JOURNAL DE THÉORIE DES NOMBRES DE BORDEAUX

NIGEL P. BYOTT

Associated orders of certain extensions arising from Lubin-Tate formal groups

Journal de Théorie des Nombres de Bordeaux, tome 9, n° 2 (1997), p. 449-462

<http://www.numdam.org/item?id=JTNB_1997__9_2_449_0>

Journal de Théorie des Nombres
de Bordeaux **9** (1997), 449–462

Associated Orders of Certain Extensions Arising from Lubin-Tate Formal Groups

par NIGEL P. BYOTT

RÉSUMÉ. Soit k une extension finie de $\mathbb{Q}_p$, k_1 et k_3 les corps de division de niveaux respectifs 1 et 3 associés à un groupe formel de Lubin-Tate, et soit $\Gamma = \mathrm{Gal}(k_3/k_1)$. On sait que si $k \neq \mathbb{Q}_p$ l'anneau de valuation de k_3 n'est pas libre sur son ordre associé $\mathfrak{A}$ dans $K\Gamma$. Nous explicitons $\mathfrak{A}$ dans le cas où l'indice absolu de ramification de k est assez grand.

ABSTRACT. Let k be a finite extension of $\mathbb{Q}_p$, let k_1, respectively k_3, be the division fields of level 1, respectively 3, arising from a Lubin-Tate formal group over k, and let $\Gamma = \mathrm{Gal}(k_3/k_1)$. It is known that the valuation ring k_3 cannot be free over its associated order $\mathfrak{A}$ in $K\Gamma$ unless $k = \mathbb{Q}_p$. We determine $\mathfrak{A}$ explicitly under the hypothesis that the absolute ramification index of k is sufficiently large.

1. INTRODUCTION

Let p be a prime number and let k be a finite extension of the p-adic field $\mathbb{Q}_p$. Let $\mathfrak{o}$ be the valuation ring of k, let π be a fixed generator of the maximal ideal in $\mathfrak{o}$, and let q be the cardinality of the residue field $\mathfrak{o}/\pi\mathfrak{o}$. Let $f(X) \in \mathfrak{o}[[X]]$ be a Lubin-Tate power series for k corresponding to π. By standard theory, as described for example in [S], there is a unique formal group F over $\mathfrak{o}$ with $f(X)$ as an endomorphism. For $n \geq 1$, the set G_n of zeros of the nth iterate of $f(X)$ is a group under F. The field k_n, obtained by adjoining to k the elements of G_n, is a totally ramified abelian extension of k with Galois group isomorphic to $(\mathfrak{o}/\pi^n\mathfrak{o})^\times$. We denote the valuation ring of k_n by $\mathfrak{o}_n$.

1991 *Mathematics Subject Classification.* 11S23, 11S31, 11R33.
Key words and phrases. Associated order, Lubin-Tate formal group.
Manuscrit reçu le 12 décembre 1996

This work was started while I was visiting the Institut für Mathematik, Karl-Franzens Universität, Graz, with financial support from the British Council (project number VIE/891/5). I would like to thank the Institut for their hospitality, and Günter Lettl for useful conversations.

Let r, $m \geq 1$ and let $\Gamma = \mathrm{Gal}(k_{m+r}/k_r)$. In the so-called Kummer case $m \leq r$, Taylor [T] determined the associated order of $\mathfrak{o}_{m+r}$ in the group algebra $k_r\Gamma$, and showed that $\mathfrak{o}_{m+r}$ is a free module over this order. In the non-Kummer case $m > r$, Chan and Lim [C-L] showed that $\mathfrak{o}_{m+r}$ is again free over its associated order if $k = \mathbb{Q}_p$. Subsequently Chan [C] gave an explicit description of this associated order. When $m > r$ and $k \neq \mathbb{Q}_p$, however, $\mathfrak{o}_{m+r}$ is not free over its associated order. This is proved in [B2] by an indirect argument which does not require explicit knowledge of the associated order.

The aim of this paper is to determine the associated order in a certain family of extensions of the above type. We consider only the case $r = 1$, $m = 2$, and we assume that the absolute ramification index e of k satisfies $e > q^2$. Under these hypotheses, the associated order admits a somewhat similar description to that of the order determined in [B1]. Although our hypotheses are rather restrictive, k may be chosen to make q arbitrarily large. If p is odd, the extension k_3/k_1 is elementary abelian of degree q^2. Our result therefore provides examples of elementary abelian extensions L/K of arbitrarily large even rank, in which the valuation ring of L is not free over its associated order, but for which this order is known explicitly.

The fields k_n depend only on π, and not on the Lubin-Tate power series $f(X)$. We are therefore free to make a convenient choice of $f(X)$. We take $f(X)$ to be the polynomial $X^q + \pi X$. The use of this particularly simple Lubin-Tate series, together with the hypothesis that e is sufficiently large, enables us to obtain strong congruences for the action of Γ on a basis of $\mathfrak{o}_3$. It is these congruences which permit us to determine the associated order.

2. Notation and Statement of the Main Result

We first establish some notation and recall some standard facts from the theory of Lubin-Tate formal groups. For proofs of these, see [S, §3]. The following notation is fixed for the rest of the paper:

k: a finite extension of $\mathbb{Q}_p$.

$\mathfrak{o}$: the valuation ring of k.

π: a fixed generator of the maximal ideal of $\mathfrak{o}$.

$q = p^f$: the cardinality of $\mathfrak{o}/\pi\mathfrak{o}$.

e: the absolute ramification index of k (so $\pi^e\mathfrak{o} = p\mathfrak{o}$).

μ: the $(q-1)$th roots of unity in k. (These form a cyclic group of order

$q-1$).

$f(X) = X^q + \pi X$, our chosen Lubin-Tate series.

$F(X,Y) \in \mathfrak{o}[[X,Y]]$: the formal group with f as an endomorphism.

$[a](X) \in \mathfrak{o}[[X]]$ (for each $a \in \mathfrak{o}$): the unique endomorphism of $F(X,Y)$ with $[a](X) \equiv aX \pmod{X^2\mathfrak{o}[[X]]}$.

The existence and uniqueness of $F(X,Y)$, and of $[a](X)$ for each a, are guaranteed by Lubin-Tate theory. In particular, it follows that $[\pi](X) = f(X)$, and that $[ab](X) = [a]([b](X))$ for all $a, b \in \mathfrak{o}$.

Let k^c be a fixed algebraic closure of k. For $n \geq 0$ let

$$G_n = \{x \in K^c \mid [\pi^n](x) = 0\}.$$

Then G_n is an $\mathfrak{o}$-module, where addition is given by F, and where $a \in \mathfrak{o}$ takes $x \in G_n$ to $[a](x)$.

For $n \geq 1$ let ω_n denote a fixed element of $G_n \backslash G_{n-1}$. In particular, we have $\omega_1^q + \pi\omega_1 = 0 \neq \omega_1$, so

$$\omega_1^{q-1} = -\pi. \tag{2.1}$$

For notational convenience, we assume that the ω_n are chosen so that $[\pi](\omega_{n+1}) = \omega_n$. Let $k_n = k(G_n)$, and let $\mathfrak{o}_n$ be its valuation ring. Then k_n/k is a totally ramified abelian extension, and ω_n generates the maximal ideal of $\mathfrak{o}_n$. The action of $\mathfrak{o}$ on G_n induces an isomorphism $\mathrm{Gal}(k_n/k) \cong (\mathfrak{o}/\pi^n\mathfrak{o})^\times$. Let $\langle a \rangle$ denote the element of $\mathrm{Gal}(k_n/k)$ corresponding to $a \in \mathfrak{o}$. Then $\langle a \rangle(x) = [a](x)$ for $x \in G_n$.

We will be concerned with the extension k_3/k_1. Set $\Gamma = \mathrm{Gal}(k_3/k_1)$. Then $\Gamma \cong (1+\pi\mathfrak{o})/(1+\pi^3\mathfrak{o})$. It follows that Γ is elementary abelian of order q^2 unless either $e = 1$ or $p = 2$. Let

$$\mathfrak{A} = \{\alpha \in k_1\Gamma \mid \alpha\mathfrak{o}_3 \subseteq \mathfrak{o}_3\},$$

the associated order of $\mathfrak{o}_3$ in the group algebra $k_1\Gamma$.

We next define some elements of $k_1\Gamma$ which will turn out to lie in $\mathfrak{A}$.

DEFINITION 2.2. For $1 \leq i \leq q-1$ let

$$\sigma_i = \frac{1}{(1-q)\pi}\sum_{\alpha\in\mu}(\langle\alpha\rangle(\omega_1))^{q-1-i}(\langle 1+\alpha\pi^2\rangle - \langle 1\rangle).$$

For $1 \leq h \leq q-1$ let

$$\tau_h = \frac{1}{(q-1)\omega_1^{q-1-h}} \sum_{\alpha\in\mu} (\langle\alpha\rangle(\omega_1))^{q-1-h}(\langle 1+\alpha\pi\rangle - \langle 1\rangle).$$

Also let $\sigma_0 = \tau_0 = 1$.

Remark. The σ_i are essentially the basis elements given by Taylor [T] for the associated order in the extension k_3/k_2, but with the numbering reversed.

We require certain numbers $a(h,i)$, related to the radix p expansions of h and i. For any integers $c \geq 0$ and $N \geq 1$, we write $(c \bmod N)$ for the least non-negative residue of c modulo N. Thus $0 \leq (c \bmod N) \leq N-1$ and $c - (c \mod N) \in N\mathbb{Z}$.

DEFINITION 2.3. Let $0 \leq h, i \leq q-1$.

If $(h \bmod p^{t+1}) + (i \bmod p^{t+1}) < p^{t+1}$ for all $t \in \{0, \dots, f-1\}$ (that is, if no carries occur in the radix p addition of h and i) define

$$a(h,i) = 0.$$

Otherwise, let $t \in \{0, \dots, f-1\}$ be maximal such that $(h \bmod p^{t+1}) + (i \bmod p^{t+1}) \geq p^{t+1}$. (Thus the "last" carry in the radix p addition of h and i is from the p^t-digit.) Then define

$$a(h,i) = (h \bmod p^{t+1}) + (i \bmod p^{t+1}) - p^{t+1} + 1 = (h+i+1 \bmod p^{t+1}).$$

We can now state our main result.

THEOREM 2.4. *If $e > q^2$ then the q^2 elements $(\omega_1^{-a(h,i)}\tau_h\sigma_i)_{0\leq h,i\leq q-1}$ of $k_1\Gamma$ form an $\mathfrak{o}_1$-basis of $\mathfrak{A}$.* □

3. THE FORMAL GROUP $F(X,Y)$

In this section we obtain some properties of $F(X,Y)$ which result from our choice of the special Lubin-Tate series $X^q + \pi X$ for $f(X)$.

PROPOSITION 3.1. *If $\alpha \in \mu$ then $[\alpha](X) = \alpha X$.*

Proof. We know from [S, §3, Proposition 2] that $[\alpha](X)$ is uniquely determined by the two conditions

$$[\alpha](X) \equiv \alpha X \pmod{X^2\mathfrak{o}[[X]]}, \qquad f([\alpha](X)) = [\alpha](f(X)).$$

Clearly αX satisfies the first of these, and, since $\alpha^q = \alpha$, it also satisfies the second: $f(\alpha X) = (\alpha X)^q + \pi(\alpha X) = \alpha(X^q + \pi X) = \alpha f(X)$. □

PROPOSITION 3.2.

$$F(X,Y) = X + Y + \sum_{r,s\geq 1} c_{r,s}X^rY^s \tag{3.3}$$

where the coefficients $c_{r,s} \in \mathfrak{o}$ *satisfy*

(i) $c_{r,s} = 0$ *if* $r + s \not\equiv 1 \pmod{q-1}$*;*

(ii) $c_{r,s} \equiv 0 \pmod{\pi\mathfrak{o}}$ *if* $r + s \leq (q-1)e$.

Proof. Any formal group can be written in the form (3.3) for some coefficients $c_{r,s}$. Let $\alpha \in \mu$ have order $q-1$. As $[\alpha](X)$ is an endomorphism, we have $F(\alpha X, \alpha Y) = \alpha F(X,Y)$ by Proposition 3.1. Equating coefficients of X^rY^s gives $\alpha^{r+s}c_{r,s} = \alpha c_{r,s}$, proving (i).

Now $f(X) = X^q + \pi X$ is also an endomorphism. Expanding the identity $f(F(X,Y)) = F(f(X), f(Y))$, reducing mod p, and subtracting the terms πX, πY, X^q, Y^q, we obtain

$$\begin{aligned} \pi\sum_{r,s} c_{r,s}X^rY^s + \sum_{r,s} c_{r,s}^q X^{qr}Y^{qs} \\ \equiv \sum_{r,s} c_{r,s}(\pi X + X^q)^r(\pi Y + Y^q)^s \pmod{p\mathfrak{o}[[X,Y]]}. \end{aligned} \tag{3.4}$$

We will show by induction on j in the range $1 \leq j \leq e-1$ that

$$\text{if } r + s = 1 + (q-1)j \text{ then } c_{r,s} \equiv 0 \pmod{\pi^{e-j}\mathfrak{o}}. \tag{3.5}$$

Indeed, for any r', s' with $r' + s' < 1 + (q-1)j$ we have $c_{r',s'} \equiv 0 \pmod{\pi^{e-j+1}\mathfrak{o}}$ by (i) and the induction hypothesis. Thus, if $r + s = 1 + (q-1)j$, equating coefficients of X^rY^s in (3.4) gives

$$\pi c_{r,s} \equiv \pi^{r+s}c_{r,s} \pmod{\pi^{e-j+1}\mathfrak{o}}.$$

Hence $(1 - \pi^{r+s-1})c_{r,s} \equiv 0 \pmod{\pi^{e-j}\mathfrak{o}}$. Since $1 - \pi^{r+s-1}$ is a unit in $\mathfrak{o}$, this completes the induction. Statement (ii) now follows from (3.5) and (i). □

We adopt the convention that the binomial coefficient $\binom{j}{s}$ is to be interpreted as 0 if $s > j$. As an immediate consequence of Proposition 3.2, we have

COROLLARY 3.6. *For $j \geq 0$,*

$$F(X,Y)^j - X^j = \sum_{s\geq 1} \binom{j}{s} X^{j-s}Y^s + \sum_{r,s\geq 1} b_{r,s}X^rY^s$$

where the coefficients $b_{r,s} \in \mathfrak{o}$ (depending on j) satisfy

(3.7) $\qquad b_{r,s} = 0 \qquad$ *if* $r+s < j+q-1$;

(3.8) $\qquad b_{r,s} \equiv 0 \pmod{\pi\mathfrak{o}} \qquad$ *if* $r+s < j+(q-1)e$.

□

For $N > n \geq 1$, let $\mathrm{Tr}_{N,n}$ denote the trace from k_N to k_n. The following result was pointed out to me by Günter Lettl.

PROPOSITION 3.9.

$$\mathrm{Tr}_{n+1,n}(\omega_{n+1}^j) = \begin{cases} q & \text{if } j=0; \\ 0 & \text{if } 1 \leq j \leq q-2; \\ (1-q)\pi & \text{if } j = q-1. \end{cases}$$

Proof. If $x_1, \dots, x_m$ are the zeros of a monic polynomial $X^m + \sum_{r=0}^{m-1} a_r X^r$ of degree m, then for $1 \leq j \leq m$, one can express $\sum_i x_i^j$ as a polynomial in $a_{m-1}, \dots, a_{m-j}$ with no constant term. Applying this to the minimal polynomial $X^q + \pi X - \omega_n$ of ω_{n+1} over k_n, we find immediately that $\mathrm{Tr}_{n+1,n}(\omega_{n+1}^j) = 0$ for $1 \leq j \leq q-2$. Clearly $\mathrm{Tr}_{n+1,n}(\omega_{n+1}^0) = \mathrm{Tr}_{n+1,n}(1) = q$, so it remains to consider the case $j = q-1$.

Let $y = \omega_n \omega_{n+1}^{-1}$. Multiplying the equation $\omega_{n+1}^q + \pi\omega_{n+1} - \omega_n = 0$ by $\omega_n^{q-1}\omega_{n+1}^{-q}$, we obtain $\omega_n^{q-1} + \pi y^{q-1} - y^q = 0$. Since $k_n(y) = k_{n+1}$, it follows that $\mathrm{Tr}_{n+1,n}(y) = \pi$. Thus $\mathrm{Tr}_{n+1,n}(\omega_{n+1}^{q-1}) = \mathrm{Tr}_{n+1,n}(y - \pi) = \pi - q\pi$ as required. □

COROLLARY 3.10. *If $q \equiv 0 \pmod{\pi^3\mathfrak{o}}$ then for $0 \leq r \leq q-2$ we have*

$$\tau_{q-1}\sigma_{q-1}(\omega_3^{rq+q-1}) \equiv 0 \pmod{\pi^2\mathfrak{o}}.$$

Proof. As $\omega_3^q + \pi\omega_3 = \omega_2$, we have

$$\omega_3^{rq+q-1} = (\omega_2 - \pi\omega_3)^r \omega_3^{q-1} \equiv \omega_2^r \omega_3^{q-1} \pmod{\pi\mathfrak{o}_3}.$$

Now $\mathrm{Tr}_{n+1,n}(\mathfrak{o}_{n+1}) \subseteq \pi\mathfrak{o}_n$ by Proposition 3.9, so

$$\mathrm{Tr}_{3,2}(\omega_3^{rq+q-1}) \equiv \omega_2^r \mathrm{Tr}_{3,2}(\omega_3^{q-1}) \pmod{\pi^2\mathfrak{o}_2}.$$

Applying Proposition 3.9 again, we therefore have

$$\mathrm{Tr}_{3,2}(\omega_3^{rq+q-1}) \equiv \omega_2^r(1-q)\pi \pmod{\pi^2\mathfrak{o}_2},$$

and yet another application of Proposition 3.9 gives

$$\mathrm{Tr}_{3,1}(\omega_3^{rq+q-1}) \equiv (1-q)\pi\mathrm{Tr}_{2,1}(\omega_2^r) = 0 \pmod{\pi^3\mathfrak{o}_1}. \tag{3.11}$$

As $\mathrm{Gal}(k_3/k_2)$ consists of the automorphisms $\langle 1+\alpha\pi^2\rangle$ for $\alpha \in \mu \cup \{0\}$, we have

$$\begin{aligned}(1-q)\pi\sigma_{q-1}(\omega_3^{rq+q-1}) &= \sum_{\alpha\in\mu}\Big(\langle 1+\alpha\pi^2\rangle(\omega_3^{rq+q-1}) - \omega_3^{rq+q-1}\Big)\\ &= \mathrm{Tr}_{3,2}(\omega_3^{rq+q-1}) - q\omega_3^{rq+q-1}\end{aligned}$$

and hence

$$\pi\sigma_{q-1}(\omega_3^{rq+q-1}) \equiv \mathrm{Tr}_{3,2}(\omega_3^{rq+q-1}) \pmod{q\mathfrak{o}_3}. \tag{3.12}$$

Similarly, $(q-1)\tau_{q-1} = \sum_\alpha(\langle 1+\alpha\pi\rangle - \langle 1\rangle)$, and this acts on k_2 as $(\mathrm{Tr}_{2,1} - q)$. Since $\tau_{q-1}(q\mathfrak{o}_3) \subseteq q\mathfrak{o}_3$, we have from (3.12) that

$$-\pi\tau_{q-1}\sigma_{q-1}(\omega_3^{rq+q-1}) \equiv \mathrm{Tr}_{3,1}(\omega_3^{rq+q-1}) \pmod{q\mathfrak{o}_3}.$$

As $q\pi^{-1} \equiv 0 \pmod{\pi^2\mathfrak{o}}$, the result now follows from (3.11). □

4. Galois action congruences

From now on, we assume that $e > q^2$. Let $v\colon k_3 \to \mathbb{Z} \cup \{-\infty\}$ denote the additive valuation, normalised so that $v(\omega_3) = 1$. Thus $v(\omega_2) = q$, $v(\omega_1) = q^2$ and $v(\pi) = (q-1)q^2$.

Lemma 4.1.

Let $0 \le i \le q-1$. Then, for $j \ge 0$,

$$\sigma_i(\omega_3^j) \equiv \binom{j}{i}\omega_3^{j-i} \pmod{\pi\mathfrak{o}_3}. \tag{4.2}$$

In particular, $\sigma_i(\mathfrak{o}_3) \subseteq \mathfrak{o}_3$*, and* $v(\sigma_i(x)) \geq v(x) - i$ *for all* $x \in k_3$.

Proof. If $i = 0$ then $\sigma_i = 1$ and (4.2) is clear. Now let $i \geq 1$. From Definition 2.2 and Proposition 3.1 we have

$$(4.3) \qquad (1-q)\pi\sigma(\omega_3^j) = \sum_{\alpha\in\mu}(\alpha\omega_1)^{q-1-i}\Big(\langle 1+\alpha\pi^2\rangle(\omega_3^j) - \omega_3^j\Big).$$

Now $\langle 1+\alpha\pi^2\rangle(\omega_3^j) = ([1+\alpha\pi^2](\omega_3))^j$. (Note that this is *not* the same as $[1+\alpha\pi^2](\omega_3^j)$.) As G_3 is an $\mathfrak{o}$-module, we calculate

$$[1+\alpha\pi^2](\omega_3) = F(\omega_3, [\alpha\pi^2](\omega_3)) = F(\omega_3, [\alpha](\omega_1)) = F(\omega_3, \alpha\omega_1),$$

again using Proposition 3.1. Thus

$$\langle 1+\alpha\pi^2\rangle(\omega_3^j) - \omega_3^j = \sum_{s\geq 1}\binom{j}{s}\omega_3^{j-s}\alpha^s\omega_1^s + \sum_{r,s\geq 1} b_{r,s}\omega_3^r\alpha^s\omega_1^s,$$

with coefficients $b_{r,s} \in \mathfrak{o}$ as in Corollary 3.6. Substituting into (4.3) and reversing the order of summation, we have

$$(1-q)\pi\sigma(\omega_3^j) =$$

$$\sum_{s\geq 1}\binom{j}{s}\omega_3^{j-s}\omega_1^{q-1-i+s}\sum_{\alpha}\alpha^{q-1-i+s} + \sum_{r,s\geq 1} b_{r,s}\omega_3^r\omega_1^{q-1-i+s}\sum_{\alpha}\alpha^{q-1-i+s}.$$

This simplifies to

$$(4.4) \quad \sigma_i(\omega_3^j) = \sum_{\substack{s\geq 1\\ s\equiv i \pmod{q-1}}}\binom{j}{s}\omega_3^{j-s}\omega_1^{s-i} + \sum_{\substack{r,s\geq 1\\ s\equiv i \pmod{q-1}}} b_{r,s}\omega_3^r\omega_1^{s-i},$$

using (2.1) and the fact that

$$\sum_{\alpha\in\mu}\alpha^t = \begin{cases} q-1 & \text{if } t\equiv 0 \pmod{q-1};\\ 0 & \text{otherwise.}\end{cases}$$

The terms in the first sum of (4.4) with $s \neq i$ are divisible by $\omega_1^{q-1} = -\pi$. To evaluate $\sigma_i(\omega_3^j) \bmod \pi\mathfrak{o}_3$, we may therefore replace this sum by the single term with $s = i$. This applies even when $i > j$, since then the binomial coefficient vanishes. To prove (4.2) we must therefore show that the second sum in (4.4) vanishes mod $\pi\mathfrak{o}_3$. But by (3.8), $b_{r,s} \equiv 0 \pmod{\pi\mathfrak{o}}$ when $r+s < j+(q-1)e$, and for the remaining terms we have $v(\omega_3^r\omega_1^{s-i}) \geq r+s-i \geq (q-1)(e-1) \geq v(\pi)$ since $e \geq q^2+1$ by hypothesis. This completes the proof of (4.2), and the remaining statements of the Lemma follow since $(\omega_3^j)_{0\leq j\leq q^2-1}$ is an $\mathfrak{o}_1$-basis for $\mathfrak{o}_3$. $\square$

LEMMA 4.5. *Let* $1 \leq h \leq q-1$. *Then, for* $j \geq 0$,

$$\tau_h(\omega_3^j) \equiv \sum_{\substack{s \geq 1 \\ s \equiv h \pmod{q-1}}} \binom{j}{s} \omega_3^{j-s} \omega_2^s \pmod{\pi \omega_3^{j+(q-1)(h+1)} \mathfrak{o}_3}. \tag{4.6}$$

In particular, $\tau_h(\mathfrak{o}_3) \subseteq \mathfrak{o}_3$, *and* $v(\tau_h(x)) \geq v(x) + (q-1)h$ *for all* $x \in k_3$.

Proof. Calculating as in the proof of Lemma 4.1, but this time using that

$$[1 + \alpha\pi](\omega_3) = F(\omega_3, \alpha\omega_2),$$

we obtain

$$\tau_h(\omega_3^j) = \sum_{\substack{s \geq 1 \\ s \equiv h \pmod{q-1}}} \binom{j}{s} \omega_3^{j-s} \omega_2^s + \sum_{\substack{r,s \geq 1 \\ s \equiv h \pmod{q-1}}} b_{r,s} \omega_3^r \omega_2^s, \tag{4.7}$$

where again the coefficients $b_{r,s}$ are as in Corollary 3.6. In the second sum, all non-zero terms have $r + s \geq j + q - 1$ by (3.7). If $b_{r,s} \equiv 0 \pmod{\pi\mathfrak{o}}$ then

$$\begin{aligned} v(b_{r,s}\omega_3^r\omega_2^s) &\geq v(\pi) + r + qs \\ &\geq v(\pi) + (j + q - 1) + (q-1)s \\ &\geq v(\pi) + j + (q-1)(h+1) \end{aligned}$$

since $s \geq h$. On the other hand, if $b_{r,s} \not\equiv 0 \pmod{\pi\mathfrak{o}}$ then $r+s \geq j+(q-1)e$ by (3.8), and

$$\begin{aligned} v(b_{r,s}\omega_3^r\omega_2^s) &\geq j + (q-1)e + (q-1)s \\ &\geq j + (q-1)(e-1) + (q-1)(h+1) \\ &\geq j + v(\pi) + (q-1)(h+1) \end{aligned}$$

since $v(\pi) = (q-1)q^2$ and $e \geq q^2+1$. Thus the second sum in (4.7) vanishes mod $\pi\omega_3^{j+(q-1)(h+1)}\mathfrak{o}_3$. This proves (4.6). The remaining statements follow since $(\omega_3^j)_{0 \leq j \leq q^2-1}$ is an $\mathfrak{o}_1$-basis of $\mathfrak{o}_3$. □

LEMMA 4.8. *Let* $0 \leq i \leq q-1$ *and* $1 \leq h \leq q-1$. *Then, for* $j \geq 0$,

(4.9)

$$\tau_h\sigma_i(\omega_3^j) \equiv \sum_{\substack{s \geq 1 \\ s \equiv h \pmod{q-1}}} \binom{j}{i+s} \binom{i+s}{s} \omega_3^{j-i-s} \omega_2^s \pmod{\pi \omega_3^{(q-1)h} \mathfrak{o}_3}.$$

In particular, $\tau_h\sigma_i(\mathfrak{o}_3) \subseteq \mathfrak{o}_3$.

Proof. By the last assertion of Lemma 4.5 we have

$$\tau_h(\pi\mathfrak{o}_3) \subseteq \pi\omega_3^{(q-1)h}\mathfrak{o}_3.$$

We may therefore apply (4.6) (with $j-i$ in place of j) to (4.2), obtaining

$$\tau_h\sigma_i(\omega_3^j) \equiv \binom{j}{i} \sum_{\substack{s\geq 1,\\ s\equiv h \pmod{q-1}}} \binom{j-i}{s}\omega_3^{j-i-s}\omega_2^s \pmod{\pi\omega_3^{(q-1)h}\mathfrak{o}_3}.$$

Since $\binom{j}{i}\binom{j-i}{s} = \binom{j}{i+s}\binom{i+s}{s}$, this gives the congruence (4.9). The final assertion is then clear. □

5. BINOMIAL COEFFICIENTS AND THE NUMBERS $a(h,i)$

We shall need to know when the binomial coefficients $\binom{i+s}{s}$ in (4.9) are divisible by p. It is this which accounts for the appearance of the numbers $a(h,i)$ of Definition 2.3 in the description of the associated order.

By a result of Kummer (see for instance [R, p. 24]), the exact power of p dividing $\binom{i+s}{s}$ is given by the number of carries occurring in the radix p addition of i and s. In particular, $\binom{i+s}{s} \not\equiv 0 \pmod p$ precisely when no carries occur. Thus, writing

$$i = \sum_{t\geq 0} p^t i_t, \qquad 0 \leq i_t \leq p-1, \tag{5.1}$$

and adopting similar notation for s, we have that $\binom{i+s}{s} \not\equiv 0 \pmod p$ if and only if $i_t + s_t < p$ for all t, or equivalently, if and only if $(i \bmod p^{t+1}) + (s \bmod p^{t+1}) < p^{t+1}$ for all t.

LEMMA 5.2. *Let* $0 \leq h, i \leq q-1$. *Then the smallest integer* $s \geq h$ *satisfying the two conditions*

$$s \equiv h \pmod{q-1}, \qquad \binom{i+s}{s} \not\equiv 0 \pmod p$$

is given by $s = h + (q-1)a(h,i)$.

Proof. Set $s = h + (q-1)a$ with $a \geq 0$. We will show that $a(h,i)$ is the minimal value of a for which $\binom{i+s}{s} \not\equiv 0 \pmod p$.

If no carries occur in the radix p addition of h and i then $\binom{i+h}{h} \not\equiv 0 \pmod{p}$, and also $a(h,i) = 0$. The Lemma therefore holds in this case.

Now suppose that at least one carry occurs in the addition of h and i. Expand i, h and s in radix p, as in (5.1). Then $i_t = h_t = 0$ for $t \geq f$. Let $t \in \{0, \ldots, f-1\}$ be maximal such that $(h \bmod p^{t+1}) + (i \bmod p^{t+1}) \geq p^{t+1}$. We then have $a(h,i) = (h \bmod p^{t+1}) + (i \bmod p^{t+1}) - p^{t+1} + 1$. Clearly $a(h,i) \leq (h \bmod p^{t+1})$, so if $a \leq a(h,i)$ we have $(s \bmod p^{t+1}) = (h - a \bmod p^{t+1}) = (h \bmod p^{t+1}) - a$.

If $a < a(h,i)$ then

$$(i \bmod p^{t+1}) + (s \bmod p^{t+1}) > (i \bmod p^{t+1}) + (h \bmod p^{t+1}) - a(h,i)$$
$$= p^{t+1} - 1.$$

Thus, in the radix p addition of i and s, a carry occurs from the p^t-digit, and hence $\binom{i+s}{s}$ is divisible by p.

It remains to show that if $a = a(h,i)$ then no carries occur in the radix p addition of s and i. In this case we have

$$(i \bmod p^{t+1}) + (s \bmod p^{t+1}) = p^{t+1} - 1.$$

This implies that there is no carry from the $p^{t'}$-digit for any $t' \leq t$. (Indeed, if t' were minimal such that there is a carry from the $p^{t'}$-digit then $i_{t'} + s_{t'} \geq p$ and $i_{t'} + s_{t'} \equiv p - 1 \pmod{p}$, which is impossible as $0 \leq i_{t'}, s_{t'} \leq p-1$.) Since $a(h,i) \leq (h \bmod p^{t+1})$ and $s = qa + h - a$, we have $s_{t'} = h_{t'}$ if $t < t' < f$, and by the maximality of t there can be no carry from the $p^{t'}$-digit. As $i_{t'} = 0$ for $t' \geq f$, this completes the proof. □

The next result records some further properties of the $a(h,i)$. These are all immediate from Definition 2.3.

PROPOSITION 5.3.

(i) $0 \leq a(h,i) \leq \min(h,i) \leq q-1$. *In particular,* $a(h,0) = a(0,i) = 0$.
(ii) $a(q-1,1) = 1$.
(iii) $0 \leq i + h - a(h,i) \leq q-1$. □

6. PROOF OF THEOREM 2.4

Theorem 2.4 will be proved by a similar method to [B1].

We first show that

(6.1) $$\tau_h \sigma_i(\omega_3^j) \in \omega_1^{a(h,i)} \mathfrak{o}_3 \qquad \text{for } 0 \leq h, i \leq q-1 \text{ and } j \geq 0.$$

For $h = 0$, this is clear from Lemma 4.1. For $h \geq 1$ we use Lemma 4.8. By Lemma 5.2, the term $\binom{j}{i+s}\binom{i+s}{s}\omega_3^{j-i-s}\omega_2^s$ in the sum on the right of (4.9) vanishes mod p if $s < h+(q-1)a(h,i)$. This term also vanishes if $j < i+s$, and for the remaining terms we have

$$v(\omega_3^{j-i-s}\omega_2^s) \geq qs \geq qh + q(q-1)a(h,i) \geq q^2 a(h,i) = v(w_1^{a(h,i)})$$

since $a(h,i) \leq h$ by Proposition 5.3(i). Since $\pi\omega_3^{(q-1)h}\mathfrak{o}_3 \subseteq \omega_1^{a(h,i)}\mathfrak{o}_3$ and $p \in \omega_1^{a(h,i)}\mathfrak{o}_3$, this implies (6.1).

It is clear from (6.1) that the elements $(\omega_1^{-a(h,i)}\tau_h\sigma_i)_{0\leq h,i\leq q-1}$ lie in the associated order $\mathfrak{A}$. By Nakayama's Lemma, they will span $\mathfrak{A}$ over $\mathfrak{o}_1$, provided that their images span $\mathfrak{A}/\omega_1\mathfrak{A}$ over the residue field $\mathfrak{o}_1/\omega_1\mathfrak{o}_1$. Counting dimensions, this will occur if these images are linearly independent. It is therefore sufficient to prove the following: if we are given

$$\xi = \sum_{h,i} x_{h,i}\omega_1^{-a(h,i)}\tau_h\sigma_i \in \mathfrak{A}, \qquad x_{h,i} \in \mathfrak{o}_1, \tag{6.2}$$

with the property that

$$\xi(\omega_3^j) \in \omega_1\mathfrak{o}_3 \quad \text{for each } j \geq 0, \tag{6.3}$$

then each coefficient $x_{h,i}$ must lie in $\omega_1\mathfrak{o}_1$.

We will show by induction on r in the range $0 \leq r \leq q-1$ that, if ξ satisfies (6.3), then $x_{h,i} \in \omega_1\mathfrak{o}_1$ for each pair (h,i) with $a(h,i) = r$. This will complete the proof of the Theorem.

From Lemma 4.8,

$$\tau_h\sigma_i(\omega_3^j) \equiv \sum_{\substack{s\geq 1 \\ s\equiv h \pmod{q-1}}} \binom{j}{i+s}\binom{i+s}{s}\omega_3^{j-i-s}\omega_2^s \pmod{\pi\omega_3^{(q-1)h}\mathfrak{o}_3}$$

for all $j \geq 0$, provided that $h \geq 1$. We take $j = rq + q - 1$.

First consider pairs (h,i) with $a(h,i) \geq r+1$. (For these, $h \geq 1$ since $a(0,i) = 0$.) For such pairs, $i + h - (r+1) \geq 0$ by Proposition 5.3(iii), so $i + h + (r+1)(q-1) \geq (r+1)q > j$. Thus, in each term of the above sum, we have $s \leq j - i < h + (r+1)(q-1)$, and these terms vanish mod p by Lemma 5.2. We have therefore shown that $\omega_1^{-a(h,i)}\tau_h\sigma_i(\omega_3^{rq+q-1}) \equiv 0$ (mod $\pi\omega_1^{-a(h,i)}\mathfrak{o}_3$) if $a(h,i) \geq r+1$, and hence that $\omega_1^{-a(h,i)}\tau_h\sigma_i(\omega_3^{rq+q-1}) \equiv$

$0 \pmod{\omega_1 \mathfrak{o}_3}$ if $a(h,i) \geq r+1$ and $a(h,i) \neq q-1$. But in the excluded case $a(h,i) = q-1 > r$ we have $h = i = q-1$, so $\omega_1^{-(q-1)} \tau_{q-1}\sigma_{q-1}(\omega_3^{rq+q-1}) \equiv 0 \pmod{\pi \mathfrak{o}_3}$ by Corollary 3.10. Thus, in either case, we have

$$\omega_1^{-a(h,i)} \tau_h \sigma_i(\omega_3^{rq+q-1}) \equiv 0 \pmod{\omega_1 \mathfrak{o}_3} \qquad \text{if } a(h,i) \geq r+1. \tag{6.4}$$

Next consider pairs (h,i) with $r = a(h,i)$. For any such pair with $h \neq 0$, the above argument shows that all terms in (4.9) vanish mod p except possibly that with $s = h + (q-1)r$. Thus

$$\omega_1^{-a(h,i)} \tau_h \sigma_i(\omega_3^{rq+q-1}) \equiv \binom{rq+q-1}{i+h+(q-1)r} \binom{i+h+(q-1)r}{h+(q-1)r} \times \\ \omega_3^{rq+q-1-i-h-(q-1)r} \omega_2^{h+(q-1)r} \omega_1^{-a(h,i)} \pmod{\pi \omega_3^{(q-1)h} \omega_1^{-a(h,i)} \mathfrak{o}_3}.$$

By Lemma 4.1, this is still valid when $h = 0$ (so $r = a(h,i) = 0$). The second binomial coefficient is a unit mod p by Lemma 5.2. The first binomial coefficient is also a unit mod p; this is because no carries can occur in the radix p addition of $q-1-(h+i-r)$ to $rq + (h+i-r)$. (We have $0 \leq h+i-r \leq q-1$ by Proposition 5.3(iii).) Thus, for all pairs (h,i) with $a(h,i) = r$, it follows that

$$\begin{aligned} v(\omega_1^{-a(h,i)} \tau_h \sigma_i(\omega_3^{rq+q-1})) &= (rq+q-1-i-h-(q-1)r) \\ &\quad + (h+(q-1)r)q - q^2 r \\ &= (q-1)(1+h-r) - i, \end{aligned} \tag{6.5}$$

provided that

$$(q-1)(1+h-r) - i < v(\pi \omega_3^{(q-1)h} \omega_1^{-a(h,i)}) = q^2(q-1-r) + (q-1)h.$$

This condition is clearly satisfied if $r < q-1$, since $(q-1)(1+h-r) < q^2$, and is also satisfied when $r = q-1$ since then $h = i = q-1$. Thus (6.5) holds whenever $a(h,i) = r$.

Recall that ξ is given by (6.2) and satisfies (6.3). Our induction hypothesis is that $x_{h,i} \in \omega_1 \mathfrak{o}_1$ when $a(h,i) < r$. It follows from (6.4) and (6.3) that

$$\xi(\omega_3^{rq+q-1}) \equiv \sum_{a(h,i)=r} x_{h,i} \omega_1^{-a(h,i)} \tau_h \sigma_i(\omega_3^{rq+q-1}) \equiv 0 \pmod{\omega_1 \mathfrak{o}_3}. \tag{6.6}$$

Let (h,i) be any pair with $a(h,i) = r$ and $x_{h,i} \notin \omega_1 \mathfrak{o}_1$. Then by (6.5), the corresponding term in (6.6) has valuation $(q-1)(1+h-r)-i$. This is at most $(q-1)q$. Moreover, it is easily verified that if $(q-1)(1+h-r)-i = (q-1)(1+h'-r)-i'$ with $a(h,i) = r = a(h',i')$ then $(h,i) = (h',i')$, Thus the terms in (6.6) with $x_{h,i} \notin \omega_1 \mathfrak{o}_1$ have distinct valuations, all less than $v(\omega_1) = q^2$. Since a non-empty sum of such terms cannot vanish mod $\omega_1 \mathfrak{o}_3$, it follows that $x_{h,i} \in \omega_1 \mathfrak{o}_1$ for all pairs (h,i) with $a(h,i) = r$. This completes the induction. □

REFERENCES

[B1] N. P. Byott, *Some self-dual rings of integers not free over their associated orders*, Math. Proc. Camb. Phil. Soc. **110** (1991), 5–10; Corrigendum, **116** (1994), 569.

[B2] N. P. Byott, *Galois structure of ideals in wildly ramified abelian p-extensions of a p-adic field, and some applications*, J. de Théorie des Nombres de Bordeaux **9** (1997), 201–219.

[C] S.-P. Chan, *Galois module structure of non-Kummer extensions*, Preprint, National University of Singapore (1995).

[C-L] S.-P. Chan and C.-H. Lim, *The associated orders of rings of integers in Lubin-Tate division fields over the p-adic number field*, Ill. J. Math. **39** (1995), 30–38.

[R] P. Ribenboim, *The Book of Prime Number Records*, 2nd edition, Springer, 1989.

[S] J.-P. Serre, *Local Class Field Theory*, in Algebraic Number Theory (J.W.S. Cassels and A. Fröhlich, eds.), Academic Press, 1967.

[T] M. J. Taylor, *Formal groups and the Galois module structure of local rings of integers*, J. reine angew. Math. **358** (1985), 97–103.

Nigel P. BYOTT
Department of Mathematics
University of Exeter
North Park Road
Exeter EX4 4QE
UK
email: NPByott@maths.exeter.ac.uk