Werk

Titel: On Galois isomorphisms between ideals in extensions of local fields.

Autor: Byott, Nigel

Jahr: 1991

PURL: https://resolver.sub.uni-goettingen.de/purl?365956996_0073|log21

Kontakt/Contact

Digizeitschriften e.V.
SUB Göttingen
Platz der Göttinger Sieben 1
37073 Göttingen

info@digizeitschriften.de

manuscripta math. 73, 289 - 311 (1991)

manuscripta
mathematica

ON GALOIS ISOMORPHISMS BETWEEN IDEALS IN EXTENSIONS OF LOCAL FIELDS

Nigel Byott

Let L/K be a totally ramified, finite abelian extension of local fields, let $\mathfrak{O}_L$ and $\mathfrak{O}$ be the valuation rings, and let G be the Galois group. We consider the powers $\mathfrak{P}_L{}^r$ of the maximal ideal of $\mathfrak{O}_L$ as modules over the group ring $\mathfrak{O}G$. We show that, if G has order p^m (with p the residue field characteristic), if G is not cyclic (or if G has order p), and if a certain mild hypothesis on the ramification of L/K holds, then $\mathfrak{P}_L{}^r$ and $\mathfrak{P}_L{}^{r'}$ are isomorphic iff $r \equiv r' \bmod p^m$. We also give a generalisation of this result to certain extensions not of p-power degree, and show that, in the case $p = 2$, the hypotheses that G is abelian and not cyclic can be removed.

1 Introduction and statement of results

Let K be the field of fractions of a complete discrete valuation ring $\mathfrak{O}$ of characteristic 0 and residual characteristic $p > 0$. Throughout this paper we regard $\mathfrak{O}$ and hence K as fixed. We write $\mathfrak{P}$ for the maximal ideal of $\mathfrak{O}$ and e for the absolute ramification index of K (so $p\mathfrak{O} = \mathfrak{P}^e$). L/K will always denote a finite Galois field extension of K, and G its Galois group. We write $\mathfrak{O}_L$ for the valuation ring of L, and $\mathfrak{P}_L$ for the maximal ideal of $\mathfrak{O}_L$.

$\mathfrak{O}_L$ can be regarded as a (left) module over the group ring $\mathfrak{O}G$, and more generally so can each fractional $\mathfrak{O}_L$-ideal ${\mathfrak{P}_L}^r$. It is well-known that $\mathfrak{O}_L$ is free as an $\mathfrak{O}G$-module if and only if L/K is at most tamely ramified, and Ullom [16] has shown that every fractional ideal is then free over $\mathfrak{O}G$. In this paper, we assume that L/K is totally and wildly ramified, and investigate when two fractional ideals ${\mathfrak{P}_L}^r$ and ${\mathfrak{P}_L}^{r'}$ are isomorphic as $\mathfrak{O}G$-modules. Clearly a sufficient condition for this is that $r \equiv r' \pmod{n}$, where n is the degree of the extension L/K. Our main result is that, if L/K satisfies certain hypotheses, this congruence condition is also necessary.

Recall that the ramification groups G_i of L/K are defined by

$$G_i = \begin{cases} G & \text{if } i = -1 \\ \{\sigma \in G : (\sigma - 1)\mathfrak{O}_L \subseteq {\mathfrak{P}_L}^{i+1}\} & \text{if } i \geq 0. \end{cases}$$

L/K is totally ramified if and only if $G_0 = G$, and is then wildly ramified if and only if $G_1 \neq \{1\}$. If L/K is wildly ramified, we write $t(L/K)$ for the first positive ramification number, i.e. $t(L/K) = \max\{t : G_t = G_1\}$. If G has order $p^m k$, where $(p, k) = 1$, then $t(L/K) \leq ekp/(p-1)$ (see Proposition 3*(iv)* below):- in particular, if G is a p-group then $t(L/K) \leq ep/(p-1)$.

Our main result is the following:

Theorem 1 *Let L/K be a totally ramified abelian extension of degree p^m with*

$$t(L/K) \leq \frac{ep}{p-1} - 1.$$

If $m \geq 2$, assume that G is not cyclic. Then, for any integers r and r', the fractional $\mathfrak{O}_L$-ideals ${\mathfrak{P}_L}^r$ and ${\mathfrak{P}_L}^{r'}$ are isomorphic as $\mathfrak{O}G$-modules if and only if $r \equiv r' \pmod{p^m}$.

The proof of this involves an analysis of the case where L/K is cyclic of degree p, using the calculations of Ferton [6], and a reduction of the general case to this special case using the notion of factor equivalence, which has recently been studied extensively by Fröhlich ([9], [10]). We will also use standard ramification theory for local fields, as presented for instance in [14].

The necessity of the hypothesis on $t(L/K)$ is shown by the following example:- let K contain a primitive pth root of unity, and take $L = K(\sqrt[p]{\omega})$, where ω generates the maximal ideal $\mathfrak{P}$ of $\mathfrak{O}$. Then $t(L/K) = ep/(p-1)$. It is easily seen that every fractional $\mathfrak{O}_L$-ideal is a free module over the maximal order in KG, and hence that any two such ideals are isomorphic as $\mathfrak{O}G$-modules. We shall show that the conclusion of Theorem 1 is in fact false for any cyclic extension of degree p with

$$t(L/K) > \frac{ep}{p-1} - 1,$$

so that, for extensions of degree p, Theorem 1 is best possible.

If we remove the hypothesis that L/K be of p-power degree, our methods can still be applied to give some partial results in certain cases. To illustrate this, we will prove the following generalisation of the non-cyclic case of Theorem 1:

Theorem 2 *Let L/K be a totally ramified abelian extension of degree $p^m k$, where $(p,k) = 1$, and suppose that*

$$t(L/K) \leq \frac{ekp}{p-1} - k,$$

that G is not cyclic, and that

$$k \leq \frac{p^m - 1}{p-1}.$$

If $\mathfrak{P}_L{}^r$ and $\mathfrak{P}_L{}^{r'}$ are isomorphic as $\mathfrak{O}G$-modules, then either $r \equiv r' \pmod{p^m k}$ or, interchanging r and r' if necessary, $r = ap^m$ and $r' \equiv ap^m + 1 \pmod{p^m k}$ for some $a \not\equiv 0 \pmod{k}$.

Factor equivalence yields no information about cyclic extensions, and, at least in the simple formulation given in [9], is only applicable to abelian extensions. One can, however, extend Theorem 1 to non-abelian extensions and to cyclic p-extensions in the case $p = 2$. Indeed, without using factor equivalence, we will prove the following supplementary result to Theorem 1:

Theorem 3 *Let L/K be a totally ramified extension of degree p^m, with*

$$t(L/K) \leq \frac{ep}{p-1} - 1.$$

Then the p^m $\mathfrak{O}_L$-ideals $\mathfrak{P}_L{}^r$ $(1 \leq r \leq p^m)$ represent at least $2^{m-1}p$ distinct isomorphism classes of $\mathfrak{O}G$-modules. In particular, if $p = 2$ then $\mathfrak{P}_L{}^r$ and $\mathfrak{P}_L{}^{r'}$ are isomorphic as $\mathfrak{O}G$-modules if and only if $r \equiv r' \pmod{2^m}$.

Before commencing the proofs of these results, we indicate how they can be used to investigate the occurrence of extensions L/K with self-dual rings of integers. Given any $\mathfrak{O}G$-lattice M, the dual lattice M^* is defined to be $Hom_{\mathfrak{O}}(M, \mathfrak{O})$, with the G-action $(g\theta)(m) = \theta(g^{-1}m)$ for $\theta \in M^*$, $g \in G$, $m \in M$. We say that $\mathfrak{O}_L$ is self-dual if it is isomorphic to $\mathfrak{O}_L{}^*$ as an $\mathfrak{O}G$-module. The trace pairing $L \times L \longrightarrow K$ identifies $\mathfrak{O}_L^*$ with the inverse different $\mathfrak{D}_{L/K}{}^{-1}$ of L/K, so $\mathfrak{O}_L$ is self-dual if and only if $\mathfrak{O}_L \cong \mathfrak{D}_{L/K}{}^{-1}$ as $\mathfrak{O}G$-modules. Thus Theorem 1 has the following consequence:

Corollary 1 *Let L/K be a totally ramified abelian extension of degree p^m, and let $\mathfrak{P}_L{}^{-v} = \mathfrak{D}_{L/K}{}^{-1}$ be its inverse different. If $\mathfrak{O}_L$ is self-dual then*

$$\begin{aligned} &\textit{either} \quad v \equiv 0 \pmod{p^m} \\ &\textit{or} \quad\quad t(L/K) > \frac{ep}{p-1} - 1 \\ &\textit{or} \quad\quad L/K \textit{ is cyclic and } m \geq 2. \end{aligned}$$

Note that v is determined by the ramification groups of L/K ([14] IV Proposition 4).

We end this section with some conditions on the associated order $\mathfrak{A}_{L/K}$ of L/K which ensure that $\mathfrak{O}_L$ is self-dual. Recall that

$$\mathfrak{A}_{L/K} = \{\alpha \in KG : \alpha\mathfrak{O}_L \subseteq \mathfrak{O}_L\}$$

(and more generally, the associated order of any fractional ideal $\mathfrak{P}_L{}^r$ is defined by replacing both occurrences of $\mathfrak{O}_L$ by $\mathfrak{P}_L{}^r$ in this definition). For any element $\alpha = \sum_{g \in G} a_g g$ of KG, we write $\bar{\alpha} = \sum a_g g^{-1}$.

Proposition 1 *Let L/K be an abelian extension.*
(i) If $\mathfrak{A}_{L/K} = \bar{\mathfrak{A}}_{L/K}$ and $\mathfrak{A}_{L/K} \cong (\mathfrak{A}_{L/K})^*$ as $\mathfrak{O}G$-modules, then $\mathfrak{O}_L$ is self-dual.
(ii) If $\mathfrak{A}_{L/K}$ is a Hopf order in the Hopf algebra KG (cf. [15]), then $\mathfrak{O}_L$ is self-dual.

Proof. (i) Since ${\mathfrak{O}_L}^* \cong {\mathfrak{D}_{L/K}}^{-1}$, the associated order of ${\mathfrak{D}_{L/K}}^{-1}$ is $\bar{\mathfrak{A}}_{L/K}$, which coincides with $\mathfrak{A}_{L/K}$. Moreover, as $\bar{\mathfrak{A}}_{L/K} \cong (\mathfrak{A}_{L/K})^*$, $\mathfrak{A}_{L/K}$ is a (weakly) self-dual order in the sense of [7] §8. By Theorem 10 of that paper, $\mathfrak{O}_L$ and ${\mathfrak{D}_{L/K}}^{-1}$ are both free over $\mathfrak{A}_{L/K}$, and so are isomorphic.
(ii) is a special case of (i): if $\mathfrak{A}_{L/K}$ is a Hopf order then by [13] $(\mathfrak{A}_{L/K})^* \cong \mathfrak{A}_{L/K}$, since $\mathfrak{O}$ is a principal ideal domain; and $\bar{\mathfrak{A}}_{L/K} = \mathfrak{A}_{L/K}$ since $\alpha \mapsto \bar{\alpha}$ is the antipode of the Hopf algebra KG.

2 Extensions of degree p

In this section, we will prove Theorem 1 for extensions of degree p, and will also discuss almost maximally ramified extensions of degree p. We make use of the calculations of Ferton [6], and largely follow her notation.

Thus let L/K be a totally ramified cyclic extension of degree p, and let $t = t(L/K)$. Then $1 \leq t \leq ep/(p-1)$, and $(t,p) = 1$ unless $t = ep/(p-1)$ ([14] IV §2 Ex.3). Any such value of t can occur (*loc. cit.* Ex.5).

Let $t = pa_0 + a$ with $0 \leq a \leq p-1$. Note that if $t+1 \geq ep/(p-1)$ then $ep-(p-1) \leq (p-1)t \leq ep$ and $t \equiv a \pmod{p}$, so

$$t = \frac{ep-a}{p-1} \text{ if and only if } t \geq \frac{ep}{p-1} - 1. \tag{1}$$

Now let ω (resp. π) be a generator of $\mathfrak{P}$ (resp. $\mathfrak{P}_L$), and fix a generator σ of the Galois group G of L/K. Set $f = \sigma - 1 \in \mathfrak{O}G$. Since $(f+1)^p = \sigma^p = 1$, we then have

$$f^p = -\sum_{n=1}^{p-1} \binom{p}{n} f^n. \tag{2}$$

If $a \neq 0$ then π^a is a normal basis for L/K, i.e. $L = KG\pi^a$ ([3] Proposition 3). For $a + 1 - p \leq r \leq a$ let

$$\mathfrak{U}_r = \{\alpha \in KG : \alpha\, \pi^a \in \mathfrak{P}_L{}^r\}.$$

Then $\mathfrak{U}_r$ is a fractional $\mathfrak{O}G$-ideal containing $\mathfrak{O}G$, and $\mathfrak{U}_r \cong \mathfrak{P}_L{}^r$ as $\mathfrak{O}G$-modules. From [6] Proposition 3 we have the following explicit description of the lattices $\mathfrak{U}_r$:

Proposition 2 *If $a \neq 0$ and $a + 1 - p \leq r \leq a$ then the elements*

$$\frac{f^i}{\omega^{\nu_i(r)}} \quad (0 \leq i \leq p-1)$$

form an $\mathfrak{O}$-basis of $\mathfrak{U}_r$, where

$$\nu_i(r) = \left[\frac{it + a - r}{p}\right].$$

(For any real number y, $[y]$ denotes the largest integer not exceeding y.)

We can now prove Theorem 1 for extensions of degree p:

Lemma 1 *Let L/K be a totally ramified cyclic extension of degree p, such that*

$$t(L/K) \leq \frac{ep}{p-1} - 1.$$

For any integers r and r', $\mathfrak{P}_L{}^r$ and $\mathfrak{P}_L{}^{r'}$ are isomorphic as $\mathfrak{O}G$-modules if and only if $r \equiv r' \pmod{p}$.

Proof. With the above notation, $a \neq 0$ by the hypothesis on t, and if $r \equiv r' \pmod{p}$ then certainly $\mathfrak{P}_L{}^r \cong \mathfrak{P}_L{}^{r'}$. Thus, adjusting r and r' by multiples of p, and interchanging them if necessary, we may assume that $a + 1 - p \leq r \leq r' \leq a$; it is then sufficient to show that if $\mathfrak{U}_r \cong \mathfrak{U}_{r'}$ then $r = r'$.

To simplify notation, let $\mathfrak{U} = \mathfrak{U}_r$, $\mathfrak{U}' = \mathfrak{U}_{r'}$, $\nu_i = \nu_i(r)$, $\nu_i' = \nu_i(r')$. Then $\nu_i' \leq \nu_i \leq e$ for $0 \leq i \leq p-1$. Any isomorphism $\theta : \mathfrak{U} \longrightarrow \mathfrak{U}'$ of $\mathfrak{O}G$-modules

is determined by $\theta(1)$. Setting $\alpha = \theta(1) \in \mathfrak{U}'$ and using Proposition 2, we have

$$\alpha = \sum_{j=0}^{p-1} c_j \frac{f^j}{\omega^{\nu'_j}} \text{ for some } c_j \in \mathfrak{O}.$$

The elements

$$\alpha \frac{f^i}{\omega^{\nu_i}} = \sum_{j=0}^{p-1} c_j \frac{f^{i+j}}{\omega^{\nu_i+\nu'_j}} \quad (0 \leq i \leq p-1)$$

form an $\mathfrak{O}$-basis for $\mathfrak{U}'$. Using (2) to expand f^{i+j} for $i+j \geq p$, comparing coefficients of $1 = f^0$, and noting that $\nu_0 = \nu'_0 = 0$, we see that $c_0 \in \mathfrak{O}^\times$, where $\mathfrak{O}^\times$ denotes the group of units of $\mathfrak{O}$. Without loss of generality, we suppose $c_0 = 1$. Then $\mathfrak{U}'$ has a basis consisting of the elements

$$\alpha \frac{f^i}{\omega^{\nu_i}} = \omega^{\nu'_i - \nu_i} \frac{f^i}{\omega^{\nu'_i}} + \sum_{j=1}^{p-1-i} c_j \frac{f^{i+j}}{\omega^{\nu_i+\nu'_j}} + \sum_{j=p-i}^{p-1} c_j \frac{f^{i+j}}{\omega^{\nu_i+\nu'_j}}. \tag{3}$$

We will show that

$$\frac{f^{i+j}}{\omega^{\nu_i+\nu'_j}} \in \mathfrak{U}' \text{ whenever } p-i \leq j \leq p-1. \tag{4}$$

Admitting this for the moment, we must have $\nu'_i - \nu_i \geq 0$ for each i, since the elements (3) lie in $\mathfrak{U}'$. We have already observed, however, that $\nu'_i \leq \nu_i$, so $\nu'_i = \nu_i$ for $0 \leq i \leq p-1$. It then follows from the definitions of ν_i and ν'_i that $r = r'$. Thus it only remains to prove (4).

Writing $i+j = p+k$ and using (2), we have

$$\frac{f^{i+j}}{\omega^{\nu_i+\nu'_j}} = -\sum_{n=1}^{p-1} \binom{p}{n} \frac{f^{k+n}}{\omega^{\nu_i+\nu'_j}}.$$

If $k+n \geq p$ then, using (2) again and noting that the binomial coefficients are divisible by p, we have

$$\binom{p}{n} \frac{f^{k+n}}{\omega^{\nu_i+\nu'_j}} \in \frac{p^2}{\omega^{\nu_i+\nu'_j}} \mathfrak{O}G \subseteq \mathfrak{O}G \subseteq \mathfrak{U}'.$$

On the other hand, if $k+n<p$ then

$$\binom{p}{n}\frac{f^{k+n}}{\omega^{\nu_i+\nu'_j}}=\binom{p}{n}\omega^{\nu'_{k+n}-\nu_i-\nu'_j}\frac{f^{k+n}}{\omega^{\nu'_{k+n}}}$$

and we must show that

$$e+\nu'_{k+n}-\nu_i-\nu'_j\geq 0 \text{ whenever } i+j=p+k\geq p \text{ and } 1\leq n\leq p-1. \quad (5)$$

Clearly it is sufficient to take $n=1$. Now

$$\begin{aligned}
&e+\nu'_{k+1}-\nu_i-\nu'_j\\
&\quad= e+\left[\frac{(i+j-p+1)t+a-r'}{p}\right]-\left[\frac{it+a-r}{p}\right]-\left[\frac{jt+a-r'}{p}\right]\\
&\quad\geq e+\left[\frac{(1-p)t-a+r}{p}\right]\\
&\quad= e-t+a_0+\left[\frac{r}{p}\right].
\end{aligned}$$

If $t=\dfrac{ep}{p-1}-1$ then $a=p-1$, $a_0=\dfrac{e}{p-1}-1$ and $0\leq r\leq p-1$, so

$$e-t+a_0+\left[\frac{r}{p}\right]=e-\left(\frac{ep}{p-1}-1\right)+\left(\frac{e}{p-1}-1\right)+0=0;$$

whereas if $t<\dfrac{ep}{p-1}-1$ then $(p-1)t<ep-a$ by (1), and $r\geq a+1-p>-p$, so

$$\begin{aligned}
e-t+a_0+\left[\frac{r}{p}\right] &> \frac{(p-1)t+a}{p}-t+a_0+\left[\frac{r}{p}\right]\\
&= -\frac{t}{p}+\left(a_0+\frac{a}{p}\right)+\left[\frac{r}{p}\right]\\
&= \left[\frac{r}{p}\right]\\
&\geq -1,
\end{aligned}$$

and since the left-hand side is an integer, it follows that

$$e-t+a_0+\left[\frac{r}{p}\right]\geq 0.$$

Thus (5) holds in all cases, which completes the proof of (4) and thus of the Lemma.

In [11], Jacobinski defines the notion of an almost maximally ramified extension. In the case of a cyclic extension of degree p, the definition reduces to the following condition:

$$L/K \text{ is almost maximally ramified} \Leftrightarrow t \geq \frac{ep}{p-1} - 1.$$

Although it is unnecessary for the proofs of the three theorems, we will now consider extensions with this property, thereby showing that Theorem 1 is best possible for extensions of degree p:

Lemma 2 *Let L/K be an almost maximally ramified cyclic extension of degree p. Then $\mathfrak{O}_L$ is self-dual as an $\mathfrak{O}G$-module. In particular, if $t+1 > ep/(p-1)$ then the conclusion of Theorem 1 is false for L/K.*

Proof. We first consider the maximally ramified case $t = ep/(p-1)$. Here, K contains a primitive pth root of 1 ([12] Theorem 3), and $L = K(\sqrt[p]{\omega})$ for some generator ω of $\mathfrak{P}$. As noted after the statement of Theorem 1, it follows that every fractional $\mathfrak{O}_L$-ideal is free over the maximal order in KG, and hence is isomorphic to every other fractional $\mathfrak{O}_L$-ideal.

For any value of t, we have $\mathfrak{D}_{L/K}^{-1} = \mathfrak{P}_L{}^{-v}$, where, by [14] IV Proposition 4, $v = (p-1)(t+1) \equiv -a-1 \pmod{p}$. If $t+1 = ep/(p-1)$ then $v \equiv 0 \pmod{p}$, so certainly $\mathfrak{O}_L \cong \mathfrak{D}_{L/K}^{-1}$; whilst if $t+1 > ep/(p-1)$ then by (1), $t = (ep-a)/(p-1)$ with $0 \leq a \leq p-2$, so $v \not\equiv 0 \pmod{p}$.

It remains to show that, if $t = (ep-a)/(p-1)$ with $1 \leq a \leq p-2$ then $\mathfrak{O}_L \cong \mathfrak{D}_{L/K}^{-1}$. Now $\mathfrak{O}_L \cong \mathfrak{U}_0$ and $\mathfrak{D}_{L/K}^{-1} \cong \mathfrak{U}_{a+1-p}$, so writing $\mathfrak{U} = \mathfrak{U}_0$ and $\mathfrak{U}' = \mathfrak{U}_{a+1-p}$, it suffices to show that $\mathfrak{U} \cong \mathfrak{U}'$. By Proposition 2, these two lattices have $\mathfrak{O}$-bases

$$\frac{f^i}{\omega^{\nu_i}} \text{ respectively } \frac{f^i}{\omega^{\nu_i'}} \quad (0 \leq i \leq p-1),$$

where

$$\nu_i = \left[\frac{it+a}{p}\right] = ia_0 + \left[\frac{(i+1)a}{p}\right]$$

and

$$\begin{aligned}\nu_i' = \left[\frac{it+p-1}{p}\right] &= ia_0 + \left[\frac{ia+p-1}{p}\right] \\ &= \begin{cases} 0 & \text{if } i = 0 \\ 1 + a_0 + \nu_{i-1} & \text{if } 1 \le i \le p-1. \end{cases}\end{aligned}$$

Let

$$\alpha = 1 + \frac{f}{\omega^{\nu_1'}} = 1 + \frac{f}{\omega^{1+a_0}}.$$

We will show that multiplication by the element α of $\mathfrak{U}'$ induces an $\mathfrak{O}$-linear isomorphism between $\mathfrak{U}$ and $\mathfrak{U}'$; this map is then necessarily an isomorphism of $\mathfrak{O}G$-modules. For $0 \le i \le p-2$ we have

$$\alpha \frac{f^i}{\omega^{\nu_i}} = \omega^{\nu_i' - \nu_i} \frac{f^i}{\omega^{\nu_i'}} + \frac{f^{i+1}}{\omega^{\nu_{i+1}'}} \in \mathfrak{U}'$$

since $\nu_i \le \nu_i'$. Also, using (2),

$$\alpha \frac{f^{p-1}}{\omega^{\nu_{p-1}}} = \omega^{\nu_{p-1}' - \nu_{p-1}} \frac{f^{p-1}}{\omega^{\nu_{p-1}'}} + \sum_{n=1}^{p-1} b_n \frac{f^n}{\omega^{\nu_n'}},$$

where

$$b_n = -\binom{p}{n} \omega^{\nu_n' - \nu_{p-1} - 1 - a_0}.$$

Since $\nu_{p-1} = e$, b_n has valuation $\nu_n' - 1 - a_0 = \nu_{n-1} \ge 0$, so $b_n \in \mathfrak{O}$ for all n. Thus $\alpha\,\mathfrak{U} \subseteq \mathfrak{U}'$, and the matrix expressing multiplication by α in terms of the above bases of $\mathfrak{U}$ and $\mathfrak{U}'$ is

$$B = \begin{pmatrix} \omega^{\nu_0' - \nu_0} & 0 & 0 & \cdots & 0 \\ 1 & \omega^{\nu_1' - \nu_1} & 0 & \cdots & b_1 \\ 0 & 1 & \omega^{\nu_2' - \nu_2} & \cdots & b_2 \\ \vdots & 0 & \ddots & \ddots & \vdots \\ & \vdots & & & \\ & & & \omega^{\nu_{p-2}' - \nu_{p-2}} & b_{p-2} \\ 0 & 0 & & 1 & \omega^{\nu_{p-1}' - \nu_{p-1}} + b_{p-1} \end{pmatrix}$$

To complete the proof, we must show that $\det(B) \in \mathfrak{O}^\times$.

Since $a < p-1$, there is an integer h with $1 \leq h \leq p-2$ such that

$$\left(\frac{h-1}{h}\right)p < a < \left(\frac{h}{h+1}\right)p.$$

We then have

$$\begin{aligned} \nu_i &= (a_0+1)i \qquad \text{if } i < h \\ \nu_h &= (a_0+1)h - 1. \end{aligned}$$

Thus if $2 \leq n \leq h$ then $\nu_{n-1} > 0$ and $b_n \in \mathfrak{P}$, while $b_1 \in \mathfrak{O}^\times$ as $\nu_0 = 0$. Also, $\nu'_h - \nu_h = 1 + a_0 + \nu_{h-1} - \nu_h = 1$. Thus the matrix entries $\omega^{\nu'_h - \nu_h}$ and b_n $(2 \leq n \leq h)$ lie in $\mathfrak{P}$. It follows that $\det(B) \equiv \pm\omega^{\nu'_0 - \nu_0} b_1 = \pm b_1 \pmod{\mathfrak{P}}$, every other term in the expansion of $\det(B)$ lying in $\mathfrak{P}$. Thus $\det(B) \in \mathfrak{O}^\times$ as required.

We remark that if $t+1 > ep/(p-1)$ there may be other isomorphisms between ideals in addition to that given by Lemma 2. For example, in the absolutely unramified case $e = 1$, any ideal ${\mathfrak{P}_L}^r$ must have as its associated order either the group ring $\mathfrak{O}G$ or the maximal order

$$\mathfrak{M} = \mathfrak{O}G + \frac{1}{p}\sum_{\sigma \in G} \sigma.$$

These are both self-dual orders in the sense of [7], so ${\mathfrak{P}_L}^r$ is free over its associated order, and hence isomorphic to either $\mathfrak{O}G$ or $\mathfrak{M}$. Thus there must be many isomorphisms between the ideals $\mathfrak{O}_L, \mathfrak{P}_L, \ldots, {\mathfrak{P}_L}^{p-1}$. (The author is indebted to D.Burns for this observation.)

In the situation of Lemma 2, $\mathfrak{O}_L$ need not be free over its associated order. Indeed, Bertrandias, Bertrandias and Ferton [2] give a criterion for $\mathfrak{O}_L$ to be free when L/K is almost maximally ramified:- writing $t/p = [a_0; a_1, \ldots, a_n]$ for the continued fraction expansion of t/p, $\mathfrak{O}_L$ is free over its associated order if and only if $n \leq 4$. (The same is also true for almost maximally ramified cyclic extensions of degree p^m, $m \geq 2$:- see [1]). Thus if L/K is almost maximally ramified and cyclic of degree p, with $n \geq 5$, then $\mathfrak{O}_L$ is self-dual but not free over its associated order. The first example of this is

$p = 13$, $a = 8$. The question of the existence of abelian extensions with this property was raised in [5] (p148). Some elementary abelian examples of degree p^2 are constructed in [4]; these have $t + 1 = ep/(p-1)$.

3 Factor equivalence

We now recall from [9] the notion of factor equivalence between $\mathfrak{O}G$-lattices spanning the same KG-module. We will then derive a necessary and sufficient condition for two fractional $\mathfrak{O}_L$-ideals to be factor equivalent.

Let Γ be a finite abelian group, let $\Gamma^\dagger$ denote its group of (complex-valued) abelian characters, and let $S(\Gamma^\dagger)$ denote the lattice of subgroups of $\Gamma^\dagger$. There is an inclusion-reversing bijection between the lattice of subgroups of Γ and $S(\Gamma^\dagger)$, given by associating to each $\Delta \leq \Gamma$ the subgroup $X_\Delta = \{\chi : \chi(\Delta) = 1\}$ of $\Gamma^\dagger$.

A *division* D of $\Gamma^\dagger$ is an equivalence class of characters, two characters being deemed equivalent if they generate the same cyclic subgroup of $\Gamma^\dagger$. We write $\bar{D}$ for the subgroup generated by any element of D. Let I_K denote the group of fractional ideals of $\mathfrak{O}$ (written multiplicatively). We extend any function $f : S(\Gamma^\dagger) \longrightarrow I_K$ to the set of divisions D of $\Gamma^\dagger$ by defining

$$f(D) = \prod_{C \leq \bar{D}} f(C)^{\mu(\bar{D}:C)},$$

where the product is over all subgroups of $\bar{D}$, and μ denotes the Möbius function. By Möbius inversion, we then have

$$f(X) = \prod_{D \subseteq X} f(D) \tag{6}$$

for every cyclic subgroup X of $\Gamma^\dagger$. The function f is said to be *factorisable* if (6) holds for every subgroup X.

Now let M, N be two $\mathfrak{O}\Gamma$-lattices spanning the same $K\Gamma$-module V. We define a function $f : S(\Gamma^\dagger) \longrightarrow I_K$ by setting

$$f(X_\Delta) = [M^\Delta : N^\Delta]_\mathfrak{O} \text{ for each } \Delta \leq \Gamma,$$

where M^Δ, N^Δ denote the lattices of Δ-fixed points of M, N, and $[\,:\,]_\mathfrak{O}$ is the $\mathfrak{O}$-module index, defined for two $\mathfrak{O}$-lattices spanning the same K-space (see e.g. [8] §3). The lattices M, N are said to be *factor equivalent*, written $M \wedge N$, if this function f is factorisable. This gives an equivalence relation on the set of $\mathfrak{O}\Gamma$-lattices spanning a given $K\Gamma$-module V, and moreover, it is shown in [9] that $M \wedge N$ whenever M and N are isomorphic as $\mathfrak{O}\Gamma$-modules.

We remark that factor equivalence is independent of the base field K in the following sense:- if F is a finite extension of K, and M, N are $\mathfrak{O}_F\Gamma$-lattices, then they are factor equivalent as such (i.e. working with $\mathfrak{O}_F$-module indices) if and only if they are factor equivalent when considered as $\mathfrak{O}\Gamma$-lattices by restriction of scalars. We will use this observation in the proof of Theorem 2.

We now take M, N to be $\mathfrak{O}_L$-ideals, and Γ to be the Galois group G.

Lemma 3 *Let L/K be a totally ramified abelian extension of degree p^m, and assume that its Galois group G is not cyclic. For any integers r, r', write*

$$s = r - 1 = s_0 + ps_1 + \cdots + p^{m-1}s_{m-1} + p^m x$$

$$s' = r' - 1 = s'_0 + ps'_1 + \cdots + p^{m-1}s'_{m-1} + p^m x'$$

$$\text{with } 0 \le s_i, s'_i \le p-1 \text{ for } 0 \le i \le m-1.$$

Then the $\mathfrak{O}G$-modules $\mathfrak{P}_L{}^r$, $\mathfrak{P}_L{}^{r'}$ are factor equivalent if and only if $s'_i = s_i + v$ for $0 \le i \le m-1$, where v is independent of i.

Proof. If $r \equiv r' \pmod{p^m}$ then $\mathfrak{P}_L{}^r \cong \mathfrak{P}_L{}^{r'}$, so certainly $\mathfrak{P}_L{}^r \wedge \mathfrak{P}_L{}^{r'}$. Thus we may assume that $x = x' = 0$.

Let $v_i = s'_i - s_i$ for $0 \le i \le m-1$. Also, for $k \ge 0$, set

$$s(k) = \left[\frac{s}{p^k}\right], \quad s'(k) = \left[\frac{s'}{p^k}\right], \quad v(k) = s'(k) - s(k).$$

Thus

$$v(k) = \begin{cases} v_k + pv_{k+1} + \cdots + p^{m-1-k}v_{m-1} & \text{if } k < m \\ 0 & \text{if } k \ge m \end{cases}$$

Let H be a subgroup of G of order p^k, with fixed field $F = L^H$. Then

$$(\mathfrak{P}_L{}^r)^H = \mathfrak{P}_L{}^r \cap F = \mathfrak{P}_F{}^{1+s(k)}$$

(and similarly for $\mathfrak{P}_L{}^{r'}$) since the smallest integer not less than r/p^k is

$$\left[\frac{r+p^k-1}{p^k}\right] = 1 + s(k).$$

Thus

$$\begin{aligned}[(\mathfrak{P}_L{}^r)^H : (\mathfrak{P}_L{}^{r'})^H]_{\mathfrak{O}} &= [\mathfrak{P}_F{}^{1+s(k)} : \mathfrak{P}_F{}^{1+s'(k)}]_{\mathfrak{O}} \\ &= [\mathfrak{O}_F : \mathfrak{P}_F{}^{v(k)}]_{\mathfrak{O}} \\ &= \mathfrak{P}^{v(k)},\end{aligned}$$

since F/K is totally ramified. Hence the assertion $\mathfrak{P}_L{}^r \wedge \mathfrak{P}_L{}^{r'}$ is equivalent to the factorisability of the map $f : S(G^\dagger) \longrightarrow I_K$ given by

$$f(X_H) = \mathfrak{P}^{v(k)} \text{ for any } H \leq G \text{ of order } p^k.$$

For j in the range $1 \leq j \leq m$, consider the following three assertions:-

(I) $f(X_H) = \prod_{D \subseteq X_H} f(D)$ for every $H \leq G$ of order at least p^{m-j};

(II) $v_{m-i} = v_{m-1}$ for $1 \leq i \leq j$;

(III) if D is a division of $G^\dagger$ and $\bar{D}$ has order p^d with $d \leq j$ then

$$f(D) = \begin{cases} \mathfrak{O} & \text{if } d = 0 \\ \mathfrak{P}^{p^{d-1}v_{m-1}} & \text{if } d \geq 1. \end{cases}$$

We shall prove by induction on j that (I) $\Leftrightarrow$ (II) $\Rightarrow$ (III) for each j. In the case $j = m$, the equivalence (I) $\Leftrightarrow$ (II) proves the Lemma.

For $j = 1$, (I) holds since X_H is cyclic, being of order 1 or p, and (II) holds trivially. For (III) we must consider divisions D for which $\bar{D}$ has order 1 or p. But $f(\{1\}) = \mathfrak{P}^{v(m)} = \mathfrak{O}$, whilst if $\bar{D}$ has order p then

$$f(D) = f(\bar{D})f(\{1\})^{-1} = \mathfrak{P}^{v(m-1)}\mathfrak{O}^{-1} = \mathfrak{P}^{v_{m-1}}.$$

Thus (III) holds for $j = 1$.

Now let $2 \leq j \leq m$ and suppose that (I), (II), (III) all hold with j replaced by $j-1$. As G is not cyclic, it has a subgroup H of order p^{m-j} such that G/H is not cyclic. Thus any division $D \subseteq X_H$ generates a group $\bar{D}$ of order p^d for some $d \leq j-1$. If $d > 0$ then D contains $|D| = p^{d-1}(p-1)$ characters, and by (III) for $j-1$, $f(D) = \mathfrak{P}^{|D|\, v_{m-1}/(p-1)}$. For any such H, the condition in (I) therefore becomes

$$\mathfrak{P}^{v(m-j)} = f(\{1\}) \prod_{1 \neq \chi \in X_H} \mathfrak{P}^{v_{m-1}/(p-1)},$$

or equivalently,

$$v(m-j) = \frac{p^j - 1}{p-1}\, v_{m-1}.$$

Using (II) for $j-1$ and the definition of $v(m-j)$, this can be rewritten as

$$v_{m-j} + (p + \cdots + p^{j-1}) v_{m-1} = \frac{p^j - 1}{p-1}\, v_{m-1},$$

i.e. $v_{m-j} = v_{m-1}$. Thus (I) $\Rightarrow$ (II) for j, and conversely if (II) holds for j then (I) holds for j, except possibly when H is of order p^{m-j} and G/H is cyclic. But (I) always holds when G/H is cyclic, so we have shown (I) $\Leftrightarrow$ (II) for j. Finally, if D is a division for which $\bar{D}$ has order p^j then $\bar{D} = X_H$ for some subgroup $H \leq G$ of order p^{m-j} with G/H cyclic. Applying (I) and arguing as above for the divisions $\{1\} \neq D' \neq D$ contained in $\bar{D}$,

$$\begin{aligned} \mathfrak{P}^{v(m-j)} &= f(\{1\}) \left(\prod_{D'} f(D') \right) f(D) \\ &= \mathfrak{O}\, \mathfrak{P}^{(p^{j-1}-1)\, v_{m-1}/(p-1)}\, f(D) \end{aligned}$$

so $f(D) = \mathfrak{P}^y$, where

$$\begin{aligned} y &= v(m-j) - \frac{p^{j-1}-1}{p-1}\, v_{m-1} \\ &= (1 + p + \cdots + p^{j-1})\, v_{m-1} - \frac{p^{j-1}-1}{p-1}\, v_{m-1} \\ &= p^{j-1} v_{m-1}. \end{aligned}$$

Thus (III) holds for j, which completes the induction and the proof of the Lemma.

The following corollaries indicate that factor equivalence considerations go a long way towards proving Theorem 1 (in the non-cyclic case), but are not in themselves sufficient.

Corollary 2 *Let L/K be as in the Lemma, and let r be divisible by p, with $0 \leq r \leq p^{m-1}$. If $\mathfrak{P}_L{}^r \wedge \mathfrak{P}_L{}^{r'}$ then $r \equiv r' \pmod{p^m}$.*

Proof. In the notation of the Lemma, $s_0 = p-1$ and $s_{m-1} = 0$. Thus $v + (p-1) = s'_0 \leq p-1$ and $v + 0 = s'_{m-1} \geq 0$, whence $v = 0$.

Corollary 3 *Let L/K be as in the Lemma. Then $\mathfrak{O}_L \wedge \mathfrak{P}_L$.*

Proof. Taking $r = 0$ and $r' = 1$, we have $s_i = p-1$ and $s'_i = 0$ for all i, so the condition of the Lemma holds with $v = 1-p$.

4 Conclusion of the proofs

We begin with some ramification theory.

Proposition 3 *Let L/K be a totally ramified extension of degree $p^m k$, where $(p,k) = 1$ and $m \geq 1$. Let G be its Galois group. Then:-*

(i) G_1 has order p^m, and G is a semidirect product of G_1 by a cyclic group C of order k;

(ii) if C is normal in G then, writing $M = L^C$ for the fixed field of C,

$$t(M/K) = \frac{1}{k}\, t(L/K);$$

(iii) if $k = 1$ or if G is abelian then G has a normal subgroup H of index p whose fixed field $F = L^H$ satisfies

$$t(F/K) = \frac{1}{k}\, t(L/K);$$

(iv) if C is normal in G then

$$t(L/K) \leq \frac{ekp}{p-1};$$

(v) if $k = 1$ and $m \geq 2$ then G has a normal subgroup N of order p whose fixed field $E = L^N$ satisfies $t(E/K) = t(L/K)$ and $t(L/E) \equiv t(L/K) \pmod{p}$.

Proof. *(i)*: see [14] IV §2.

(ii) follows from *(i)* and [14] IV Proposition 14.

(iii): $G_{t+1} \neq G_t = G_1$, where $t = t(L/K)$, so G_{t+1} has order dividing p^{m-1}. If $k = 1$ take for H any subgroup of order p^{m-1} containing G_{t+1}; then H is normal in G being a subgroup of index p in a finite p-group. If G is abelian, take for H any subgroup of order $p^{m-1}k$ containing G_{t+1}. In either case, H has the required property by [14] IV Proposition 14.

(iv): If L/K has degree p then $t(L/K) \leq ep/(p-1)$ by [14] IV §2 Ex.3. In the case $k = 1$ the result now follows from *(iii)*. Finally, if $k > 1$ and M is as in *(ii)*, then

$$t(L/K) = k\, t(M/K) \leq \frac{ekp}{p-1}.$$

(v): Let n be the integer such that $G_n \neq G_{n+1} = \{1\}$. Since $G_n \lhd G$, G acts on G_n by conjugation, and as G is a p-group, each orbit has p-power cardinality. As at least one orbit, namely $\{1\}$, has cardinality 1, it follows

that some element $g \neq 1$ of G_n is central in G, so there is a subgroup N of G_n of order p, central and hence normal in G. N has the required properties by [14] IV Propositions 2, 11 and 14.

We can now prove the three theorems:

Proof of Theorem 1. By Lemma 1, we may assume that $m \geq 2$, so G is not cyclic. If $r \equiv r' \pmod{p^m}$ then certainly $\mathfrak{P}_L{}^r \cong \mathfrak{P}_L{}^{r'}$. Writing $s = r - 1$, $s' = r' - 1$, we may therefore assume for the converse that $0 \leq s, s' \leq p^m - 1$. If $\mathfrak{P}_L{}^r \cong \mathfrak{P}_L{}^{r'}$ then these ideals are factor equivalent, so by Lemma 3, $s_i' = s_i + v$ for some v, where the notation is as in the Lemma. We must show that $v = 0$.

Let H and F be as in Proposition 3*(iii)*, and let $Q = G/H$. Taking H-fixed points in the isomorphism $\mathfrak{P}_L{}^r \cong \mathfrak{P}_L{}^{r'}$ of $\mathfrak{O}G$-modules, we obtain an isomorphism $(\mathfrak{P}_L{}^r)^H \cong (\mathfrak{P}_L{}^{r'})^H$ of $\mathfrak{O}Q$-modules. But, arguing as in the proof of Lemma 3,

$$(\mathfrak{P}_L{}^r)^H = \mathfrak{P}_F{}^{1+s_{m-1}},$$

and similarly for $\mathfrak{P}_L{}^{r'}$. Since

$$t(F/K) = t(L/K) \leq \frac{ep}{p-1} - 1,$$

we can apply Lemma 1 to the extension F/K of degree p. Hence

$$1 + s_{m-1} \equiv 1 + s_{m-1}' = 1 + s_{m-1} + v \pmod{p},$$

and since $|v| \leq p - 1$, it follows that $v = 0$ as required.

Proof of Theorem 2. Writing $s = r - 1$, $s' = r' - 1$, we can assume that $0 \leq s, s' \leq p^m k - 1$. Interchanging r and r' if necessary, we assume also that $s' \geq s$.

Let C and $M = L^C$ be as in Proposition 3. By hypothesis, $\mathfrak{P}_L{}^r \cong \mathfrak{P}_L{}^{r'}$ as $\mathfrak{O}G$-modules, and taking C-fixed points, we obtain an isomorphism of

$\mathfrak{O}G_1$-modules

$$\mathfrak{P}_M{}^{1+[s/k]} = (\mathfrak{P}_L{}^r)^C \cong (\mathfrak{P}_L{}^{r'})^C = \mathfrak{P}_M{}^{1+[s'/k]}.$$

By Proposition 3*(ii)* and the hypothesis on $t(L/K)$, we can apply Theorem 1 to the non-cyclic extension M/K of degree p^m to deduce that $1 + [s/k] \equiv 1 + [s'/k] \pmod{p^m}$. The assumptions on s and s' ensure that this congruence is an equality, so

$$0 \leq s' - s \leq k - 1. \tag{7}$$

Now let $L_1 = L^{G_1}$. We may regard $\mathfrak{P}_L{}^r$ and $\mathfrak{P}_L{}^{r'}$ as $\mathfrak{O}G_1$-modules by restricting the action of G, and they are factor equivalent as such. We may also regard them as $\mathfrak{O}_{L_1}G_1$-modules, since G_1 acts trivially on L_1, and, as noted in the previous section, they are then still factor equivalent. Writing

$$s = s_0 + ps_1 + \cdots + p^{m-1}s_{m-1} + bp^m$$

$$s' = s'_0 + ps'_1 + \cdots + p^{m-1}s'_{m-1} + b'p^m$$

$$\text{with } 0 \leq s_i, s'_i \leq p-1 \text{ and } 0 \leq b \leq b' \leq k-1,$$

and applying Lemma 3 to the extension L/L_1 of degree p^m, we have $s'_i = s_i + v$ for $0 \leq i \leq m-1$, where $1 - p \leq v \leq p - 1$. Thus

$$s' - s = (1 + p + \cdots + p^{m-1})v + (b' - b)p^m,$$

and comparing with (7) we have

$$0 \leq \left(\frac{p^m - 1}{p - 1}\right) v + (b' - b)p^m \leq k - 1. \tag{8}$$

By hypothesis,

$$\frac{p^m - 1}{p - 1} > k - 1. \tag{9}$$

Thus if $b' = b$ we must have $v = 0$, and so $s' = s$, giving $r' = r$. On the other hand, if $b' - b \geq 1$ then, since $v \geq 1 - p$, (8) and (9) can only be satisfied

simultaneously by $b' - b = 1$, $v = 1 - p$. This value of v forces $s_i = p - 1$, $s_i' = 0$ for all i, so $s = p^m - 1 + (b' - 1)p^m$, $s' = b'p^m$. Thus, putting $a = b'$, we have $r = ap^m$, $r' = ap^m + 1$.

It only remains to show that $a \not\equiv 0 \pmod{k}$. Take H and F as in Proposition 3*(iii)*, so F/K is cyclic of degree p with Galois group $Q = G/H$, and

$$t(F/K) \leq \frac{ep}{p-1} - 1.$$

Taking H-fixed points in the original isomorphism of $\mathfrak{O}G$-modules, we obtain an isomorphism $(\mathfrak{P}_L{}^r)^H \cong (\mathfrak{P}_L{}^{r'})^H$ of $\mathfrak{O}Q$-modules. Applying Lemma 1 to F/K, we deduce

$$1 + \left[\frac{s}{p^{m-1}k}\right] \equiv 1 + \left[\frac{s'}{p^{m-1}k}\right] \pmod{p},$$

$$\text{i.e. } 1 + \left[\frac{ap}{k} - \frac{1}{p^{m-1}k}\right] \equiv 1 + \left[\frac{ap}{k}\right] \pmod{p},$$

which fails if $a \equiv 0 \pmod{k}$.

Proof of Theorem 3. Let a be the integer such that $t(L/K) \equiv a \pmod{p}$, $1 \leq a \leq p - 1$. Given r with $1 \leq r \leq p^m$, set

$$s = r - 1 = s_0 + ps_1 + \cdots + p^{m-1}s_{m-1} \quad \text{with } 0 \leq s_i \leq p - 1$$

as before, and define

$$I(r, L/K) = \{i : 0 \leq i \leq m - 2,\ s_i \geq a\}.$$

It is sufficient to prove the following implication:

$$\mathfrak{P}_L{}^r \cong \mathfrak{P}_L{}^{r'} \text{ as } \mathfrak{O}G\text{-modules} \Rightarrow \begin{cases} I(r, L/K) = I(r', L/K) \\ \text{and } s_{m-1} = s'_{m-1}. \end{cases} \tag{10}$$

We will prove (10) by induction on m. If $m = 1$ then $I(r, L/K) = I(r', L/K) = \emptyset$, and (10) holds by Lemma 1. Now assume that $m \geq 2$. Take

N and E as in Proposition 4(v) and set $J = G/N$. If $\mathfrak{P}_L{}^r \cong \mathfrak{P}_L{}^{r'}$ as $\mathfrak{O}G$-modules then taking N-fixed points gives the isomorphism of $\mathfrak{O}J$-modules

$$\mathfrak{P}_E{}^{1+[s/p]} \cong \mathfrak{P}_E{}^{1+[s'/p]}.$$

Since

$$\left(1 + \left[\frac{s}{p}\right]\right) - 1 = s_1 + ps_2 + \cdots + p^{m-2}s_{m-1}$$

and similarly for s', and since $t(E/K) = t(L/K) \equiv a \pmod{p}$, it follows from the induction hypothesis that

$$\{i : 1 \leq i \leq m-2,\ s_i \geq a\} = \{i : 1 \leq i \leq m-2,\ s_i' \geq a\}$$

and

$$s_{m-1} = s'_{m-1}.$$

Thus to complete the induction, it only remains to show that $s_0 \geq a$ if and only if $s_0' \geq a$. For this we compare the 0th Tate cohomology functor

$$\hat{H}^0(N, -) = \frac{(-)^N}{Tr_{L/E}(-)}$$

([14] VIII §1) on the $\mathfrak{O}N$-modules $\mathfrak{P}_L{}^r$ and $\mathfrak{P}_L{}^{r'}$. Here $Tr_{L/E}$ denotes the trace map from L to E. Let $n = t(L/E)$, so $n \equiv a \pmod{p}$ by Proposition 3(v). Then the different of L/E has valuation $v = (p-1)(n+1)$ ([14] IV Proposition 4) and

$$Tr_{L/E}(\mathfrak{P}_L{}^r) = \mathfrak{P}_E{}^{[(r+v)/p]}$$

([14] III Proposition 7). Hence

$$\hat{H}^0(N, \mathfrak{P}_L{}^r) \cong \frac{\mathfrak{P}_E{}^{[s/p]+1}}{\mathfrak{P}_E{}^{[(r+v)/p]}} \cong \frac{\mathfrak{O}_E}{\mathfrak{P}_E{}^{k(s)}},$$

where

$$k(s) = [(1 + s + v)/p] - [s/p] - 1.$$

If $\mathfrak{P}_L{}^r \cong \mathfrak{P}_L{}^{r'}$ as $\mathfrak{O}G$-modules then they are isomorphic as $\mathfrak{O}N$-modules, and we must have $k(s) = k(s')$. Since $v \equiv -1 - a \pmod{p}$, this simplifies to

$$\left[\frac{s_0 - a}{p}\right] = \left[\frac{s_0' - a}{p}\right].$$

Hence $s_0 \geq a$ if and only if $s_0' \geq a$, completing the induction.

References

[1] Bertrandias, F.: Sur les extensions cycliques de degré p^n d'un corps local. Acta Arith. **34**, 361-377 (1979)

[2] Bertrandias, F., Bertrandias, J-P. and Ferton, M-J,: Sur l'anneau des entiers d'une extension cyclique de degré premier d'un corps local. C. R. Acad. Sci. Paris **274**, A1388-A1391 (1972)

[3] Bertrandias, F. and Ferton, M-J.: Sur l'anneau des entiers d'une extension cyclique de degré premier d'un corps local. C. R. Acad. Sci. Paris **274**, A1330-A1333 (1972)

[4] Byott, N.P.: Some self-dual local rings of integers not free over their associated orders. to appear in Math. Proc. Camb. Phil. Soc. 1991

[5] Cassou-Noguès, Ph. and Taylor, M.J.: Elliptic functions and rings of integers. (Progress in Mathematics 66) Boston-Basel-Stuttgart: Birkhäuser 1987

[6] M.-J.Ferton, M-J.: Sur les idéaux d'une extension cyclique de degré premier d'un corps local. C. R. Acad. Sci. Paris **276**, A1483-A1486 (1973)

[7] Fröhlich, A.: Invariants for modules over commutative separable orders. Quart. J. Math. Oxford (2) **16**, 193-232 (1965)

[8] Fröhlich, A.: Local fields. in: Cassels, J.W.S. and Fröhlich, A. (eds.): Algebraic number theory. London: Academic Press 1967

[9] Fröhlich, A.: Module defect and factorisability. Illinois J. Math. **32**, 407-421 (1988)

[10] Fröhlich, A.: L-values at zero and multiplicative Galois module structure (also Galois Gauss sums and additive Galois module structure). J. reine angew. Math. **397**, 42-99 (1989)

[11] Jacobinski, H.: Über die Hauptordnung eines Körpers als Gruppenmodul. J. reine angew. Math. **213**, 151-164 (1963)

[12] MacKenzie, R.E. and Whaples, G.: Artin-Schreier equations in characteristic zero. Am. J. Math. **78**, 473-485 (1956)

[13] Larson, R.G. and Sweedler, M.E.: An associative orthogonal bilinear form for Hopf algebras. Am. J. Math. **91**, 75-94 (1969).

[14] Serre, J-P.: Local Fields. (Graduate Texts in Mathematics 67) Berlin-Heidelberg-New York: Springer 1979.

[15] Taylor, M.J.: Hopf structure and the Kummer theory of formal groups. J. reine angew. Math. **375/376**, 1-11 (1987)

[16] Ullom, S.: Integral normal bases in Galois extensions of local fields. Nagoya Math. J. **39**, 141-148 (1970)

Nigel Byott,
New College,
Oxford OX1 3BN,
U.K.

(Received December 3, 1990;
in revised form June 28, 1991)