (i, i′) also result from the different

$$\mathfrak{D}_{\mathbf{Z}_{(p)}[\pi_{m+i}]|\mathbf{Z}_{(p)}[\pi_m]} = \left(\mu'_{\pi_{m+i},E_m}(\pi_{m+i})\right) = \left(p^i\pi_{m+i}^{p^i-1-(p^i-1)/(p-1)}\right).$$

Moreover, (ii) yields (iii) by an argument using the different (in the function field case below, we will no longer be able to use the different for the assertion analogous to (i, i′), and we will have to resort to induction).

Suppose $m = 1$. Let us call an index $j \in [1, p^i - 1]$ *exact,* if either $j < p^i(p-2)/(p-1)$ and $p^i\pi_m$ exactly divides $ja_{i,j}$, or $j \geq p^i(p-2)/(p-1)$ and p^i exactly divides $ja_{i,j}$. If $i = 1$ and e.g. $p \in \{3, 19, 29, 41\}$, then all indices $j \in [1, p-1]$ are exact. If $i \geq 2$, we propose to ask whether the number of non-exact indices j asymptotically equals p^{i-1} as $p \to \infty$.

0.2.2. *The function field case.* Let $p \geq 3$ be a prime, $\rho \geq 1$ and $r = p^\rho$. We write $\mathcal{Z} = \mathbf{F}_r[Y]$ and $\mathcal{Q} = \mathbf{F}_r(Y)$. We want to study a function field analogue over $\mathcal{Q}$ of the number field extension $\mathbf{Q}(\zeta_{p^n})|\mathbf{Q}$. Since 1 is the only p^nth root of unity in an algebraic closure $\bar{\mathcal{Q}}$, we have to proceed differently, following CARLITZ [1] and HAYES [5]. First of all, the power operation of p^n on $\bar{\mathbf{Q}}$ becomes replaced by a module operation of f^n on $\bar{\mathcal{Q}}$, where $f \in \mathcal{Z}$ is an irreducible polynomial. The group of p^nth roots of unity

$$\boldsymbol{\mu}_{p^n} = \{\xi \in \bar{\mathbf{Q}} : \xi^{p^n} = 1\}$$

becomes replaced by the annihilator submodule

$$\boldsymbol{\lambda}_{f^n} = \{\xi \in \bar{\mathcal{Q}} : \xi^{f^n} = 0\}.$$

Instead of choosing a primitive p^nth root of unity ζ_{p^n}, i.e. a $\mathbf{Z}$-linear generator of that abelian group, we choose a $\mathcal{Z}$-linear generator θ_n of this $\mathcal{Z}$-submodule. A bit more precisely speaking, the element $\theta_n \in \bar{\mathcal{Q}}$ plays the role of $\vartheta_n := \zeta_{p^n} - 1 \in \bar{\mathbf{Q}}$. Now $\mathcal{Q}(\theta_n)|\mathcal{Q}$ is the function field analogue of $\mathbf{Q}(\vartheta_n)|\mathbf{Q}$. See also [3, sec. 2].

To state the result, let $f(Y) \in \mathcal{Z}$ be a monic irreducible polynomial and write $q = r^{\deg f}$. Let $\xi^Y := Y\xi + \xi^r$ define the $\mathcal{Z}$-linear Carlitz module structure on an algebraic closure $\bar{\mathcal{Q}}$, and choose a $\mathcal{Z}$-linear generator θ_n of $\mathrm{ann}_{f^n} \bar{\mathcal{Q}}$ in such a way that $\theta_{n+1}^f = \theta_n$ for all $n \geq 1$. We write $\mathcal{F}_n = \mathcal{Q}(\theta_n)$, so that $\mathrm{Gal}(\mathcal{F}_n|\mathcal{Q}) \simeq (\mathcal{Z}/f^n)^*$. Letting $\mathcal{E}_n = \mathrm{Fix}_{C_{q-1}} \mathcal{F}_n$, we get $[\mathcal{E}_n : \mathcal{Q}] = q^n$. Denoting $\varpi_n = \mathrm{N}_{\mathcal{F}_n|\mathcal{E}_n}(\theta_n) = \prod_{e \in (\mathcal{Z}/f)^*} \theta_n^{e^{q^{n-1}}}$, we obtain $\mathcal{E}_n = \mathcal{Q}(\varpi_n)$. In particular, $\mathcal{E}_{m+i} = \mathcal{E}_m(\varpi_{m+i})$ for $m, i \geq 1$. We fix m and write

$$\begin{aligned} \mu_{\varpi_{m+i},\mathcal{E}_m}(X) &= \sum_{j \in [0,q^i]} a_{i,j} X^j \\ &= X^{q^i} + \Big(\sum_{j \in [1,q^i-1]} a_{i,j} X^j \Big) - \varpi_m \in \mathcal{Z}_{(f)}[\varpi_m][X] . \end{aligned}$$

Let $v_q(j) := \max\{\alpha \in \mathbf{Z}_{\geq 0} \;:\; q^\alpha \mid j \}$.

Theorem (6.6, 6.7, 6.9).

(i) *We have* $f^{i - v_q(j)} \mid a_{i,j}$ *for* $j \in [0, q^i]$.

(i′) *If* $j < q^i(q-2)/(q-1)$, *then* $f^{i - v_q(j)} \varpi_m \mid a_{i,j}$.

(ii) *We have* $a_{i,j} \equiv_{f^{i+1}} a_{i+\beta, q^\beta j}$ *for* $j \in [0, q^i]$ *and* $\beta \geq 1$.

(ii′) *If* $j < q^i(q-2)/(q-1)$, *then* $a_{i,j} \equiv_{f^{i+1}\varpi_m} a_{i+\beta, q^\beta j}$ *for* $\beta \geq 1$.

(iii) *The element* $f^{i-\beta}$ *exactly divides* $a_{i, q^i - (q^i - q^\beta)/(q-1)}$ *for* $\beta \in [0, i-1]$.

(iv) *If* $f = Y$, *then* $\mu_{\varpi_{m+i},\mathcal{E}_m}(X) \equiv_{Y^2} X^{q^i} + Y X^{(q-1)q^{i-1}} - \varpi_m$.

A comparison of the assertions (iv) in the number field case and in the function field case indicates possible generalizations — we do not know what happens for $\mu_{\pi_{m+i},E_m}(X)$ for $m \geq 2$ in the number field case; moreover, we do not know what happens for $f \neq Y$ in the function field case.

0.3. Notations and conventions.

(o) Within a chapter, the lemmata, propositions etc. are numbered consecutively.

(i) For $a, b \in \mathbf{Z}$, we denote by $[a,b] := \{c \in \mathbf{Z} \;:\; a \leq c \leq b\}$ the interval in $\mathbf{Z}$.

(ii) For $m \in \mathbf{Z} \smallsetminus \{0\}$ and a prime p, we denote by $m[p] := p^{v_p(m)}$ the p-part of m, where v_p denotes the valuation of an integer at p.

(iii) If R is a discrete valuation ring with maximal ideal generated by r, we write $v_r(x)$ for the valuation of $x \in R \smallsetminus \{0\}$ at r, i.e. $x/r^{v_r(x)}$ is a unit in R. In addition, $v_r(0) := +\infty$.

(iv) Given an element x algebraic over a field K, we denote by $\mu_{x,K}(X) \in K[X]$ the minimal polynomial of x over K.

(v) Given a commutative ring A and an element $a \in A$, we sometimes denote the quotient by $A/a := A/aA$ — mainly if A plays the role of a base ring. For $b, c \in A$, we write $b \equiv_a c$ if $b - c \in aA$.

(vi) For an assertion X, which might be true or not, we let $\{X\}$ equal 1 if X is true, and equal 0 if X is false.

$\boxed{\text{Throughout, let } p \geq 3 \text{ be a prime.}}$

1. A polynomial lemma

We consider the polynomial ring $\mathbf{Z}[X,Y]$.

Lemma 1.1. *We have* $(X+pY)^k \equiv_{k[p]\cdot p^2Y^2} X^k + kX^{k-1}pY$ *for* $k \geq 1$.

Proof. Since $\binom{k}{j} = k/j \cdot \binom{k-1}{j-1}$, we obtain for $j \geq 2$ that

$$\begin{aligned} v_p(p^j\tbinom{k}{j}) &\geq j + v_p(k) - v_p(j) \\ &\geq v_p(k) + 2 \ , \end{aligned}$$

where the second inequality follows from $j \geq 2$ if $v_p(j) = 0$, and from $j \geq p^{v_p(j)} \geq 3^{v_p(j)} \geq v_p(j) + 2$ if $v_p(j) \geq 1$. □

Corollary 1.2. *We have* $(X+pY)^k \equiv_{k[p]\cdot pY} X^k$ *for* $k \geq 1$.

Corollary 1.3. *For* $l \geq 1$ *and* $x, y \in \mathbf{Z}$ *such that* $x \equiv_{p^l} y$*, we have* $x^k \equiv_{k[p]\cdot p^l} y^k$ *for* $k \geq 1$.

Corollary 1.4. *We have* $(X+Y)^{p^{\beta+\alpha}} \equiv_{p^{\alpha+1}} (X^{p^\beta} + Y^{p^\beta})^{p^\alpha}$ *for all* $\alpha, \beta \geq 0$.

Proof. The assertion follows by (1.2) since $f(X,Y) \equiv_p g(X,Y)$ implies that $f(X,Y)^{p^\alpha} \equiv_{p^{\alpha+1}} g(X,Y)^{p^\alpha}$, where $f(X,Y),\, g(X,Y) \in \mathbf{Z}[X,Y]$. □

2. Consecutive purely ramified extensions

2.1. Setup. Let $T|S$ and $S|R$ be finite and purely ramified extensions of discrete valuation rings, of residue characteristic $\operatorname{char} R/rR = p$. The maximal ideals of R, S and T are generated by $r \in R$, $s \in S$ and $t \in T$, and the fields of fractions are denoted by $K = \operatorname{frac} R$, $L = \operatorname{frac} S$ and $M = \operatorname{frac} T$, respectively. Denote $m = [M:L]$ and $l = [L:K]$. We may and will assume $s = (-1)^{m+1}\mathrm{N}_{M|L}(t)$ and $r = (-1)^{l+1}\mathrm{N}_{L|K}(s)$.

We have $S = R[s]$ with

$$\mu_{s,K}(X) \;=\; X^l + \Big(\sum_{j\in[1,l-1]} a_j X^j\Big) - r \;\in\; R[X] \ ,$$

and $T = R[t]$ with

$$\mu_{t,K}(X) \;=\; X^{lm} + \Big(\sum_{j\in[1,lm-1]} b_j X^j\Big) - r \;\in\; R[X] \ .$$

Cf. [9, I.§7, prop. 18]. The situation can be summarized in the diagram

$$\begin{tikzcd}
 & M \arrow[dl, dash] \arrow[dd, dash, "m"] \\
tT \subseteq T = S[t] = R[t] \arrow[dd, dash] & \\
 & L \arrow[dl, dash] \arrow[dd, dash, "l"] \\
sS \subseteq S = R[s] \arrow[dd, dash] & \\
 & K \arrow[dl, dash] \\
rR \subseteq R &
\end{tikzcd}$$

Note that $r \mid p$, and that for $z \in M$, we have $v_t(z) = m \cdot v_s(z) = ml \cdot v_r(z)$.

2.2. Characteristic 0. In this section, we assume $\operatorname{char} K = 0$. In particular, $\mathbf{Z}_{(p)} \subseteq R$.

Assumption 2.1. Suppose given $x, y \in T$ and $k \in [1, l-1]$ such that

(i) $p \mid y$ and $t^m \equiv_y s$,
(ii) $x \mid ja_j$ for all $j \in [1, l-1]$, and
(iii) $xr \mid ja_j$ for all $j \in [1, k-1]$.

Put $c := \gcd(xys^{k-1}, yls^{l-1}) \in T$.

Lemma 2.2. *Given* (2.1), *we have* $c \mid \mu_{s,K}(t^m)$.

Proof. We may decompose

$$\begin{aligned}
\mu_{s,K}(t^m) &= \mu_{s,K}(t^m) - \mu_{s,K}(s) \\
&= (t^{ml} - s^l) + \Big(\sum_{j \in [1,k-1]} a_j (t^{mj} - s^j) \Big) \\
&\quad + \Big(\sum_{j \in [k,l-1]} a_j (t^{mj} - s^j) \Big) .
\end{aligned}$$

Now since $t^m = s + zy$ for some $z \in T$ by (2.1.i), we have

$$t^{mj} \overset{(1.1)}{\equiv}_{jy^2} s^j + js^{j-1}zy \equiv_{js^{j-1}y} s^j$$

for any $j \geq 1$, so that $s^{j-1} \mid r \mid p \mid y$ gives $t^{mj} \equiv_{js^{j-1}y} s^j$.

In particular, $yls^{l-1} \mid t^{ml} - s^l$. Moreover, $xys^l \mid \sum_{j \in [1,k-1]} a_j (t^{mj} - s^j)$ by (2.1.iii). Finally, $xys^{k-1} \mid \sum_{j \in [k,l-1]} a_j (t^{mj} - s^j)$ by (2.1.ii). $\square$

The following proposition will serve as inductive step in (3.2).

Proposition 2.3. *Given* (2.1), *we have* $t^{-j}c \mid b_j$ *if* $j \not\equiv_m 0$ *and* $t^{-j}c \mid (b_j - a_{j/m})$ *if* $j \equiv_m 0$, *where* $j \in [1, lm-1]$.

Proof. From (2.2) we take

$$\sum_{j\in[1,lm-1]} \big(b_j - \{j \equiv_m 0\}\, a_{j/m}\big)\, t^j \;=\; -\mu_{s,K}(t^m) \;\equiv_c\; 0\,.$$

Since the summands have pairwise different valuations at t, we obtain

$$\big(b_j - \{j \equiv_m 0\}\, a_{j/m}\big)\, t^j \;\equiv_c\; 0$$

for all $j \in [1, lm-1]$. □

2.3. As an illustration: cyclotomic polynomials. For $n \geq 1$, we choose primitive roots of unity ζ_{p^n} over $\mathbf{Q}$ in such a manner that $\zeta_{p^{n+1}}^p = \zeta_{p^n}$. We abbreviate $\vartheta_n = \zeta_{p^n} - 1$.

We shall show by induction on n that writing

$$\mu_{\vartheta_n,\mathbf{Q}}(X) \;=\; \Phi_{p^n}(X+1) \;=\; \sum_{j\in[0,p^{n-1}(p-1)]} d_{n,j} X^j$$

with $d_{n,j} \in \mathbf{Z}$, we have $p^{n-1} \mid j d_{n,j}$ for $j \in [0, p^{n-1}(p-1)]$, and even $p^n \mid j d_{n,j}$ for $j \in [0, p^{n-1}(p-2)]$.

This being true for $n = 1$ since $\Phi_p(X+1) = ((X+1)^p - 1)/X$, we assume it to be true for $n-1$ and shall show it for n, where $n \geq 2$. We apply the result of the previous section to $R = \mathbf{Z}_{(p)}$, $r = -p$, $S = \mathbf{Z}_{(p)}[\vartheta_{n-1}]$, $s = \vartheta_{n-1}$ and $T = \mathbf{Z}_{(p)}[\vartheta_n]$, $t = \vartheta_n$. In particular, we have $l = p^{n-2}(p-1)$ and $\mu_{s,K}(X) = \Phi_{p^{n-1}}(X+1)$; we have $m = p$ and $\mu_{t,L}(X) = (X+1)^p - 1 - \vartheta_{n-1}$; finally, we have $\mu_{t,K}(X) = \Phi_{p^n}(X+1)$.

We may choose $y = p\vartheta_n$, $x = p^{n-2}$ and $k = p^{n-2}(p-2)+1$ in (2.1). Hence $c = p^{n-1}\vartheta_n^{p^n - 2p^{n-1}+1}$. By (2.3), we obtain that $p^{n-1}\vartheta_n^{p^n-2p^{n-1}+1-j}$ divides $d_{n,j} - d_{n-1,j/p}$ if $j \equiv_p 0$ and that it divides $d_{n,j}$ if $j \not\equiv_p 0$. Since the coefficients in question are in R, we may draw the following conclusion.

$$\text{(I)}\quad \left\{ \begin{array}{ll} \text{If } j \equiv_p 0, & \text{then } p^n \mid d_{n,j} - d_{n-1,j/p} \text{ if } j \leq p^{n-1}(p-2), \\ & \text{and } p^{n-1} \mid d_{n,j} - d_{n-1,j/p} \text{ if } j > p^{n-1}(p-2); \\ \text{if } j \not\equiv_p 0, & \text{then } p^n \mid d_{n,j} \text{ if } j \leq p^{n-1}(p-2), \\ & \text{and } p^{n-1} \mid d_{n,j} \text{ if } j > p^{n-1}(p-2). \end{array} \right.$$

By induction, this establishes the claim.

Using (1.4), assertion (I) also follows from the more precise relation

(II)

$$\Phi_{p^n}(X+1) - \Phi_{p^{n-1}}(X^p+1) \;\equiv_{p^n}\; X^{p^{n-1}(p-2)} \Big((X^p+1)^{p^{n-2}} - (X+1)^{p^{n-1}} \Big)$$

for $n \geq 2$, which we shall show now. In fact, by (1.4) we have $(X+1)^{p^n} \equiv_{p^n} (X^p+1)^{p^{n-1}}$ as well as $(X^p+1)^{p^{n-2}} - (X+1)^{p^{n-1}} \equiv_{p^{n-1}} 0$, and so

$$\begin{aligned}
&\big((X+1)^{p^n} - 1\big)\Big((X^p+1)^{p^{n-2}} - 1\Big) \\
&\qquad - \Big((X^p+1)^{p^{n-1}} - 1\Big)\Big((X+1)^{p^{n-1}} - 1\Big) \\
&\equiv_{p^n} \Big((X^p+1)^{p^{n-1}} - 1\Big)\Big((X^p+1)^{p^{n-2}} - 1\Big) \\
&\qquad - \Big((X^p+1)^{p^{n-1}} - 1\Big)\Big((X+1)^{p^{n-1}} - 1\Big) \\
&= \Big((X^p+1)^{p^{n-1}} - 1\Big)\Big((X^p+1)^{p^{n-2}} - (X+1)^{p^{n-1}}\Big) \\
&\equiv_{p^n} X^{p^n}\Big((X^p+1)^{p^{n-2}} - (X+1)^{p^{n-1}}\Big) \\
&= X^{p^{n-1}(p-2)}\Big((X^p+1)^{p^{n-2}} - (X+1)^{p^{n-1}}\Big) \cdot X^{p^{n-1}} \cdot X^{p^{n-1}} \\
&\equiv_{p^n} X^{p^{n-1}(p-2)}\Big((X^p+1)^{p^{n-2}} - (X+1)^{p^{n-1}}\Big) \\
&\qquad \cdot \Big((X+1)^{p^{n-1}} - 1\Big)\Big((X^p+1)^{p^{n-2}} - 1\Big) ,
\end{aligned}$$

and the result follows by division by the monic polynomial

$$\Big((X+1)^{p^{n-1}} - 1\Big)\Big((X^p+1)^{p^{n-2}} - 1\Big) .$$

Finally, we remark that writing

$$F_n(X) \ := \ \Phi_{p^n}(X+1) + X^{p^n - 2p^{n-1}}(X+1)^{p^{n-1}},$$

we can equivalently reformulate (II) to

$$\text{(II}'\text{)} \qquad F_n(X) \ \equiv_{p^n} \ F_{n-1}(X^p) .$$

2.4. Characteristic p. In this section, we assume $\operatorname{char} K = p$.

Assumption 2.4. Suppose given $x, y \in T$ and $k \in [1, l-1]$ such that

(i) $t^m \equiv_{ys} s$,
(ii) $x \mid a_j y^{j[p]}$ for all $j \in [1, l-1]$, and
(iii) $xr \mid a_j y^{j[p]}$ for all $j \in [1, k-1]$.

Let $c := \gcd(xs^k, y^{l[p]} s^l) \in T$.

Lemma 2.5. *Given* (2.4), *we have* $c \mid \mu_{s,K}(t^m)$.

Proof. We may decompose

$$\begin{aligned}\mu_{s,K}(t^m) &= \mu_{s,K}(t^m) - \mu_{s,K}(s) \\ &= (t^{ml} - s^l) + \Big(\sum_{j \in [1,k-1]} a_j (t^{mj} - s^j) \Big) \\ &\quad + \Big(\sum_{j \in [k,l-1]} a_j (t^{mj} - s^j) \Big) \,.\end{aligned}$$

Now since $t^m \equiv_{ys} s$, we have $t^{mj} \equiv_{y^{j[p]} s^j} s^j$ for any $j \geq 1$.

In particular, $y^{l[p]} s^l \mid t^{ml} - s^l$. Moreover, $xs^l \mid \sum_{j \in [1,k-1]} a_j (t^{mj} - s^j)$ by (2.4.iii). Finally, $xs^k \mid \sum_{j \in [k,l-1]} a_j (t^{mj} - s^j)$ by (2.4.ii). $\square$

Proposition 2.6. *Given* (2.4)*, we have* $t^{-j} c \mid b_j$ *if* $j \not\equiv_m 0$ *and* $t^{-j} c \mid (b_j - a_{j/m})$ *if* $j \equiv_m 0$ *for* $j \in [1, lm-1]$*.*

This follows using (2.5), cf. (2.3).

3. Towers of purely ramified extensions

Suppose given a chain

$$R_0 \subseteq R_1 \subseteq R_2 \subseteq \cdots$$

of finite purely ramified extensions $R_{i+1}|R_i$ of discrete valuations rings, with maximal ideal generated by $r_i \in R_i$, of residue characteristic $\operatorname{char} R_i/r_i R_i = p$, with field of fractions $K_i = \operatorname{frac} R_i$, and of degree $[K_{i+1} : K_i] = p^\kappa = q$ for $i \geq 0$, where $\kappa \geq 1$ is an integer stipulated to be independent of i. We may and will suppose that $\mathrm{N}_{K_{i+1}|K_i}(r_{i+1}) = r_i$ for $i \geq 0$. We write

$$\mu_{r_i,K_0}(X) = X^{q^i} + \Big(\sum_{j \in [1,q^i-1]} a_{i,j} X^j \Big) - r_0 \in R_0[X] \,.$$

For $j \geq 1$, we denote $v_q(j) := \max\{\alpha \in \mathbf{Z}_{\geq 0} : j \equiv_{q^\alpha} 0\}$. That is, $v_q(j)$ is the largest integer below $v_p(j)/\kappa$. We abbreviate $g := (q-2)/(q-1)$.

Assumption 3.1. Suppose given $f \in R_0$ such that $r_i^{q-1} f \mid r_i^q - r_{i-1}$ for all $i \geq 0$. If $\operatorname{char} K_0 = 0$, then suppose $p \mid f \mid q$. If $\operatorname{char} K_0 = p$, then suppose $r_0 \mid f$.

Proposition 3.2. *Assume* (3.1).

(i) *We have* $f^{i - v_q(j)} \mid a_{i,j}$ *for* $i \geq 1$ *and* $j \in [1, q^i - 1]$*.*

(i′) *If* $j < q^i g$*, then* $f^{i - v_q(j)} r_0 \mid a_{i,j}$*.*

(ii) *We have* $a_{i,j} \equiv_{f^{i+1}} a_{i+\beta, q^\beta j}$ *for* $i \geq 1$*,* $j \in [1, q^i - 1]$ *and* $\beta \geq 1$*.*

(ii′) *If* $j < q^i g$*, then* $a_{i,j} \equiv_{f^{i+1} r_0} a_{i+\beta, q^\beta j}$ *for* $\beta \geq 1$*.*

Proof. Consider the case $\operatorname{char} K_0 = 0$. To prove (i, i′), we perform an induction on i, the assertion being true for $i = 1$ by (3.1). So suppose given $i \geq 2$ and the assertion to be true for $i - 1$. To apply (2.3), we let $R = R_0$, $r = r_0$, $S = R_{i-1}$, $s = r_{i-1}$, $T = R_i$ and $t = r_i$. Furthermore, we let $y = r_i^{q-1} f$, $x = f^{i-1}$ and $k = q^{i-1} - (q^{i-1} - 1)/(q - 1)$, so that (2.1) is satisfied by (3.1) and by the inductive assumption. We have $c = f^i r_i^{qk-1}$.

Consider $j \in [1, q^i - 1]$. If $j \not\equiv_q 0$, then (2.3) gives

$$v_{r_i}(a_{i,j}/f^i) \;\geq\; qk - 1 - j \;,$$

whence f^i divides $a_{i,j}$; f^i strictly divides $a_{i,j}$ if $j < q^i g$, since $0 < (qk - 1) - q^i g = 1/(q - 1) < 1$.

If $j \equiv_q 0$, then (2.3) gives

$$v_{r_i}((a_{i,j} - a_{i-1,j/q})/f^i) \;\geq\; qk - 1 - j \;,$$

whence f^i divides $a_{i,j} - a_{i-1,j/q}$; strictly, if $j < q^i g$. By induction, $f^{i-1-v_q(j/q)}$ divides $a_{i-1,j/q}$; strictly, if $j/q < q^{i-1} g$. But $a_{i-1,j/q} \equiv_{f^i} a_{i,j}$, and therefore $f^{i-v_q(j)}$ divides also $a_{i,j}$; strictly, if $j < q^i g$. This proves (i, i′).

The case $\beta = 1$ of (ii, ii′) has been established in the course of the proof of (i, i′). The general case follows by induction.

Consider the case $\operatorname{char} K_0 = p$. To prove (i, i′), we perform an induction on i, the assertion being true for $i = 1$ by (3.1). So suppose given $i \geq 2$ and the assertion to be true for $i - 1$. To apply (2.6), we let $R = R_0$, $r = r_0$, $S = R_{i-1}$, $s = r_{i-1}$, $T = R_i$ and $t = r_i$. Furthermore, we let $y = r_i^{-1} f$, $x = r_i^{-1} f^i$ and $k = q^{i-1} - (q^{i-1} - 1)/(q - 1)$, so that (2.4) is satisfied by (3.1) and by the inductive assumption. In fact, $xy^{-j[p]} = r_i^{j[p]-1} f^{i-j[p]}$ divides $f^{i-1-v_q(j)}$ both if $j \not\equiv_p 0$ and if $j \equiv_p 0$; in the latter case we make use of the inequality $p^{\alpha-1}(p - 1) \geq \alpha + 1$ for $\alpha \geq 1$, which needs $p \geq 3$. We obtain $c = f^i r_i^{qk-1}$.

Using (2.6) instead of (2.3), we may continue as in the former case to prove (i, i′), and, in the course of this proof, also (ii, ii′). □

4. Galois descent of a divisibility

Let

$$\begin{tikzcd} T \arrow[r, hook, "G"] & \tilde{T} \\ S \arrow[u, hook, "m"] \arrow[r, hook, "G"] & \tilde{S} \arrow[u, hook, "m"'] \end{tikzcd}$$

be a commutative diagram of finite, purely ramified extensions of discrete valuation rings. Let $s \in S$, $t \in T$, $\tilde{s} \in \tilde{S}$ and $\tilde{t} \in \tilde{T}$ generate the respective maximal ideals. Let $L = \operatorname{frac} S$, $M = \operatorname{frac} T$, $\tilde{L} = \operatorname{frac} \tilde{S}$ and $\tilde{M} = \operatorname{frac} \tilde{T}$ denote the respective fields of fractions. We assume the extensions $M|L$ and $\tilde{L}|L$ to be linearly disjoint and $\tilde{M}$ to be the composite of M and $\tilde{L}$. Thus $m := [M : L] = [\tilde{M} : \tilde{L}]$ and $[\tilde{L} : L] = [\tilde{M} : M]$. We assume $\tilde{L}|L$ to be galois and identify $G := \operatorname{Gal}(\tilde{L}|L) = \operatorname{Gal}(\tilde{M}|M)$ via restriction. We may and will assume that $s = \mathrm{N}_{\tilde{L}|L}(\tilde{s})$, and that $t = \mathrm{N}_{\tilde{M}|M}(\tilde{t})$.

Lemma 4.1. *In* $\tilde{T}$ *, the element* $1 - \tilde{t}^m/\tilde{s}$ *divides* $1 - t^m/s$ *.*

Proof. Let $\tilde{d} = 1 - \tilde{t}^m/\tilde{s}$, so that $\tilde{t}^m = \tilde{s}(1 - \tilde{d})$. We conclude

$$\begin{aligned} t^m &= \mathrm{N}_{\tilde{M}|M}(\tilde{t}^m) \\ &= \mathrm{N}_{\tilde{L}|L}(\tilde{s}) \cdot \prod_{\sigma \in G} (1 - \tilde{d}^\sigma) \\ &\equiv_{s\tilde{d}} \; s \,. \end{aligned}$$

□

5. Cyclotomic number fields

5.1. Coefficient valuation bounds. For $n \geq 1$, we let ζ_{p^n} be a primitive p^nth root of unity over $\mathbf{Q}$. We make choices in such a manner that $\zeta_{p^n}^p = \zeta_{p^{n-1}}$ for $n \geq 2$. We denote $\vartheta_n = \zeta_{p^n} - 1$ and $F_n = \mathbf{Q}(\zeta_{p^n})$. Let $E_n = \operatorname{Fix}_{C_{p-1}} F_n$, so $[E_n : \mathbf{Q}] = p^{n-1}$. Let

$$\pi_n \;=\; \mathrm{N}_{F_n|E_n}(\vartheta_n) \;=\; \prod_{j \in [1,\, p-1]} (\zeta_{p^n}^{j^{p^{n-1}}} - 1) \,.$$

The minimal polynomial $\mu_{\vartheta_n, F_{n-1}}(X) = (X+1)^p - \vartheta_{n-1} - 1$ shows that $\mathrm{N}_{F_n|F_{n-1}}(\vartheta_n) = \vartheta_{n-1}$, hence also $\mathrm{N}_{E_n|E_{n-1}}(\pi_n) = \pi_{n-1}$. Note that $\pi_1 = p$ and $E_1 = \mathbf{Q}$.

Let $\mathcal{O}$ be the integral closure of $\mathbf{Z}_{(p)}$ in E_n. Since $\mathrm{N}_{E_n|\mathbf{Q}}(\pi_n) = \pi_1 = p$, we have $\mathbf{Z}_{(p)}/p\mathbf{Z}_{(p)} \xrightarrow{\sim} \mathcal{O}/\pi_n\mathcal{O}$. In particular, the ideal $\pi_n\mathcal{O}$ in $\mathcal{O}$ is prime. Now $\pi_n^{p^{n-1}}\mathcal{O} = p\mathcal{O}$, since $\pi_n^{p^{n-1}}/p = \pi_n^{p^{n-1}}/\mathrm{N}_{E_n|\mathbf{Q}}(\pi_n) \in \mathbf{Z}_{(p)}[\vartheta_n]^* \cap E_n = \mathcal{O}^*$. Thus $\mathcal{O}$ is a discrete valuation ring, purely ramified of degree p^{n-1} over $\mathbf{Z}_{(p)}$, and so $\mathcal{O} = \mathbf{Z}_{(p)}[\pi_n]$ [9, I.§7, prop. 18]. In particular, $E_n = \mathbf{Q}(\pi_n)$.

Remark 5.1. The subring $\mathbf{Z}[\pi_n]$ of $\mathbf{Q}(\pi_n)$, however, is not integrally closed in general. For example, if $p = 5$ and $n = 2$, then $\mu_{\pi_2,\mathbf{Q}}(X) = X^5 - 20X^4 + 100X^3 - 125X^2 + 50X - 5$ has discriminant $5^8 \cdot 7^6$, which does not divide the discriminant of $\Phi_{5^2}(X)$, which is 5^{35}.

Lemma 5.2. *We have* $\pi_n^p \equiv_{\pi_n^{p-1}p} \pi_{n-1}$ *for* $n \geq 2$.

Proof. First of all, $\vartheta_n^p \equiv_{\vartheta_n p} \vartheta_{n-1}$ since $(X-1)^p - (X^p - 1)$ is divisible by $p(X-1)$ in $\mathbf{Z}[X]$. Letting $\tilde{T} = \mathbf{Z}_{(p)}[\vartheta_n]$ and $(\tilde{t}, \tilde{s}, t, s) = (\vartheta_n, \vartheta_{n-1}, \pi_n, \pi_{n-1})$, (4.1) shows that $1 - \vartheta_n^p/\vartheta_{n-1}$ divides $1 - \pi_n^p/\pi_{n-1}$. Therefore, $\vartheta_n p\, \vartheta_{n-1}^{-1} \pi_{n-1}$ divides $\pi_{n-1} - \pi_n^p$. $\square$

Now suppose given $m \geq 1$. To apply (3.2), we let $f = q = p$, $R_i = \mathbf{Z}_{(p)}[\pi_{m+i}]$ and $r_i = \pi_{m+i}$ for $i \geq 0$. We keep the notation

$$\begin{aligned} \mu_{\pi_{m+i},\, E_m}(X) \;&=\; \mu_{r_i,\, K_0}(X) \;=\; X^{p^i} + \Big(\sum_{j \in [1, p^i - 1]} a_{i,j} X^j \Big) - \pi_m \\ &\in\; R_0[X] \;=\; \mathbf{Z}_{(p)}[\pi_m][X] \,. \end{aligned}$$

Theorem 5.3.

(i) *We have* $p^i \mid j a_{i,j}$ *for* $i \geq 1$ *and* $j \in [1, p^i - 1]$.

(i′) *If* $j < p^i(p-2)/(p-1)$, *then* $p^i \pi_m \mid j a_{i,j}$.

(ii) *We have* $a_{i,j} \equiv_{p^{i+1}} a_{i+\beta, p^\beta j}$ *for* $i \geq 1$, $j \in [1, p^i - 1]$ *and* $\beta \geq 1$.

(ii′) *If* $j < p^i(p-2)/(p-1)$, *then* $a_{i,j} \equiv_{p^{i+1}\pi_m} a_{i+\beta, p^\beta j}$.

Assumption (3.1) is fulfilled by virtue of (5.2), whence the assertions follow by (3.2).

Example 5.4. For $p = 5$, $m = 1$ and $i = 2$, we have

$$\begin{aligned} \mu_{\pi_3, \mathbf{Q}}(X) \;=\; & X^{25} - 4 \cdot 5^2 X^{24} + 182 \cdot 5^2 X^{23} - 8 \cdot 5^6 X^{22} + 92823 \cdot 5^2 X^{21} \\ -\; & 6175454 \cdot 5 X^{20} + 12194014 \cdot 5^2 X^{19} - 18252879 \cdot 5^3 X^{18} \\ +\; & 4197451 \cdot 5^5 X^{17} - 466901494 \cdot 5^3 X^{16} + 8064511079 \cdot 5^2 X^{15} \\ -\; & 4323587013 \cdot 5^3 X^{14} + 1791452496 \cdot 5^4 X^{13} \\ -\; & 113846228 \cdot 5^6 X^{12} + 685227294 \cdot 5^5 X^{11} \\ -\; & 15357724251 \cdot 5^3 X^{10} + 2002848591 \cdot 5^4 X^9 \\ -\; & 4603857997 \cdot 5^3 X^8 + 287207871 \cdot 5^4 X^7 - 291561379 \cdot 5^3 X^6 \\ +\; & 185467152 \cdot 5^2 X^5 - 2832523 \cdot 5^3 X^4 + 121494 \cdot 5^3 X^3 \\ -\; & 514 \cdot 5^4 X^2 + 4 \cdot 5^4 X - 5 \,. \end{aligned}$$

Now $v_5(a_{3,22}) = 6 \neq 5 = v_5(a_{4,5\cdot 22})$, so the valuations of the coefficients considered in (5.3.ii) differ in general. This, however, does not contradict the assertion $a_{3,22} \equiv_{5^4} a_{4,\,5\cdot 22}$ from loc. cit.

5.2. A different proof of (5.3. i, i′) and some exact valuations. Let $m \geq 1$ and $i \geq 0$. We denote $R_i = \mathbf{Z}_{(p)}[\pi_{m+i}]$, $r_i = \pi_{m+i}$, $K_i = \operatorname{frac} R_i$, $\tilde{R}_i = \mathbf{Z}_{(p)}[\vartheta_{m+i}]$ and $\tilde{r}_i = \vartheta_{m+i}$. Denoting by $\mathfrak{D}$ the respective different [9, III.§3], we have $\mathfrak{D}_{\tilde{R}_i | \tilde{R}_0} = (p^i)$ and $\mathfrak{D}_{\tilde{R}_i | R_i} = (\tilde{r}_i^{p-2})$ [9, III.§3, prop. 13],

whence
(∗)
$$\mathfrak{D}_{R_i|R_0} \;=\; \big(\mu'_{r_i,K_0}(r_i)\big) \;=\; \mathfrak{D}_{\tilde{R}_i|\tilde{R}_0}\mathfrak{D}_{\tilde{R}_0|R_0}\mathfrak{D}^{-1}_{\tilde{R}_i|R_i} \;=\; \Big(p^i r_i^{p^i-1-(p^i-1)/(p-1)}\Big)\,,$$

cf. [9, III.§3, cor. 2]. Therefore, $p^i r_i^{p^i-1-(p^i-1)/(p-1)}$ divides $ja_{i,j}r_i^{j-1}$ for $j\in[1,p^i-1]$, and (5.3. i, i′) follow.

Moreover, since only for $j = p^i-(p^i-1)/(p-1)$ the valuations at r_i of $p^i r_i^{p^i-1-(p^i-1)/(p-1)}$ and $ja_{i,j}r_i^{j-1}$ are congruent modulo p^i, we conclude by (∗) that they are equal, i.e. that p^i exactly divides $a_{i,p^i-(p^i-1)/(p-1)}$.

Corollary 5.5. *The element $p^{i-\beta}$ exactly divides $a_{i,p^i-(p^i-p^\beta)/(p-1)}$ for $\beta\in[0,i-1]$.*

Proof. This follows by (5.3.ii) from what we have just said. □

E.g. in (5.4), 5^1 exactly divides $a_{2,25-5} = a_{2,20}$, and 5^2 exactly divides $a_{2,25-5-1} = a_{2,19}$.

5.3. Some traces. Let $\boldsymbol{\mu}_{p-1}$ denote the group of $(p-1)$st roots of unity in $\mathbf{Q}_p$. We choose a primitive $(p-1)$st root of unity $\zeta_{p-1}\in\boldsymbol{\mu}_{p-1}$ and may thus view $\mathbf{Q}(\zeta_{p-1})\subseteq\mathbf{Q}_p$ as a subfield. Note that $[\mathbf{Q}(\zeta_{p-1}):\mathbf{Q}] = \varphi(p-1)$, where φ denotes Euler's function. The restriction of the valuation v_p at p on $\mathbf{Q}_p$ to $\mathbf{Q}(\zeta_p)$, is a prolongation of the valuation v_p on $\mathbf{Q}$ to $\mathbf{Q}(\zeta_{p-1})$ (there are $\varphi(p-1)$ such prolongations).

Proposition 5.6. *For $n\geq 1$, we have*
$$\mathrm{Tr}_{E_n|\mathbf{Q}}(\pi_n) \;=\; p^n s_n - p^{n-1}s_{n-1}\;,$$
where
$$s_n \;:=\; \frac{1}{p-1}\sum_{H\,\subseteq\,\boldsymbol{\mu}_{p-1}} (-1)^{\#H}\Big\{v_p\big(\textstyle\sum_{\xi\in H}\xi\big)\geq n\Big\} \quad \textit{for}\quad n\geq 0\;.$$
We have $s_0 = 0$, and $s_n\in\mathbf{Z}$ for $n\geq 0$. The sequence $(s_n)_n$ becomes stationary at some minimally chosen $N_0(p)$. We have
$$N_0(p) \;\leq\; N(p) \;:=\; \max_{H\,\subseteq\,\boldsymbol{\mu}_{p-1}} \Big\{v_p\big(\textstyle\sum_{\xi\in H}\xi\big):\ \sum_{\xi\in H}\xi\neq 0\Big\}+1\;.$$

An upper estimate for $N(p)$, hence for $N_0(p)$, is given in (5.13).

Proof. For $j\in[1,p-1]$ the p-adic limits
$$\xi(j) \;:=\; \lim_{n\to\infty} j^{p^n}$$
exist since $j^{p^{n-1}}\equiv_{p^n} j^{p^n}$ by (1.3). They are distinct since $\xi(j)\equiv_p j$, and, thus, form the group $\boldsymbol{\mu}_{p-1} = \{\xi(j)\mid j\in[1,p-1]\}$. Using the formula
$$\mathrm{Tr}_{F_n|\mathbf{Q}}(\zeta_{p^n}^m) \;=\; p^n\big\{v_p(m)\geq n\big\} - p^{n-1}\big\{v_p(m)\geq n-1\big\}$$

and the fact that $j^{p^{n-1}} \equiv_{p^n} \xi(j)$, we obtain

$$\begin{aligned}
\mathrm{Tr}_{F_n|\mathbf{Q}}(\pi_n) &= \mathrm{Tr}_{F_n|\mathbf{Q}}\Big(\prod_{j\in[1,\,p-1]} \Big(1-\zeta_{p^n}^{j^{p^{n-1}}}\Big)\Big) \\
&= \sum_{J\,\subseteq\,[1,\,p-1]} (-1)^{\#J}\, \mathrm{Tr}_{F_n|\mathbf{Q}}\Big(\zeta_{p^n}^{\sum_{j\in J} j^{p^{n-1}}}\Big) \\
&= \sum_{J\,\subseteq\,[1,\,p-1]} (-1)^{\#J} \Big(p^n \Big\{ v_p\big(\textstyle\sum_{j\in J}\xi(j)\big) \geq n \Big\} \\
&\qquad\qquad - \; p^{n-1}\Big\{ v_p\big(\textstyle\sum_{j\in J}\xi(j)\big) \geq n-1 \Big\}\Big) \\
&= (p-1)(p^n s_n - p^{n-1}s_{n-1})\ ,
\end{aligned}$$

whence

$$\mathrm{Tr}_{E_n|\mathbf{Q}}(\pi_n) \;=\; p^n s_n - p^{n-1} s_{n-1}\ .$$

Now $s_0 = 0 \in \mathbf{Z}$ by the binomial formula. Therefore, by induction, we conclude from $p^n s_n - p^{n-1}s_{n-1} \in \mathbf{Z}$ that $p^n s_n \in \mathbf{Z}$. Since $(p-1)s_n \in \mathbf{Z}$, too, we obtain $s_n \in \mathbf{Z}$.

As soon as $n \geq N(p)$, the conditions $v_p(\sum_{\xi\in H}\xi) \geq n$ and $v_p(\sum_{\xi\in H}\xi) = +\infty$ on $H \subseteq \boldsymbol{\mu}_{p-1}$ become equivalent, and we obtain

$$s_n \;=\; \frac{1}{p-1} \sum_{H\subseteq \boldsymbol{\mu}_{p-1}} (-1)^{\#H} \big\{ \textstyle\sum_{\xi\in H}\xi = 0 \big\}\ ,$$

which is independent of n. Thus $N_0(p) \leq N(p)$. □

Lemma 5.7. *We have $s_1 = 1$. In particular,* $\mathrm{Tr}_{E_2|\mathbf{Q}}(\pi_2) \;\equiv_{p^2}\; -p$.

Proof. Since $\mathrm{Tr}_{E_1|\mathbf{Q}}(\pi_1) = \mathrm{Tr}_{\mathbf{Q}|\mathbf{Q}}(p) = p$, and since $s_0 = 0$, we have $s_1 = 1$ by (5.6). The congruence for $\mathrm{Tr}_{E_2|\mathbf{Q}}(\pi_2)$ follows again by (5.6). □

Corollary 5.8. *We have*

$$\mu_{\pi_n,\mathbf{Q}}(X) \;\equiv_{p^2}\; X^{p^{n-1}} + pX^{(p-1)p^{n-2}} - p$$

for $n \geq 2$.

Proof. By dint of (5.7), this ensues from $(5.3.\,\mathrm{i}',\mathrm{ii})$. □

Example 5.9. The last n for which we list s_n equals $N(p)$, except if there is a question mark in the next column. The table was calculated using Pascal ($p \leq 53$) and Magma ($p \geq 59$). In the last column, we list the upper bound for $N(p)$ calculated below (5.13).

	$n =$								upper
s_n	0	1	2	3	4	5	6	7	bound for $N(p)$
$p = 3$	0	1							
5	0	1							1
7	0	1							1
11	0	1	3						3
13	0	1	3						3
17	0	1	8	16					5
19	0	1	10	12					4
23	0	1	33	89	93				7
29	0	1	377	571	567				8
31	0	1	315	271	259				6
37	0	1	107	940	1296				9
41	0	1	6621	51693	18286	20186	20250		12
43	0	1	1707	4767	6921	6665			9
47	0	1	2250	272242	173355	181481	182361		16
53	0	1	71201	363798	1520045	1350049	1292229	1289925	18
59	0	1	1276	?					21
61	0	1	2516	?					12
67	0	1	407186	?					15
71	0	1	5816605	?					18
73	0	1	8370710	?					18
79	0	1	169135	?					18
83	0	1	632598	?					30
89	0	1	26445104	?					30
97	0	1	282789	?					24
101	0	1	25062002	?					31
103	0	1	56744199	?					25
107	0	1	1181268305	?					40
109	0	1	91281629	?					28
113	0	1	117774911422	?					37
127	0	1	6905447	?					28
131	0	1	2988330952791	?					37
137	0	1	1409600547	?					50
139	0	1	3519937121	?					34
149	0	1	25026940499	?					56
151	0	1	164670499159	?					31
157	0	1	51594129045351	?					38
163	0	1	288966887341	?					42
167	0	1	1205890070471	?					64
173	0	1	17802886165762	?					66
179	0	1	1311887715966	?					69
181	0	1	128390222739	?					38
191	0	1	233425263577158	?					57
193	0	1	306518196952028	?					51
197	0	1	347929949728221	?					66
199	0	1	9314622093145	?					48
211	0	1	12532938009082	?					39

So for example if $p = 31$, then $\mathrm{Tr}_{\mathbf{Q}(\pi_3)|\mathbf{Q}}(\pi_3) = 271\cdot 31^3 - 315\cdot 31^2$, whereas $\mathrm{Tr}_{\mathbf{Q}(\pi_7)|\mathbf{Q}}(\pi_7) = 259 \cdot 31^7 - 259 \cdot 31^6$. Moreover, $N_0(31) = N(31) = 4 \leq 6$.

Remark 5.10. Vanishing (resp. vanishing modulo a prime) of sums of roots of unity has been studied extensively. See e.g. [2], [6], where also further references may be found.

Remark 5.11. Neither do we know whether $s_n \geq 0$ nor whether $\mathrm{Tr}_{E_n|\mathbf{Q}}(\pi_n) \geq 0$ always hold. Moreover, we do not know a prime p for which $N_0(p) < N(p)$.

Remark 5.12. We calculated some further traces appearing in (5.3), using Maple and Magma.

For $p = 3$, $n \in [2, 10]$, we have $\mathrm{Tr}_{E_n|E_{n-1}}(\pi_n) = 3 \cdot 2$.
For $p = 5$, $n \in [2, 6]$, we have $\mathrm{Tr}_{E_n|E_{n-1}}(\pi_n) = 5 \cdot 4$.
For $p = 7$, $n \in [2, 5]$, we have $\mathrm{Tr}_{E_n|E_{n-1}}(\pi_n) = 7 \cdot 6$.
For $p = 11$, we have $\mathrm{Tr}_{E_2|E_1}(\pi_2) = 11 \cdot 32$, whereas

$$\begin{aligned}
&\mathrm{Tr}_{E_3|E_2}(\pi_3)\\
&= 22 \cdot (15 + \zeta^2 + 2\zeta^3 - \zeta^5 + \zeta^6 - 2\zeta^8 - \zeta^9 + 2\zeta^{14} - \zeta^{16} + \zeta^{18} - \zeta^{20}\\
&- 2\zeta^{24} + 2\zeta^{25} - 2\zeta^{26} - \zeta^{27} - \zeta^{31} + 2\zeta^{36} - \zeta^{38} + \zeta^{41} - \zeta^{42} - 2\zeta^{43} + 2\zeta^{47}\\
&- 3\zeta^{49} - \zeta^{53} + \zeta^{54} + 2\zeta^{58} - \zeta^{60} - \zeta^{64} + \zeta^{67} + 2\zeta^{69} - \zeta^{71} - 2\zeta^{72} - \zeta^{75}\\
&- 2\zeta^{78} + 3\zeta^{80} - \zeta^{82} - \zeta^{86} + 2\zeta^{91} - \zeta^{93} - 2\zeta^{95} - 3\zeta^{97} + 2\zeta^{102} + \zeta^{103}\\
&- \zeta^{104} - \zeta^{108})\\
&= 22 \cdot 2014455354550939310427^{-1} \cdot (3433387135252772281065 4\\
&+ 1360272405267541318242502\pi - 31857841148164445311437042\pi^2\\
&+ 13573370840985597605965863 6\pi^3 - 837636131300171423715664 53\pi^4\\
&+ 204448065993444081042992 52\pi^5 - 229636463121144263216893 2\pi^6\\
&+ 117743741083866218812293\pi^7 - 2797258465425206085093\pi^8\\
&+ 27868038642441136108\pi^9 - 791705132439248 42\pi^{10})\ ,
\end{aligned}$$

where $\zeta := \zeta_{11^2}$ and $\pi := \pi_2$.

5.4. An upper bound for $N(p)$**.** We view $\mathbf{Q}(\zeta_{p-1})$ as a subfield of $\mathbf{Q}_p$, and now, in addition, as a subfield of $\mathbf{C}$. Since complex conjugation commutes with the operation of $\mathrm{Gal}(\mathbf{Q}(\zeta_{p-1})|\mathbf{Q})$, we have $|\mathrm{N}_{\mathbf{Q}(\zeta_{p-1})|\mathbf{Q}}(x)| = |x|^{\varphi(p-1)}$ for $x \in \mathbf{Q}(\zeta_{p-1})$.

We abbreviate $\Sigma(H) := \sum_{\xi \in H} \xi$ for $H \subseteq \boldsymbol{\mu}_{p-1}$. Since $|\Sigma(H)| \leq p - 1$, we have $|\mathrm{N}_{\mathbf{Q}(\zeta_{p-1})|\mathbf{Q}}(\Sigma(H))| \leq (p-1)^{\varphi(p-1)}$. Hence, if $\Sigma(H) \neq 0$, then

$$v_p(\Sigma(H)) \ \leq\ v_p(\mathrm{N}_{\mathbf{Q}(\zeta_{p-1})|\mathbf{Q}}(\Sigma(H))) \ <\ \varphi(p-1)\ ,$$

and therefore $N(p) \leq \varphi(p-1)$. We shall ameliorate this bound by a logarithmic term.

Proposition 5.13. *We have*

$$N(p) \ \leq\ \varphi(p-1)\left(1 - \frac{\log \pi}{\log p}\right) + 1$$

for $p \geq 5$.

Proof. It suffices to show that $|\Sigma(H)| \leq p/\pi$ for $H \subseteq \boldsymbol{\mu}_{p-1}$. We will actually show that

$$\max_{H \subseteq \boldsymbol{\mu}_{p-1}} |\Sigma(H)| \;=\; \frac{1}{\sin \frac{\pi}{p-1}} \;,$$

from which this inequality follows using $\sin x \geq x - x^3/6$ and $p \geq 5$.

Choose $H \subseteq \boldsymbol{\mu}_{p-1}$ such that $|\Sigma(H)|$ is maximal. Since $p-1$ is even, the $(p-1)$st roots of unity fall into pairs $(\eta, -\eta)$. The summands of $\Sigma(H)$ contain exactly one element of each such pair, since $|\Sigma(H)+\eta|^2 + |\Sigma(H)-\eta|^2 = 2|\Sigma(H)|^2 + 2$ shows that at least one of the inequalities $|\Sigma(H)+\eta| \leq |\Sigma(H)|$ and $|\Sigma(H)-\eta| \leq |\Sigma(H)|$ fails.

By maximality, replacing a summand η by $-\eta$ in $\Sigma(H)$ does not increase the value of $|\Sigma(H)|$, whence

$$|\Sigma(H)|^2 \;\geq\; |\Sigma(H) - 2\eta|^2 \;=\; |\Sigma(H)|^2 - 4\,\mathrm{Re}(\eta \cdot \overline{\Sigma(H)}) + 4 \;,$$

and thus

$$\mathrm{Re}(\eta \cdot \overline{\Sigma(H)}) \;\geq\; 1 \;>\; 0 \;.$$

Therefore, the $(p-1)/2$ summands of $\Sigma(H)$ lie in one half-plane, whence the value of $|\Sigma(H)|$. $\square$

6. Cyclotomic function fields, after Carlitz and Hayes

6.1. Notation and basic facts.

We shall give a brief review while fixing notation.

Let $\rho \geq 1$ and $r := p^\rho$. Write $\mathcal{Z} := \mathbf{F}_r[Y]$ and $\mathcal{Q} := \mathbf{F}_r(Y)$, where Y is an independent variable. We fix an algebraic closure $\bar{\mathcal{Q}}$ of $\mathcal{Q}$. The *Carlitz module structure* on $\bar{\mathcal{Q}}$ is defined by the $\mathbf{F}_r$-algebra homomorphism given on the generator Y as

$$\begin{array}{rcl} \mathcal{Z} & \longrightarrow & \mathrm{End}_{\mathcal{Q}} \bar{\mathcal{Q}} \\ Y & \longmapsto & \Big(\xi \longmapsto \xi^Y \;:=\; Y\xi + \xi^r\Big) \;. \end{array}$$

We write the module product of $\xi \in \bar{\mathcal{Q}}$ with $e \in \mathcal{Z}$ as ξ^e. For each $e \in \mathcal{Z}$, there exists a unique polynomial $P_e(X) \in \mathcal{Z}[X]$ that satisfies $P_e(\xi) = \xi^e$ for all $\xi \in \bar{\mathcal{Q}}$. In fact, $P_1(X) = X$, $P_Y(X) = YX + X^r$, and $P_{Y^{i+1}} = YP_{Y^i}(X) + P_{Y^i}(X^r)$ for $i \geq 1$. For a general $e \in \mathcal{Z}$, the polynomial $P_e(Y)$ is given by the according linear combination of these.

Note that $P_e(0) = 0$, and that $P_e'(X) = e$, whence $P_e(X)$ is separable, i.e. it decomposes as a product of distinct linear factors in $\bar{\mathcal{Q}}[X]$. Let

$$\boldsymbol{\lambda}_e \;=\; \mathrm{ann}_e \bar{\mathcal{Q}} \;=\; \{\xi \in \bar{\mathcal{Q}} \;:\; \xi^e = 0\} \;\subseteq\; \bar{\mathcal{Q}}$$

be the annihilator submodule. Separability of $P_e(X)$ shows that $\#\boldsymbol{\lambda}_e = \deg P_e(X) = r^{\deg e}$. Given a $\mathcal{Q}$-linear automorphism σ of $\bar{\mathcal{Q}}$, we have $(\xi^e)^\sigma = P_e(\xi)^\sigma = P_e(\xi^\sigma) = (\xi^\sigma)^e$. In particular, $\boldsymbol{\lambda}_e$ is stable under σ. Therefore, $\mathcal{Q}(\boldsymbol{\lambda}_e)$ is a Galois extension of $\mathcal{Q}$.

Since $\#\mathrm{ann}_{\tilde{e}}\boldsymbol{\lambda}_e = \#\boldsymbol{\lambda}_{\tilde{e}} = r^{\deg \tilde{e}}$ for $\tilde{e} \mid e$, we have $\boldsymbol{\lambda}_e \simeq \mathcal{Z}/e$ as $\mathcal{Z}$-modules. It is not possible, however, to distinguish a particular isomorphism.

We shall restrict ourselves to prime powers now. We fix a monic irreducible polynomial $f = f(Y) \in \mathcal{Z}$ and write $q := r^{\deg f}$. For $n \geq 1$, we let θ_n be a $\mathcal{Z}$-linear generator of $\boldsymbol{\lambda}_{f^n}$. We make our choices in such a manner that $\theta_{n+1}^f = \theta_n$ for $n \geq 1$. Note that $\mathcal{Z}[\boldsymbol{\lambda}_{f^n}] = \mathcal{Z}[\theta_n]$ since the elements of $\boldsymbol{\lambda}_{f^n}$ are polynomial expressions in θ_n.

Suppose given two roots $\xi, \tilde{\xi} \in \bar{\mathcal{Q}}$ of

$$\Psi_{f^n}(X) \;:=\; P_{f^n}(X)/P_{f^{n-1}}(X) \;\in\; \mathcal{Z}[X] \;,$$

i.e. $\xi, \tilde{\xi} \in \boldsymbol{\lambda}_{f^n} \smallsetminus \boldsymbol{\lambda}_{f^{n-1}}$. Since ξ is a $\mathcal{Z}$-linear generator of $\boldsymbol{\lambda}_{f^n}$, there is an $e \in \mathcal{Z}$ such that $\tilde{\xi} = \xi^e$. Since $\xi^e/\xi = P_e(X)/X|_{X=\xi} \in \mathcal{Z}[\theta_n]$, $\tilde{\xi}$ is a multiple of ξ in $\mathcal{Z}[\theta_n]$. Reversing the argument, we see that $\tilde{\xi}$ is in fact a unit multiple of ξ in $\mathcal{Z}[\theta_n]$.

Lemma 6.1. *The polynomial $\Psi_{f^n}(X)$ is irreducible.*

Proof. We have $\Psi_{f^n}(0) = \left.\dfrac{P_{f^n}(X)/X}{P_{f^{n-1}}(X)/X}\right|_{X=0} = f$. We decompose $\Psi_{f^n}(X) = \prod_{i\in[1,k]} F_i(X)$ in its distinct monic irreducible factors $F_i(X) \in \mathcal{Z}[X]$. One of the constant terms, say $F_j(0)$, is thus a unit multiple of f in $\mathcal{Z}$, while the other constant terms are units. Thus, being conjugate under the Galois action, all roots of $F_j(X)$ in $\mathcal{Q}[\theta_n]$ are non-units in $\mathcal{Z}[\theta_n]$, and the remaining roots of $\Psi_{f^n}(X)$ are units. But all roots of $\Psi_{f^n}(X)$ are unit multiples of each other. We conclude that $\Psi_{f^n}(X) = F_j(X)$ is irreducible. □

By (6.1), $\Psi_{f^n}(X)$ is the minimal polynomial of θ_n over $\mathcal{Q}$. In particular, $[\mathcal{Q}(\theta_n) : \mathcal{Q}] = q^{n-1}(q-1)$, and so

$$\mathcal{Z}[\theta_n]\theta_n^{(q-1)q^{n-1}} \;=\; \mathcal{Z}[\theta_n]\mathrm{N}_{\mathcal{Q}(\theta_n)|\mathcal{Q}}(\theta_n) \;=\; \mathcal{Z}[\theta_n]f \;.$$

In particular, $\mathcal{Z}_{(f)}[\theta_n]$ is a discrete valuation ring with maximal ideal generated by θ_n, purely ramified of index $q^{n-1}(q-1)$ over $\mathcal{Z}_{(f)}$, cf. [9, I.§7, prop. 18]. There is a group isomorphism

$$\begin{array}{rcl} (\mathcal{Z}/f^n)^* & \xrightarrow{\sim} & \mathrm{Gal}(\mathcal{Q}(\theta_n)|\mathcal{Q}) \\ e & \longmapsto & (\theta_n \longmapsto \theta_n^e) \;, \end{array}$$

well defined since θ_n^e is a root of $\Psi_{f^n}(X)$, too; injective since θ_n generates $\boldsymbol{\lambda}_{f^n}$ over $\mathcal{Z}$; and surjective by cardinality.

Note that the Galois operation on $\mathcal{Q}(\theta_n)$ corresponding to $e \in (\mathcal{Z}/f^n)^*$ coincides with the module operation of e on the element θ_n, but not everywhere. For instance, if $f \neq Y$, then the Galois operation corresponding to Y sends 1 to 1, whereas the module operation of Y sends 1 to $Y + 1$.

The discriminant of $\mathcal{Z}[\theta_n]$ over $\mathcal{Z}$ is given by

$$\begin{aligned}
\Delta_{\mathcal{Z}[\theta_n]|\mathcal{Z}} &= \mathrm{N}_{\mathcal{Q}(\theta_n)|\mathcal{Q}}(\Psi'_{f^n}(\theta_n)) \\
&= \mathrm{N}_{\mathcal{Q}(\theta_n)|\mathcal{Q}}\left(P'_{f^n}(\theta_n)/P_{f^{n-1}}(\theta_n)\right) \\
&= \mathrm{N}_{\mathcal{Q}(\theta_n)|\mathcal{Q}}\left(f^n/\theta_1\right) \\
&= f^{q^{n-1}(nq-n-1)} .
\end{aligned}$$

Lemma 6.2. *The ring $\mathcal{Z}[\theta_n]$ is the integral closure of $\mathcal{Z}$ in $\mathcal{Q}(\theta_n)$.*

Proof. Let $e \in \mathcal{Z}$ be a monic irreducible polynomial different from f. Write $\mathcal{O}_0 := \mathcal{Z}_{(e)}[\theta_n]$ and let $\mathcal{O}$ be the integral closure of $\mathcal{O}_0$ in $\mathcal{Q}(\theta_n)$. Let

$$\begin{aligned}
\mathcal{O}_0^+ &:= \{\xi \in \mathcal{Q}(\theta_n) \,:\, \mathrm{Tr}_{\mathcal{Q}(\theta_n)|\mathcal{Q}}(\xi\mathcal{O}_0) \subseteq \mathcal{Z}_{(e)}\} \\
\mathcal{O}^+ &:= \{\xi \in \mathcal{Q}(\theta_n) \,:\, \mathrm{Tr}_{\mathcal{Q}(\theta_n)|\mathcal{Q}}(\xi\mathcal{O}) \subseteq \mathcal{Z}_{(e)}\} .
\end{aligned}$$

Then $\mathcal{O}_0 \subseteq \mathcal{O} \subseteq \mathcal{O}^+ \subseteq \mathcal{O}_0^+$. But $\mathcal{O}_0 = \mathcal{O}_0^+$, since the $\mathcal{Z}_{(e)}$-linear determinant of this embedding is given by the discriminant $\Delta_{\mathcal{Z}[\theta_n]|\mathcal{Z}}$, which is a unit in $\mathcal{O}_0$. □

We resume.

Proposition 6.3 ([1],[5], cf. [3, p. 115])**.** *The extension $\mathcal{Q}(\theta_n)|\mathcal{Q}$ is galois of degree $[\mathcal{Q}(\theta_n) : \mathcal{Q}] = (q-1)q^{n-1}$, with Galois group isomorphic to $(\mathcal{Z}/f^n)^*$. The integral closure of $\mathcal{Z}$ in $\mathcal{Q}(\theta_n)$ is given by $\mathcal{Z}[\theta_n]$. We have $\mathcal{Z}[\theta_n]\theta_n^{[\mathcal{Q}(\theta_n):\mathcal{Q}]} = \mathcal{Z}[\theta_n]f$. In particular, θ_n is a prime element of $\mathcal{Z}[\theta_n]$, and the extension $\mathcal{Z}_{(f)}[\theta_n]|\mathcal{Z}_{(f)}$ of discrete valuation rings is purely ramified.*

6.2. Coefficient valuation bounds. Denote $\mathcal{F}_n = \mathcal{Q}(\theta_n)$. Let $\mathcal{E}_n = \mathrm{Fix}_{C_{q-1}}\mathcal{F}_n$, so $[\mathcal{E}_n : \mathcal{Q}] = q^{n-1}$. Let

$$\varpi_n = \mathrm{N}_{\mathcal{F}_n|\mathcal{E}_n}(\theta_n) = \prod_{e\in(\mathcal{Z}/f)^*} \theta_n^{e^{q^{n-1}}} .$$

The minimal polynomial $\mu_{\theta_n,\mathcal{F}_{n-1}}(X) = P_f(X) - \theta_{n-1}$ together with the fact that X divides $P_f(X)$ shows that $\mathrm{N}_{\mathcal{F}_n|\mathcal{F}_{n-1}}(\theta_n) = \theta_{n-1}$, whence $\mathrm{N}_{\mathcal{E}_n|\mathcal{E}_{n-1}}(\varpi_n) = \varpi_{n-1}$. Note that $\varpi_1 = \prod_{e\in(\mathcal{Z}/f)^*}\theta_1^e = \Psi_f(0) = f$.

The extension $\mathcal{Z}_{(f)}[\varpi_n]$ is a discrete valuation ring with maximal ideal generated by ϖ_n, purely ramified of index q^{n-1} over $\mathcal{Z}_{(f)}$. In particular, $\mathcal{E}_n = \mathcal{Q}(\varpi_n)$.

Example 6.4. Let $r = 3$ and $f(Y) = Y^2 + 1$, so $q = 9$. A Magma calculation shows that

$$\begin{aligned}
\varpi_2 \;=\; & \theta_2^{60} - Y\theta_2^{58} + Y^2\theta_2^{56} + (-Y^9-Y^3-Y)\theta_2^{42} + (Y^{10}+Y^4+Y^2+1)\theta_2^{40} \\
+\; & (-Y^{11}-Y^5-Y^3+Y)\theta_2^{38} + (-Y^6-Y^4-Y^2)\theta_2^{36} \\
+\; & (Y^7+Y^5+Y^3+Y)\theta_2^{34} + (-Y^8-Y^6+Y^4-Y^2-1)\theta_2^{32} \\
+\; & (-Y^5+Y^3-Y)\theta_2^{30} + (Y^{18}-Y^{12}-Y^{10}+Y^6-Y^4+Y^2)\theta_2^{24} \\
+\; & (-Y^{19}+Y^{13}+Y^{11}+Y^9-Y^7+Y^5+Y)\theta_2^{22} \\
+\; & (Y^{20}-Y^{14}-Y^{12}+Y^{10}+Y^8-Y^6-Y^4+Y^2+1)\theta_2^{20} \\
+\; & (-Y^{15}-Y^{13}-Y^{11}-Y^9+Y^7+Y^5-Y^3)\theta_2^{18} \\
+\; & (Y^{16}+Y^{14}+Y^{12}-Y^{10}-Y^8-Y^2)\theta_2^{16} \\
+\; & (-Y^{17}-Y^{15}+Y^{13}+Y^{11}+Y^7+Y^5-Y^3+Y)\theta_2^{14} \\
+\; & (-Y^{14}-Y^{12}+Y^{10}-Y^8-Y^6-Y^4+Y^2+1)\theta_2^{12} \\
+\; & (-Y^{13}+Y^{11}-Y^7+Y^3)\theta_2^{10} + (Y^{14}-Y^{12}-Y^{10}+Y^6+Y^4)\theta_2^{8} \\
+\; & (-Y^{11}-Y^7+Y^5+Y^3+Y)\theta_2^{6} + (Y^8+Y^6+Y^2+1)\theta_2^{4}\,.
\end{aligned}$$

With regard to section 6.4, we remark that $\varpi_2 \neq \pm\,\theta_2^{q-1}$.

Lemma 6.5. *We have* $\varpi_n^q \;\equiv_{\varpi_n^{q-1} f}\; \varpi_{n-1}$ *for* $n \geq 2$.

Proof. We claim that $\theta_n^q \equiv_{\theta_n f} \theta_{n-1}$. In fact, the non-leading coefficients of the Eisenstein polynomial $\Psi_f(X)$ are divisible by f, so that the congruence follows by $\theta_{n-1} - \theta_n^q = P_f(\theta_n) - \theta_n^q = \theta_n(\Psi_f(\theta_n) - \theta_n^{q-1})$. Letting $\tilde{T} = \mathcal{Z}_{(f)}[\theta_n]$ and $(\tilde{t}, \tilde{s}, t, s) = (\theta_n, \theta_{n-1}, \varpi_n, \varpi_{n-1})$, (4.1) shows that $1 - \theta_n^q/\theta_{n-1}$ divides $1 - \varpi_n^q/\varpi_{n-1}$. Therefore, $\theta_n f \theta_{n-1}^{-1}\varpi_{n-1} \mid \varpi_{n-1} - \varpi_n^q$. $\square$

Now suppose given $m \geq 1$. To apply (3.2), we let $R_i = \mathcal{Z}_{(f)}[\varpi_{m+i}]$ and $r_i = \varpi_{m+i}$ for $i \geq 0$. We continue to denote

$$(\#) \qquad \begin{aligned} \mu_{\varpi_{m+i},\mathcal{E}_m}(X) \;=\; \mu_{r_i, K_0}(X) \;&=\; X^{q^i} + \Big(\textstyle\sum_{j\in[1,q^i-1]} a_{i,j} X^j\Big) - \varpi_m \\ &\in\; R_0[X] \;=\; \mathcal{Z}_{(f)}[\varpi_m][X]\,, \end{aligned}$$

and $v_q(j) = \max\{\alpha \in \mathbf{Z}_{\geq 0} \;:\; j \equiv_{q^\alpha} 0\,\}$.

Theorem 6.6.

(i) *We have* $f^{i-v_q(j)} \mid a_{i,j}$ *for* $i \geq 1$ *and* $j \in [1, q^i - 1]$.

(i′) *If* $j < q^i(q-2)/(q-1)$, *then* $f^{i-v_q(j)}\varpi_m \mid a_{i,j}$.

(ii) *We have* $a_{i,j} \equiv_{f^{i+1}} a_{i+\beta, q^\beta j}$ *for* $i \geq 1$, $j \in [1, q^i - 1]$ *and* $\beta \geq 1$.

(ii′) *If* $j < q^i(q-2)/(q-1)$, *then* $a_{i,j} \equiv_{f^{i+1}\varpi_m} a_{i+\beta, q^\beta j}$ *for* $\beta \geq 1$.

Assumption (3.1) is fulfilled by virtue of (6.5), whence the assertions follow by (3.2).

6.3. Some exact valuations. Let $m \geq 1$ and $i \geq 0$. We denote $R_i = \mathcal{Z}_{(f)}[\varpi_{m+i}]$, $r_i = \varpi_{m+i}$, $K_i = \operatorname{frac} R_i$, $\tilde{R}_i = \mathcal{Z}_{(f)}[\theta_{m+i}]$ and $\tilde{r}_i = \theta_{m+i}$. We obtain $\mathfrak{D}_{\tilde{R}_i|\tilde{R}_0} = (f^i)$ and $\mathfrak{D}_{\tilde{R}_i|R_i} = (\tilde{r}_i^{q-2})$ [9, III.§3, prop. 13], whence

$$(**) \qquad \mathfrak{D}_{R_i|R_0} \;=\; \big(\mu'_{r_i,K_0}(r_i)\big) \;=\; \Big(f^i r_i^{q^i-1-(q^i-1)/(q-1)}\Big)\;.$$

Therefore, $f^i r_i^{q^i-1-(q^i-1)/(q-1)}$ divides $j a_{i,j} r_i^{j-1}$ for $j \in [1, q^i - 1]$, which is an empty assertion if $j \equiv_p 0$. Thus (6.6. i, i′) do not follow entirely.

However, since only for $j = q^i - (q^i - 1)/(q-1)$ the valuations at r_i of $f^i r_i^{q^i-1-(q^i-1)/(q-1)}$ and $j a_{i,j} r_i^{j-1}$ are congruent modulo q^i, we conclude by $(**)$ that they are equal, i.e. that f^i exactly divides $a_{i,q^i-(q^i-1)/(q-1)}$.

Corollary 6.7. *The element $f^{i-\beta}$ exactly divides $a_{i,q^i-(q^i-q^\beta)/(q-1)}$.*

Proof. This follows by (6.6.ii) from what we have just said. □

6.4. A simple case. Suppose that $f(Y) = Y$ and $m \geq 1$. Note that

$$\varpi_{m+1} \;=\; \prod_{e\in\mathbf{F}_q^*} \theta_{m+1}^e \;=\; \prod_{e\in\mathbf{F}_q^*} e\theta_{m+1} \;=\; -\theta_{m+1}^{q-1}\;.$$

Lemma 6.8. *We have*

$$\mu_{\varpi_{m+1},\mathcal{E}_m}(X) \;=\; -\varpi_m + \sum_{j\in[1,q]} Y^{q-j} X^j\;.$$

Proof. Using the minimal polynomial $\mu_{\theta_{m+1},\mathcal{F}_m}(X) = P_Y(X) - \theta_m = X^q + YX - \theta_m$, we get

$$\begin{aligned}
& -\varpi_m + \sum_{j\in[1,q]} Y^{q-j}\varpi_{m+1}^j \\
&= \theta_m^{q-1} + (Y^{q+1} - \theta_{m+1}^{q^2-1})/(Y + \theta_{m+1}^{q-1}) - Y^q \\
&= (Y\theta_m^{q-1}\theta_{m+1} + \theta_m^{q-1}\theta_{m+1}^q - \theta_{m+1}^{q^2} - Y^q\theta_{m+1}^q)/(\theta_{m+1}(Y + \theta_{m+1}^{q-1})) \\
&= 0\;.
\end{aligned}$$

□

Corollary 6.9. *Let $m, i \geq 1$. We have*

$$\mu_{\varpi_{m+i},\mathcal{E}_m}(X) \;\equiv_{Y^2}\; X^{q^i} + YX^{(q-1)q^{i-1}} - \varpi_m\;.$$

Proof. This follows from (6.8) using (6.6.ii). □

Remark 6.10. The assertion of (6.8) also holds if $p = 2$.

Conjecture 6.11. Let $m, i \geq 1$. We use the notation of (#) above, now in the case $f(Y) = Y$. For $j \in [1, q^i]$, we write $q^i - j = \sum_{k\in[0,i-1]} d_k q^k$ with $d_k \in [0, q-1]$. Consider the following conditions.

(i) There exists $k \in [0, i-2]$ such that $d_{k+1} < d_k$.
(ii) There exists $k \in [0, i-2]$ such that $v_p(d_{k+1}) > v_p(d_k)$.

If (i) or (ii) holds, then $a_{i,j} = 0$. If neither (i) nor (ii) holds, then

$$v_{\varpi_m}(a_{i,j}) \;=\; q^{m-1} \cdot \sum_{k \in [0,i-1]} d_k \; .$$

Remark 6.12. We shall compare (6.7) with (6.11). If $j = q^i - (q^i - q^\beta)/(q-1)$ for some $\beta \in [0, i-1]$, then $q^i - j = q^{i-1} + \cdots + q^\beta$. Hence $\sum_{k \in [0,i-1]} d_k = i - \beta$, and so according to (6.11), $v_{\varpi_m}(a_{i,j})$ should equal $q^{m-1}(i-\beta)$, which is in fact confirmed by (6.7).

References

[1] L. Carlitz, *A class of polynomials.* Trans. Am. Math. Soc. **43** (2) (1938), 167–182.

[2] R. Dvornicich, U. Zannier, *Sums of roots of unity vanishing modulo a prime.* Arch. Math. **79** (2002), 104–108.

[3] D. Goss, *The arithmetic of function fields. II. The "cyclotomic" theory.* J. Alg. **81** (1) (1983), 107–149.

[4] D. Goss, *Basic structures of function field arithmetic.* Springer, 1996.

[5] D. R. Hayes, *Explicit class field theory for rational function fields.* Trans. Am. Math. Soc. **189** (2) (1974), 77–91.

[6] T. Y. Lam, K. H. Leung, *On Vanishing Sums of Roots of Unity.* J. Alg. **224** (2000), 91–109.

[7] J. Neukirch, *Algebraische Zahlentheorie.* Springer, 1992.

[8] M. Rosen, *Number Theory in Function Fields.* Springer GTM 210, 2000.

[9] J. P. Serre, *Corps Locaux.* Hermann, 1968.

[10] H. Weber, M. Künzer, *Some additive galois cohomology rings.* Arxiv math.NT/0102048, to appear in Comm. Alg., 2004.

Matthias Künzer
Universität Ulm
Abt. Reine Mathematik
D-89069 Ulm, Allemagne
E-mail : `kuenzer@mathematik.uni-ulm.de`

Eduard Wirsing
Universität Ulm
Fak. f. Mathematik
D-89069 Ulm, Allemagne
E-mail : `ewirsing@mathematik.uni-ulm.de`