ILLINOIS JOURNAL OF MATHEMATICS
Volume 39, Number 1, Spring 1995

THE ASSOCIATED ORDERS OF RINGS OF INTEGERS IN LUBIN-TATE DIVISION FIELDS OVER THE p-ADIC NUMBER FIELD

SHIH-PING CHAN AND CHONG-HAI LIM

1. Introduction

Let p be a prime number and let $\mathbf{Q}_p$ denote the p-adic number field. The main aim of this article is to describe the associated orders of relative extensions of Lubin-Tate division fields over $\mathbf{Q}_p$. Let L/K be a Galois extension of number fields with Galois group $\Gamma = \mathrm{Gal}(L/K)$. If L is a global field, let $\mathfrak{O}_L$ denote the ring of integers in L. If L is a local field, we denote the valuation ring of L by $\mathfrak{O}_L$. We recall that the associated order of the extension L/K is the subset

$$\mathfrak{A}_{L/K} = \{\lambda \in K[\Gamma] | \lambda \mathfrak{O}_L \subseteq \mathfrak{O}_L\}$$

of the group ring $K[\Gamma]$. It is indeed an order in $K[\Gamma]$, containing $\mathfrak{O}_K[\Gamma]$.

Currently, the associated order has been calculated in the following general situations:

(a) K/k is a tamely ramified extension ([7]),
(b) K is an absolutely abelian extension of $k = \mathbf{Q}$ [5],
(c) (almost) maximally ramified Kummer extensions [2],
(d) Kummer extensions of cyclotomic extensions of $\mathbf{Q}$ and some complex multiplication analogues [[8]),
(e) 'Kummer' extensions of Lubin-Tate division fields [9].
(f) Relative cyclotomic extensions in both the local and global situations ([1]).

Let $\mathbf{Q}_{p,\pi}^n$ be the division field of level n and uniformizer π associated to some Lubin-Tate formal group, and let $\mathfrak{O}_\pi^n$ denote its valuation ring. The recent work of (f) above, makes it possible to calculate the associated order of $\mathfrak{O}_\pi^{m+r}$ in the extension $\mathbf{Q}_{p,\pi}^{m+r}/\mathbf{Q}_{p,\pi}^r$. Here p is any prime, r, $m \in \mathbf{Z}$ and $1 \le r, m$ if $p \ge 3$ and $2 \le r$, $1 \le m$ if $p = 2$. Because of the dependence on [1], we are restricted to using $\mathbf{Q}_p$ as base field. However, this represents an advance on [9] as we are no longer restricted by the 'Kummer' requirement. The results in this article and [1] are, as far as the authors are aware of, the

Received September 1, 1992.
1991 Mathematics Subject Classification. 11R33.

first which give explicit Galois Module Structure information in non-'Kummer' situations.

Our main result is stated in the final section. Briefly, by adjoining an unramified extension to $\mathbf{Q}_{p,\pi}^{r}$ we obtain a relative cyclotomic situation. We may then apply some of the ideas of [1], and with suitable modifications, obtain the associated order and a Galois generator. By 'descending' to the base field $\mathbf{Q}_p$, we can then determine the associated order in the relative Lubin-Tate situation.

This work represents one of the rare situations where the associated order can be determined independently of finding a Galois generator.

This paper is organised as follows:

§1. Introduction
§2. Review of Lubin-Tate theory
§3. The cyclotomic case
§4. Definitions and notation
§5. The descent lemma
§6. The main theorem

2. Review of Lubin-Tate theory

Let k be a local field in characteristic 0, i.e., a p-adic field. Let $\pi \in k$ be a uniformizer and let q be the cardinality of the residue class field.

Let $\mathfrak{O}_k$ denote the valuation ring of k. Let $\bar{k}$ denote a fixed algebraic closure of k. Let f be a Lubin-Tate power series associated to the uniformizer π, i.e.,

$$f(X) \equiv \pi X \pmod{\deg 2},$$
$$f(X) \equiv X^q \pmod{\pi}.$$

The roots of f^n will be denoted by W_f^n. The division field of level n and uniformizer π is the field obtained by adjoining W_f^n to k. It is well known that this is a totally ramified abelian extension of k, depending only on n and π.

We use F_f to denote the unique formal group defined over $\mathfrak{O}_k$ which admits f as an endomorphism. In the case $k = \mathbf{Q}_p$ and $\pi = p$, we may take

$$f(X) = (1+X)^p - 1,$$

in which case

$$W_f^n = \left\{\zeta_{p^n}^l - 1 \mid l \in \mathbf{Z}\right\}$$

and $\mathbf{Q}_{p,\pi}^n = \mathbf{Q}(\zeta_{p^n})$. It is standard that we have an $\mathfrak{O}_k$-module structure on the maximal ideal of the valuation ring of $\bar{k}$. In particular, the W_f^n are $\mathfrak{O}_k$-sub-modules.

Let $\bar{k}_{\mathrm{ur}}$ be the completion of the maximal unramified extension of k and let $\bar{\mathfrak{O}}_{\mathrm{ur}}$ be its valuation ring. Given two Lubin-Tate power series (possibly associated to different uniformizers) over $\mathfrak{O}_k$, by standard Lubin-Tate theory there is a unique power series defined over $\bar{\mathfrak{O}}_{\mathrm{ur}}$, $\theta_{f,g}$, which is an isomorphism of formal groups

$$\theta_{f,g}\colon F_f \to F_g .$$

In particular, we have a module isomorphism

$$\theta_{f,g}\colon W_f^n \to W_g^n,\ \xi \to \theta_{f,g}(\xi) \quad (n \geq 1).$$

Observe that $\theta(\pi)$ is the uniformizer associated with g. For details, the reader may consult [4] or [6].

3. The Cyclotomic Case

We give a brief review of the local cyclotomic case which motivates much of what follows. Let p be a rational prime, and let $m, r \in \mathbf{Z}$ with

(i) $1 \leq r, m$ if $p \geq 3$, while
(ii) $2 \leq r$, $1 \leq m$ if $p = 2$.

Let $n = m + r$. We denote by ζ a primitive p^n-th root of unity in an algebraic closure $\overline{\mathbf{Q}}_p$ of $\mathbf{Q}_p$.

DEFINITION 3.1. Let

$$\zeta_{p^k} \overset{\mathrm{def}}{=} \zeta^{p^{n-k}} \quad (0 \leq k \leq n),$$

so that ζ_{p^k} is a primitive p^k-th root of unity.

Let Γ denote the Galois group of the extension $\mathbf{Q}_p(\zeta)/\mathbf{Q}_p(\zeta_{p^r})$.

DEFINITION 3.2. For $r < k \leq n$, let

$$s(k) \overset{\mathrm{def}}{=} \min(k - r, r).$$

For $r < k \leq n$, let

$$t(k) \overset{\mathrm{def}}{=} \max(0, k - 2r).$$

DEFINITION 3.3. For $r < k \le m$, let T_k denote the trace element in $\mathbf{Q}_p(\zeta_{p^r})[\Gamma]$ of the extension $\mathbf{Q}_p(\zeta)/\mathbf{Q}_p(\zeta_{p^k})$ by

$$T_k \stackrel{\text{def}}{=} \mathrm{Tr}_{\mathbf{Q}_p(\zeta)/\mathbf{Q}_p(\zeta_{p^k})}.$$

DEFINITION 3.4. We define the idempotents $E_r, \ldots, E_n$ in $\mathbf{Q}_p(\zeta_{p^r})[\Gamma]$ as follows:

(a)
$$E_r \stackrel{\text{def}}{=} \frac{1}{p^m} T_r.$$

(b)
$$E_k \stackrel{\text{def}}{=} \frac{1}{p^{n-k}} T_k - \frac{1}{p^{n-k+1}} T_{k-1}$$

for $r < k \le n$.

DEFINITION 3.5. For any prime p, let δ denote the generator of Γ satisfying

$$\zeta^\delta = \zeta^{1+p^r}.$$

DEFINITION 3.6. (a) For p odd, $r < k \le n$, or $p = 2$, $r < k \le 2r$, we define the square matrix M_k of order $\phi(p^{s(k)})$ as follows:

$$M_k \stackrel{\text{def}}{=} \begin{pmatrix} 1 & \cdots & 1 & \cdots & 1 \\ \zeta_{p^{s(k)}} & \cdots & \zeta_{p^{s(k)}}^{l} & \cdots & \zeta_{p^{s(k)}}^{p^{s(k)}-1} \\ \zeta_{p^{s(k)}}^{2} & \cdots & \zeta_{p^{s(k)}}^{2l} & \cdots & \zeta_{p^{s(k)}}^{2(p^{s(k)}-1)} \\ \vdots & & \vdots & & \vdots \\ \zeta_{p^{s(k)}}^{\phi(p^{s(k)})-1} & \cdots & \zeta_{p^{s(k)}}^{l(\phi(p^{s(k)})-1)} & \cdots & \zeta_{p^{s(k)}}^{(p^{s(k)}-1)(\phi(p^{s(k)})-1)} \end{pmatrix}.$$

(b) For $p = 2$ and $2r < k \le n$ we define

$$M_k \stackrel{\text{def}}{=} \begin{pmatrix} 1 & \cdots & 1 & \cdots & 1 \\ -\zeta_{p^{s(k)}} & \cdots & (-\zeta_{p^{s(k)}})^{l} & \cdots & (-\zeta_{p^{s(k)}})^{p^{s(k)}-1} \\ (-\zeta_{p^{s(k)}})^{2} & \cdots & (-\zeta_{p^{s(k)}})^{2l} & \cdots & (-\zeta_{p^{s(k)}})^{2(p^{s(k)}-1)} \\ \vdots & & \vdots & & \vdots \\ (-\zeta_{p^{s(k)}})^{\phi(p^{s(k)})-1} & \cdots & (-\zeta_{p^{s(k)}})^{l(\phi(p^{s(k)})-1)} & \cdots & (-\zeta_{p^{s(k)}})^{(p^{s(k)}-1)(\phi(p^{s(k)})-1)} \end{pmatrix}.$$

In both (a) and (b), l runs over the values between 1 and $p^{s(k)} - 1$ inclusive which are co-prime to p.

DEFINITION 3.7. For each k with $r < k \le n$, we define the polynomials

$$P_{k,i}(X) \in \mathbf{Q}_p(\zeta_{p^r})[X], \qquad 1 \le i \le \phi(p^{s(k)}),$$

by means of the matrix equation

$$\begin{pmatrix} P_{k,1}(X) \\ P_{k,2}(X) \\ \vdots \\ P_{k,\phi(p^{s(k)})}(X) \end{pmatrix} \stackrel{\text{def}}{=} M_k^{-1} \begin{pmatrix} 1 \\ X \\ \vdots \\ X^{\phi(p^{s(k)})} - 1 \end{pmatrix}.$$

THEOREM 3.1. *If $\mathfrak{A}$ denotes the order in $\mathbf{Q}_p(\zeta_{p^r})[\Gamma]$ generated over $\mathbf{Z}_p[\zeta_{p^r}][\Gamma]$ by the elements*

$$\{E_r\} \cup \left\{P_{k,j}(\delta^{p^{t(k)}})E_k\right\}_{\substack{r<k\le n \\ 1\le j\le \phi(p^{s(k)})}},$$

then $\mathbf{Z}_p[\zeta_{p^n}]$ is $\mathfrak{A}$-free of rank one with Galois generator β given by

$$\beta = b_{r,1} + \sum_{r<k\le n} \sum_{\substack{l=1 \\ (l,p)=1}}^{p^{s(k)}-1} b_{k,l}\zeta_{p^k}^l,$$

where $b_{k,l} \in \mathbf{Z}_p[\zeta_{p^r}]^\times$ for all k, l.

Remark. A result similar to Theorem 3.1 holds in the global situation.

4. Definitions and notation

Let $M = \mathbf{Q}_{p,\pi}^{m+r}$ and $L = \mathbf{Q}_{p,\pi}^r$.

By local class field theory, we can choose an unramified extension F of $\mathbf{Q}_p$ such that

(i) LF contains the p^r-th roots of unity.
(ii) FM contains the p^{m+r}-th roots of unity and
(iii) FM is generated over FL by a primitive p^{m+r}-th root of unity (which we denote by ζ).

Let $L' = \mathbf{Q}_p(\zeta_{p^r})$ and $M' = \mathbf{Q}_p(\zeta_{p^n})$. We will continue to use the definitions of the previous section. In what follows, we will frequently identify $\mathrm{Gal}(FM/FL)$ with both $\mathrm{Gal}(M/L)$ and $\mathrm{Gal}(M'/L')$.

Let $\Gamma = \mathrm{Gal}(FM/FL)$ and, by abuse of notation, we will also use T_k to denote the trace element in $LF[\Gamma]$ of the extension $FM/FL(\zeta_{p^k})$:

$$T_k = \mathrm{Tr}_{FM/FL(\zeta p^k)}.$$

So T_k is 'lifted' from $L'\Gamma$.

DEFINITION 4.2. Similarly, we 'lift' the idempotents from $L'[\Gamma]$ to $FL[\Gamma]$. We define $E_r, \ldots, E_{m+r}$, as follows:

$$E_k = \frac{1}{p^{m+r-k}} T_k - \frac{1}{p^{m+r-k+1}} T_{k-1}$$

where $r < k \leq m + r$, and

$$E_r = \frac{1}{p^m} T_r,$$

where the T_k now represent the trace elements in $FL[\Gamma]$.

Henceforth, we fix a uniformizer π of $\mathbf{Q}_p$, and a Lubin-Tate power series f associated to π.

DEFINITION 4.3. Let $\mathscr{O}_k$ denote the valuation ring in the division field, $\mathbf{Q}_{p,\pi}^k$, of level k associated to π.

We define the polynomials $P_{k,j}$ in the same way as Definition 3.7.

PROPOSITION 4.1. *The associated order of FM/FL is generated over $\mathfrak{O}_{FL}[\Gamma]$ by*

$$\{E_r\} \cup \left\{P_{k,j}(\delta^{p^{t(k)}}) E_k\right\}_{\substack{r<k\leq n \\ 1\leq j\leq\phi(p^{s(k)})}}$$

Proof. This follows from the fact that $\mathfrak{O}_{FM} = \mathfrak{O}_f \otimes_{\mathbf{Z}_p} \mathfrak{O}_{M'}$ and, by Noether's Theorem, $\mathfrak{A}_{FM/FL} = \mathfrak{O}_F \otimes_{\mathbf{Z}_p} \mathfrak{A}_{M'/L'}$. □

5. The Descent Lemma

Throughout this section, let F denote a finite non-ramified extension of $\mathbf{Q}_p$, M be a finite totally ramified abelian extension of K, and let L be a subfield of M. Let $\mathfrak{O}_F$, etc. denote the valuation ring of F, etc.

LEMMA 5.1. *There is a root of unity η of order prime to p such that*

$$\mathfrak{O}_F = \mathbf{Z}_p[\eta],$$
$$\mathfrak{O}_{FL} = \mathfrak{O}_L[\eta] = \mathfrak{O}_F\mathfrak{O}_L,$$
$$\mathfrak{O}_{FM} = \mathfrak{O}_M[\eta] = \mathfrak{O}_F\mathfrak{O}_M.$$

Proof. The first equality follows directly from the general theory of local fields.

Let ξ denote a prime element of L. Since FL/F is a totally ramified extension, we may choose a set of representatives for $\mathfrak{O}_{FL}$ modulo $\xi\mathfrak{O}_{FL}$ consisting of powers of η. Denoting the prime ideal of $\mathfrak{O}_L$ by $\mathfrak{P}$, we have

$$\mathfrak{O}_{FL} = \mathfrak{O}_L[\eta] + \mathfrak{P}\mathfrak{O}_{FL}.$$

By Nakayama's Lemma, it follows that

$$\mathfrak{O}_{FL} = \mathfrak{O}_L[\eta] = \mathfrak{O}_F\mathfrak{O}_L.$$

The third equality can be proved similarly. □

Let $\mathfrak{A}$ and $\mathfrak{B}$ denote the associated orders of the extensions FM/FL and M/L respectively.

LEMMA 5.2. *We have*
(a) $\mathfrak{A} \cap L[\Gamma] = \mathfrak{B}$,
(b) $\mathfrak{A} = \mathfrak{O}_F\mathfrak{O}_L \otimes_{\mathfrak{O}_L} \mathfrak{B}$.
In fact,

$$\mathfrak{A} = \bigoplus_j (\eta^j \otimes \mathfrak{B}),$$

where the sum is taken over powers of η which collectively form an $\mathfrak{O}_L$-basis of $\mathfrak{O}_L[\eta]$.

Proof. Part (a) is trivially true. In view of (a), to prove (b), it suffices to show that

$$\mathfrak{A} \subseteq \mathfrak{O}_F\mathfrak{O}_L \otimes_{\mathfrak{O}_L} \mathfrak{B}.$$

Let

$$\phi = \sum_{\gamma\in\Gamma} A_\gamma \gamma \quad (A_\gamma \in FL)$$

by in $\mathfrak{A}$, and write

$$A_\gamma = \sum_j A_j^{(\gamma)}\eta^j \quad \left(A_j^{(\gamma)} \in L\right)$$

where the sum is taken over only those powers of η which collectively form an $\mathfrak{O}_L$-basis of $\mathfrak{O}_L[\eta]$. Then we have

$$\phi = \sum_j \eta^j \otimes \left\{ \sum_{\gamma \in \Gamma} A_j^{(\gamma)} \gamma \right\}.$$

Applying ϕ to an integral element ρ in $\mathfrak{O}_F \mathfrak{O}_M$, we see that

$$\eta^j \otimes \left\{ \sum_{\gamma \in \Gamma} A_j^{(\gamma)} \gamma(\rho) \right\} \in \mathfrak{O}_F \mathfrak{O}_M$$

for each j. Hence

$$\sum_{\gamma \in \Gamma} A_j^{(\gamma)} \gamma(\rho) \in \mathfrak{O}_M$$

for an arbitrary $\rho \in \mathfrak{O}_L$. It follows that

$$\sum_{\gamma \in \Gamma} A_j^{(\gamma)} \gamma \in \mathfrak{B}. \quad \square$$

6. The main theorem

We maintain the notation of §4.

DEFINITION 6.1. We define the polynomials $Q_{i,k,j}$ through the identity:

$$P_{k,j}(X) = \sum_i \eta^i Q_{i,k,j}(X).$$

The sum is over a $\mathbf{Z}_p$-basis of $\mathfrak{O}_F$ (see Lemma 5.1 for the definition of the η^i) and the $Q_{i,k,j}$ are polynomials belonging to $L[X]$.

Then we have the main result of this article:

THEOREM 6.1. *The associated order of M/L is the order in $L[\Gamma]$ generated over $\mathfrak{O}_L[\Gamma]$ by*

$$\{E_r\} \cup \left\{ Q_{i,k,j}(\delta^{p^{t(k)}}) E_k \right\}_{\substack{r<k\leq n \\ \leq j \leq \phi(p^{s(k)})}},$$

where i runs over the set of indices so that $\{\eta^i\}$ is a $\mathbf{Z}_p$-basis for $\mathfrak{O}_F$.

Proof. Let $\mathfrak{B}'$ denote the subring of $L[\Gamma]$ generated over $\mathfrak{O}_L[\Gamma]$ by

$$\{E_r\} \cup \left\{ Q_{i,k,j}(\delta^{p^{t(k)}}) E_k \right\}_{\substack{r<k\leq n \\ 1\leq j \leq \phi(p^{s(k)})}}.$$

From the fact that $\mathfrak{O}_{FM} = \mathfrak{O}_F \otimes_{\mathbf{Z}_p} \mathfrak{O}_M$, and Proposition 4.1, we have that $Q_{i,k,j}(\delta^{p^{t(k)}})E_k$ sends $\mathfrak{O}_M$ to $\mathfrak{O}_M$. Hence

$$\mathfrak{B}' \subset \mathfrak{B}, \tag{1}$$

where $\mathfrak{B}$ denotes the associated order of M/L.

However, from the way the polynomials $Q_{i,k,j}$ are defined, we have

$$\mathfrak{A} \subset \mathfrak{O}_{FL} \otimes_{\mathfrak{O}_L} \mathfrak{B}',$$

where $\mathfrak{A}$ denotes the associated order in FM/FL.

By Lemma 5.1 and the facts that $\mathbf{Q}_p[\eta]$ and L are linearly disjoint, and $\mathfrak{B}' \subset L[\Gamma]$,

$$\mathfrak{O}_{FL} \otimes_{\mathfrak{O}_L} \mathfrak{B}' = \sum_j (\eta^j \otimes \mathfrak{B}') \tag{2}$$

$$= \bigoplus_j (\eta^j \otimes \mathfrak{B}'), \tag{3}$$

as abelian groups. By Lemma 5.2,

$$\mathfrak{A} = \bigoplus (\eta^j \otimes \mathfrak{B}'). \tag{4}$$

Combining equations 1, 2, and 4, we obtain the inclusion $\mathfrak{B} \subseteq \mathfrak{B}'$ and hence we have the desired equality: $\mathfrak{B} = \mathfrak{B}'$. □

References

1. S.P. Chan and C.H. Lim, *Relative Galois module structure of rings of integers of cyclotomic fields*, J. Reine Angew. Math. **434** (1993), 205–220.
2. A. Fröhlich, *The module structure of Kummer extensions over Dedekind domains*, J. Reine Angew. Math. **209** (1962), 39–53.
3. ______, *Galois module structure of algebraic integers*, Ergeb. Math. Grenzgeb. 3 Folge, Band 1, Springer-Verlag (1983), New York, 1983.
4. K. Iwasawa, *Local class field theory*, Oxford University Press, Oxford, 1986.
5. H.W. Leopoldt, *Über die Hauptordnung der ganzen Elemente eines abelschen Zahlkörpers*, J. Reine Angew. Math. **201** (1959), 119–149.
6. J. Lubin and J. Tate, *Formal complex multiplication in local fields*, Ann. of Math. **81** (1965), 380–387.
7. E. Noether, *Normalbasis bei Körpern ohne höhere Verzweigung*, J. Reine Angew. Math. **167** (1932), 147–152.
8. M.J. Taylor, *Relative Galois module structure of rings of integers and elliptic functions II*, Ann. of Math. **121** (1985), 415–431.
9. ______, *Formal groups and the Galois module structure of local rings of integers*, J. Reine Angew. Math. **358** (1985), 97–103.

National University of Singapore
Republic of Singapore