

DUALITY THEOREMS IN THE MULTIVARIABLE IWASAWA  
THEORY OF NUMBER FIELDS

William G. McCallum  
January, 1996

**1. Introduction.**

Let  $K$  be a number field, let  $p$  be an odd prime, and let  $K_\infty/K$  be an extension containing all  $p$ -power roots of unity whose Galois group  $\Gamma$  is isomorphic to  $\mathbb{Z}_p^r$  for some  $r \in \mathbb{N}$ . Let  $\Lambda$  be the Iwasawa algebra  $\mathbb{Z}_p[[\Gamma]]$ . Let  $M_\infty$  be the maximal abelian pro- $p$ -extension of  $K_\infty$  unramified outside  $p$ , and let  $L_\infty$  be the maximal subextension of  $M_\infty$  in which all primes above  $p$  split completely. Let  $Y = \text{Gal}(M_\infty/K_\infty)$  and let  $X = \text{Gal}(L_\infty/K_\infty)$ . Let  $E = \varprojlim_F \mathcal{O}_F[1/p]^\times \otimes \mathbb{Z}_p$ , where the limit is taken with respect to the norm maps over all finite subextension  $F/K$  of  $K_\infty/K$ . Jannsen proved duality theorems relating the  $\Lambda$ -modules  $Y$ ,  $X$ , and  $E$  ([J2], Theorem 5.4).

Jannsen's proof uses the homotopy theory of  $\Lambda$ -modules. The aim of this paper is to give an explicit construction of the dualities in terms of the Kummer pairing, Tate duality, and a certain natural generalization of Iwasawa's construction of the adjoint module, obtained by computing Grothendieck's local cohomology groups using a particularly natural choice of regular sequences in  $\Lambda$ .

The simplest duality to describe is that between  $Y$  and  $E$ . Let  $F/K$  be a finite subextension of  $K_\infty/K$ , and denote by  $q(F)$  the order of the group of  $p$ -power roots of unity in  $F$ . Let  $\mathcal{O}'_F = \mathcal{O}_F[1/p]$ . Define a subgroup  $\mathfrak{M}_F$  of  $F^\times/F^{\times q(F)}$  by

$$\mathfrak{M}_F = \{x \in F^*/F^{*q(F)} : x\mathcal{O}'_F \text{ is the } q(F)\text{-th power of a fractional ideal in } \mathcal{O}'_F\}.$$

Let  $Y_F$  be the Galois group of the maximal abelian pro- $p$ -extension of  $F$  unramified outside  $p$ . Consider the Kummer pairing

$$\mathfrak{M}_F \times Y_F \rightarrow \mu_{q(F)}.$$

Since  $E = \varprojlim_F \mathfrak{M}_F$  and  $Y = \varprojlim_F Y_F$ , one obtains in a natural way a  $\Lambda$ -linear pairing between  $E$  and  $Y$  into  $\Lambda(1) = \Lambda \otimes_{\mathbb{Z}_p} \mathbb{Z}_p(1)$  (average the Kummer pairings at finite levels over the group ring). Hence there is a natural map

$$E \rightarrow \text{Hom}_\Lambda(Y, \Lambda(1)).$$

**THEOREM A.** *If  $r > 2$ , the pairing between  $E$  and  $Y$  induces an isomorphism*

$$E \simeq \text{Hom}_\Lambda(Y, \Lambda(1)).$$

---

This research was supported in part by National Science Foundation grant DMS-9302976.

If  $r = 1$  there is an exact sequence

$$0 \rightarrow \mathbb{Z}_p(1) \rightarrow E \rightarrow \mathrm{Hom}_\Lambda(Y, \Lambda(1)) \rightarrow 0,$$

and if  $r = 2$  there is an exact sequence

$$0 \rightarrow E \rightarrow \mathrm{Hom}_\Lambda(Y, \Lambda(1)) \rightarrow \mathbb{Z}_p(1).$$

A reflexive  $\Lambda$ -module is one for which the canonical map to its double  $\Lambda$ -dual is an isomorphism. Reflexive modules play a fundamental role in the structure theory of  $\Lambda$ -modules. Since the dual is always isomorphic to the triple dual, one obtains the following corollary to Theorem A.

**COROLLARY.** *If  $r > 2$ , then  $E$  is a reflexive  $\Lambda$ -module.*

In addition to the Hom duality between  $E$  and  $Y$ , there is an Ext duality between  $X$  and  $Y$ . In order to state this duality succinctly, we use Galois cohomology to define Iwasawa modules which are closely related to  $E$ ,  $Y$ , and  $X$ .

Given a compact or discrete  $\mathbb{Z}_p$ -module  $M$  on which  $\mathrm{Gal}(\overline{K}/F)$  acts continuously, we let  $H^i(\mathcal{O}'_F, M)$  denote the group of continuous Galois cohomology classes unramified outside  $p$ . Define Iwasawa modules

$$H_\infty^i(\mathbb{Z}_p(1)) = \varprojlim_F H^i(\mathcal{O}'_F, \mathbb{Z}_p(1))$$

and

$$Y_\infty^i(\mathbb{Z}_p(1)) = H^i(\mathcal{O}'_\infty, \mathbb{Q}_p/\mathbb{Z}_p(1))^\wedge,$$

where the wedge denotes the Pontriagin dual. Then

$$H_\infty^i(\mathbb{Z}_p(1)) = \begin{cases} 0 & i \neq 1, 2, \\ E & i = 1, \end{cases}$$

and for the case  $i = 2$  we have an exact sequence

$$0 \rightarrow X \rightarrow H_\infty^2(\mathbb{Z}_p(1)) \rightarrow \sum_{\mathfrak{p}|p} \mathbb{Z}_p \rightarrow \mathbb{Z}_p \rightarrow 0,$$

where the sum is over all primes of  $K_\infty$  dividing  $p$  (Lemma 4). Moreover,

$$Y^i(\mathbb{Z}_p(1)) = \begin{cases} 0 & i \neq 0, 1, \\ Y(-1) & i = 1, \\ \mathbb{Z}_p(-1) & i = 0. \end{cases}$$

**THEOREM B.** *If  $r \neq 2, 3$ , there is an isomorphism*

$$H_\infty^2(\mathbb{Z}_p(1)) \simeq \text{Ext}^1(Y^1(\mathbb{Z}_p(1)), \Lambda).$$

*If  $r = 2$  there is an exact sequence*

$$\mathbb{Z}_p(1) \rightarrow H_\infty^2(\mathbb{Z}_p(1)) \rightarrow \text{Ext}^1(Y^1(\mathbb{Z}_p(1)), \Lambda) \rightarrow 0,$$

*and if  $r = 3$ , there is an exact sequence*

$$0 \rightarrow H_\infty^2(\mathbb{Z}_p(1)) \rightarrow \text{Ext}^1(Y^1(\mathbb{Z}_p(1)), \Lambda) \rightarrow \mathbb{Z}_p(1).$$

Perrin-Riou [P-R] proved a similar theorem up to pseudo-isomorphism in the case  $r = 1$ , for arbitrary  $p$ -adic representations. Curiously, her map goes in the opposite direction to ours; the speculations at the end of this introduction provide a possible explanation for this. Billot [B] also proved a similar theorem (up to pseudo-isomorphism) in the case  $r = 2$ .

Theorems A and B may be viewed as special cases of a general duality theorem for  $p$ -adic representations. Let  $M = \mathbb{Z}_p(1)$ . Then Theorems A and B imply that there are exact sequences

$$0 \rightarrow \text{Ext}^1(Y^0(M), \Lambda) \rightarrow H_\infty^1(M) \rightarrow \text{Ext}^0(Y^1(M), \Lambda) \rightarrow \text{Ext}^2(Y^0(M), \Lambda)$$

and

$$\text{Ext}^2(Y^0(M), \Lambda) \rightarrow H_\infty^2 \rightarrow \text{Ext}^1(Y^1(M), \Lambda) \rightarrow \text{Ext}^3(Y^0(M), \Lambda) \rightarrow 0.$$

(The point is that  $Y^0(M) = \mathbb{Z}_p(-1)$ , and the  $\text{Ext}_\Lambda^i(\mathbb{Z}_p(-1), \Lambda) = \mathbb{Z}_p(1)$  if  $i = r - 1$ , and is zero otherwise.) These exact sequences appear to be pieces of a spectral sequence

$$\text{Ext}_\Lambda^i(Y^j(M), \Lambda) \Rightarrow H_\infty^{i+j}(M).$$

For  $r > 3$ ,  $i > 1$  the sequence predicts  $\text{Ext}_\Lambda^i(Y^1(\mathbb{Z}_p(1)), \Lambda) = 0$ , excepting  $i = r - 2$ , in which case it predicts  $\text{Ext}_\Lambda^{r-2}(Y^1(\mathbb{Z}_p(1)), \Lambda) = \text{Ext}_\Lambda^r(Y^0(\mathbb{Z}_p(1)), \Lambda) = \mathbb{Z}_p(1)$ . This prediction turns out to be correct; it follows easily from a general structure theorem for  $Y$  proved independently by Jannsen and Nguyen-Quang-Do, as we shall see in Sect. 7. I have been informed that Jannsen has described this putative spectral sequence in a talk, and that it can be derived using his methods.

### **Acknowledgements.**

I would like to thank John Coates, Ralph Greenberg, Uwe Jannsen, Thong Nguyen-Quang-Do, Bernadette Perrin-Riou, and Kay Wingberg for useful comments and conversations during the course of this work. Parts of this work were done while I was a guest at the Institut des Hautes Etudes Scientifiques, and at the Institute for Advanced Study. I would like to thank them for their hospitality.

## 2. Calculation of Ext Groups.

Let  $p$  be a prime number, and let  $\Gamma$  be a group isomorphic to  $\mathbb{Z}_p^r$  for some positive integer  $r$ . Let  $\Lambda$  be the Iwasawa algebra  $\mathbb{Z}_p[[G]]$ . First, we recall, for the ring  $\Lambda$ , Grothendieck's theory of local cohomology groups  $[G]$  and how it may be used to calculate Ext groups. A good general reference for this theory is [B-H].

Let  $N = r + 1$ , the dimension of  $\Lambda$ . Let  $\mathfrak{m}$  be the maximal ideal of  $\Lambda$ . Let  $\mathbf{x} = x_1, \dots, x_N$  be a finite sequence in  $\Lambda$  that generates an  $\mathfrak{m}$ -primary ideal. The Koszul complex

$$0 \xrightarrow{d} K_N(\mathbf{x}) \xrightarrow{d} K_{N-1}(\mathbf{x}) \xrightarrow{d} \dots \xrightarrow{d} K_1(\mathbf{x}) \xrightarrow{d} K_0(\mathbf{x}) \rightarrow 0$$

is defined as follows. Let  $\Lambda^N$  be the free  $\Lambda$ -module with basis  $\{e_i : 1 \leq i \leq N\}$ . Then

$$K_i(\mathbf{x}) = \bigwedge^i \Lambda^N$$

and

$$d(e_{j_1} \wedge \dots \wedge e_{j_i}) = \sum_{s=1}^i (-1)^{s-1} x_{j_s} e_{j_1} \wedge \dots \wedge \hat{e}_{j_s} \wedge \dots \wedge e_{j_i},$$

where the hat indicates that a term is omitted. If  $\mathbf{x}$  is a regular sequence, then the Koszul complex is a free resolution of  $\Lambda/(\mathbf{x})$  ([Ma], Theorem 43).

Given a finitely generated  $\Lambda$ -module  $X$ , we define a complex  $K^*(\mathbf{x}, X)$  by

$$K^*(\mathbf{x}, X) = \text{Hom}_\Lambda(K_*(\mathbf{x}), X)$$

and define  $H^*(\mathbf{x}, X)$  to be the cohomology of this complex.

Now let  $(\mathbf{x}_n)$  be a sequence of sequences

$$\mathbf{x}_n = (x_{n,1}, \dots, x_{n,N}),$$

such that  $x_{n,i} \mid x_{m,i}$ ,  $n \leq m$ ,  $1 \leq i \leq N$ . If  $n \leq m$ , there is a natural map of complexes

$$K(\mathbf{x}_n) \rightarrow K(\mathbf{x}_m),$$

which multiplies  $e_{j_1} \wedge \dots \wedge e_{j_i}$  by

$$\begin{pmatrix} x_{m,j_1} \\ x_{n,j_1} \end{pmatrix} \dots \begin{pmatrix} x_{m,j_i} \\ x_{n,j_i} \end{pmatrix}.$$

**THEOREM 1.** *Suppose that for each positive integer  $n$  we have a sequence  $\mathbf{x}_n = x_{n,1}, \dots, x_{n,N}$  generating an  $\mathfrak{m}$ -primary ideal, such that  $x_{n,i} \mid x_{m,i}$ ,  $n \leq m$ ,  $1 \leq i \leq N$ , and such that for each  $k \in \mathbb{N}$  there are  $i, j \in \mathbb{N}$  such that  $(\mathbf{x}_i) \subset \mathfrak{m}^k$*

and  $\mathfrak{m}^j \subset (\mathbf{x}_k)$ . Then there is an isomorphism of functors of finitely generated  $\Lambda$ -modules

$$\mathrm{Ext}_{\Lambda}^{N-i}(\cdot, \Lambda) \simeq \mathrm{Hom}_{\mathbb{Z}_p}(\varinjlim_n H^i(\mathbf{x}_n, \cdot), \mathbb{Q}/\mathbb{Z}).$$

*Proof:* For a finitely generated  $\Lambda$ -module  $X$ ,

$$\varinjlim_n H^i(\mathbf{x}_n, X)$$

is the local cohomology group  $H_{\mathfrak{m}}^i(X)$  defined by Grothendieck. This is shown in Sect. 3.5 of [B-H] for the case where  $\mathbf{x} = x_1, \dots, x_N$  is a sequence in  $\Lambda$  that generates an  $\mathfrak{m}$ -primary ideal and  $x_{n,i} = x_i^n$ . The construction there generalizes easily to our situation. The statement of our theorem is then simply the version of Grothendieck's duality theorem suggested by Exercise 3.5.14 of [B-H]. ■

Now let  $I \subset \Lambda$  be the augmentation ideal, let  $g_1, \dots, g_r$  be a set of topological generators for  $\Gamma$ , and let  $(T_1, \dots, T_r)$  be the corresponding set of generators for  $I$  ( $g_i = 1 + T_i$ ). Let

$$\omega_n(T_i) = (1 + T_i)^{p^n} - 1, \quad n \geq 0.$$

We will apply Theorem 1 using

$$\mathbf{x}_n = (p^n, \omega_n(T_1), \dots, \omega_n(T_r)).$$

One reason for choosing this sequence is that it is easy to see the relation between  $\mathrm{Ext}^1$  and Iwasawa's definition of the adjoint module. From the definition,

$$H^r(\mathbf{x}_n, X) = \frac{\{(x_0, x_1, \dots, x_r) \in X^{r+1} : p^n x_0 + \omega_n(T_1)x_1 + \dots + \omega_n(T_r)x_r = 0\}}{\{\text{obvious relations}\}},$$

where the obvious relations are those generated by elements of the form

$$\begin{aligned} (\omega_n(T_i)y, 0, \dots, 0, -p^n y, 0, \dots, 0) \quad \text{and} \\ (0, \dots, 0, \omega_n(T_j)y, 0, \dots, 0, -\omega_n(T_i)y, 0, \dots, 0). \end{aligned}$$

Let

$$\mathbf{x}'_n = (\omega_n(T_1), \dots, \omega_n(T_r)).$$

Then there is a natural short exact sequence

$$(1) \quad 0 \rightarrow H^{i-1}(\mathbf{x}'_n, X)/p^n \rightarrow H^i(\mathbf{x}_n, X) \rightarrow H^i(\mathbf{x}'_n, X)[p^n] \rightarrow 0.$$

In the case  $i = r$ , the map on the right is induced by  $(y_0, \dots, y_r) \mapsto y_0$ . Note that  $H^r(\mathbf{x}'_n, X) = X/(\omega_n(T_1), \dots, \omega_n(T_r))$ . Define a functor

$$E(X) = \mathrm{Hom}_{\mathbb{Z}_p}(\varinjlim_n H^r(\mathbf{x}'_n, X), \mathbb{Q}_p/\mathbb{Z}_p).$$

In the case where  $r = 1$  and  $X_n$  is torsion,  $E(X)$  is Iwasawa's original definition of the adjoint module of  $X$ .

**PROPOSITION 2.** *There is a functorial injective map  $E(X) \rightarrow \text{Ext}_\Lambda^1(X, \Lambda)$ . This map is an isomorphism if  $X_n$  is finite for all sufficiently large  $n$ .*

*Proof:* The first statement follows on taking the direct limit of the sequence (1) with  $i = r$  and applying Theorem 1. The cokernel is dual to

$$\varinjlim H^{r-1}(\mathbf{x}'_n, X) \otimes \mathbb{Q}_p/\mathbb{Z}_p,$$

which is zero if  $H^{r-1}(\mathbf{x}'_n, X)$  is  $\mathbb{Z}_p$ -torsion for large enough  $n$ . Thus the second statement follows from the following lemma.

**LEMMA 3.** *If  $X$  is a finitely generated  $\Lambda$ -module, and if  $X_n = H^r(\mathbf{x}'_n, X)$  is torsion, then  $H^{r-1}(\mathbf{x}'_n, X)$  is torsion.*

*Proof:* First, it suffices to prove the lemma for  $n = 1$ , since  $\mathbf{x}'_n$  is just  $\mathbf{x}'_1$  for the algebra  $\mathbb{Z}_p[[\omega_n(T_1), \dots, \omega_n(T_r)]]$ . Let  $\mathbf{x}' = \mathbf{x}'_1$ . First suppose that  $X$  is cyclic, i.e.,

$$X = \Lambda/\mathfrak{a},$$

for some ideal  $\mathfrak{a} \subset \Lambda$ . Let  $\mathfrak{a}(0) \subset \mathbb{Z}_p$  be the ideal generated by  $f(0)$  for  $f \in \mathfrak{a}$ . Then

$$H^r(\mathbf{x}', X) = X/(T_1, \dots, T_r)X = \mathbb{Z}_p/\mathfrak{a}(0),$$

and so by hypothesis there exists  $f \in \mathfrak{a}$  such that  $f(0) \neq 0$ . Since  $f$  annihilates  $X$ ,  $f_*$  annihilates  $H^{r-1}(\mathbf{x}', X)$ . But  $f_*$  is just multiplication by  $f(0)$ .

We finish the proof with an induction on the number of cyclic factors in  $X$ . Let  $k$  be a positive integer, and suppose that the proposition is true for all  $\Lambda$ -modules that have a filtration of length less than  $k$ , the factors of which are cyclic. Let  $X$  be a  $\Lambda$ -module with such a filtration of length  $k$ , and write

$$0 \rightarrow Z \rightarrow X \rightarrow Y \rightarrow 0$$

where  $Z$  and  $Y$  have filtrations with cyclic factors of length less than  $k$ . We have an exact sequence

$$\begin{aligned} H^{r-1}(\mathbf{x}', Z) &\rightarrow H^{r-1}(\mathbf{x}', X) \rightarrow H^{r-1}(\mathbf{x}', Y) \rightarrow \\ H^r(\mathbf{x}', Z) &\rightarrow H^r(\mathbf{x}', X) \rightarrow H^r(\mathbf{x}', Y) \rightarrow 0. \end{aligned}$$

If  $H^r(\mathbf{x}', X)$  is torsion, then so is  $H^r(\mathbf{x}', Y)$ ; hence, by induction,  $H^{r-1}(\mathbf{x}', Y)$  is torsion, and thus so is  $H^{r-1}(\mathbf{x}', Z)$ . Again by induction we conclude that  $H^{r-1}(\mathbf{x}', Z)$  is torsion, and so finally is  $H^{r-1}(\mathbf{x}', X)$ . ■

■

Another reason for choosing the sequence  $\mathbf{x}_n$  in computing local cohomology groups is that it is easy to see the connection with certain groups defined by Tate in terms of galois cohomology. Let

$$H_\omega^i(X) = \varinjlim H^i(\mathbf{x}'_n, X).$$

Taking the direct limit of the sequence (1), we get

$$0 \rightarrow H_\omega^{i-1}(X) \otimes \mathbb{Q}_p/\mathbb{Z}_p \rightarrow H_m^i(X) \rightarrow H_\omega^i(X)[p^\infty] \rightarrow 0.$$

It is not hard to see that the  $H_\omega^i(X)$  is the same as Tate's group  $D_{r-i}(X^\wedge)$  (see [J2], Sect. 2, for the definition). Grothendieck's duality theorem then identifies this exact sequence with the one in 2.1a of [J2].

### 3. Kummer Theory.

As in the introduction, we assume

$$p \text{ is odd and } K_\infty \text{ contains all } p\text{-power roots of unity.}$$

Note that this implies that  $K$  contains the  $p$ -th roots of unity, and hence also that  $K$  is totally complex. Recall that for any intermediate field  $K \subset F \subset K_\infty$ ,  $q(F)$  is the order of the group of  $p$ -power roots of unity in  $F$ , and

$$\mathfrak{M}_F = \{x \in F^*/F^{*q(F)} : x\mathcal{O}'_F \text{ is the } q(F)\text{-th power of a fractional ideal in } \mathcal{O}'_F\}.$$

Let  $M_F$  be the extension of  $F$  obtained by adjoining all  $q(F)$ -th roots of elements of  $\mathfrak{M}_F$ . Then  $M_F$  is the maximal abelian extension of  $F$  of exponent  $q(F)$  unramified outside the primes above  $p$ . Thus  $M_\infty$  is the compositum of  $M_F$  as  $F$  ranges over all finite subextensions of  $K_\infty/K$ , and  $Y = \text{Gal}(M_\infty/K_\infty) = \varinjlim_F \text{Gal}(M_F/F)$ .

Now, Kummer theory yields a non-degenerate pairing

$$\text{Gal}(M_F/F) \times \mathfrak{M}_F \rightarrow \mu_{q(F)}.$$

The direct limit  $\varinjlim_F \mathfrak{M}_F$  may be identified with a subgroup  $\mathfrak{M}$  of  $K_\infty^\times \otimes \mathbb{Q}_p/\mathbb{Z}_p$ , and on taking the limit we get a pairing

$$Y \times \mathfrak{M} \rightarrow \mathbb{Q}_p/\mathbb{Z}_p(1)$$

which sets the two groups in Pontriagin duality.

We have a similar theory for  $L_\infty$ . Let  $S_F$  be the set of primes of  $\mathcal{O}_F$  above  $p$ . Define a subgroup  $\mathfrak{L}_F$  of  $\mathfrak{M}_F$  by

$$\mathfrak{L}_F = \{x \in \mathfrak{M}_F : x_{\mathfrak{p}} \in F_{\mathfrak{p}}^{\times q(F)} \text{ for all primes } \mathfrak{p} \in S_F\}.$$

Let  $L_F$  be the extension of  $F$  obtained by adjoining all  $q(F)$ -th roots of all elements of  $\mathfrak{L}_F$ . Then  $L_\infty$  is the compositum of  $L_F$  as  $F$  ranges over all finite subextensions of  $K_\infty$ ,  $X = \text{Gal}(L_\infty/K_\infty)$ , and we have as before non-degenerate pairings

$$(2) \quad \text{Gal}(L_F/F) \times \mathfrak{L}_F \rightarrow \mu_{q(F)}$$

and

$$X \times \mathfrak{L} \rightarrow \mathbb{Q}_p/\mathbb{Z}_p(1),$$

where  $\mathfrak{L} = \varinjlim_F \mathfrak{L}_F$ .

*Remark.* We note that  $\mathfrak{M}_F$  and  $\mathfrak{L}_F$  may also be represented as Galois cohomology groups. For any continuous  $\text{Gal}(\bar{F}/F)$ -module  $M$ , denote by  $H^i(\mathcal{O}'_F, M)$  the subgroup of  $H^i(K, M)$  consisting of cohomology classes unramified outside all primes above  $p$ , and define  $\text{III}^i(\mathcal{O}'_F, M)$  to be the kernel of

$$H^i(\mathcal{O}'_F, M) \rightarrow \sum_{\mathfrak{p} \in S_F} H^i(F_{\mathfrak{p}}, M).$$

Then there are canonical isomorphisms

$$H^1(\mathcal{O}'_F, \mu_{q(F)}) \simeq \mathfrak{M}_F$$

and

$$(3) \quad \text{III}^1(\mathcal{O}'_F, \mu_{q(F)}) \simeq \mathfrak{L}_F.$$

LEMMA 4. *There is an exact sequence*

$$0 \rightarrow X \rightarrow H_\infty^2(\mathbb{Z}_p(1)) \rightarrow \sum_{\mathfrak{p} \in S_{K_\infty}} \mathbb{Z}_p \rightarrow \mathbb{Z}_p \rightarrow 0.$$

*Proof:* Using (2), (3), and Poitou-Tate duality, we have

$$\begin{aligned} \text{Gal}(L_F/F) &= \text{Hom}_{\mathbb{Z}_p}(\mathfrak{L}_F, \mathbb{Q}_p/\mathbb{Z}_p(1)) = \\ &= \text{Hom}_{\mathbb{Z}_p}(\text{III}^1(\mathcal{O}'_F, \mu_{q(F)}), \mathbb{Q}_p/\mathbb{Z}_p(1)) = \text{III}^2(\mathcal{O}'_F, \mu_{q(F)}). \end{aligned}$$

Thus the sequence we want is the inverse limit of the sequence

$$0 \rightarrow \text{III}^2(\mathcal{O}'_F, \mu_{q(F)}) \rightarrow H^2(\mathcal{O}'_F, \mu_{q(F)}) \rightarrow \sum_{\mathfrak{p} \in S_F} H^2(F_{\mathfrak{p}}, \mu_{q(F)}) \rightarrow \mathbb{Z}/q(F)\mathbb{Z} \rightarrow 0,$$

where the last map is the sum of the invariants. ■



#### 4. The Hom Duality.

We will apply the general theory of Sect. 2 to the case  $\Gamma = \text{Gal}(K_\infty/K)$  and the  $\Lambda$ -modules  $X$  and  $Y$  defined in the introduction. Choose a set of generators  $g_1, \dots, g_r$  for  $\text{Gal}(K_\infty/K)$ , and let  $T_i = g_i - 1$  be the corresponding generators for the augmentation ideal  $I \subset \Lambda$ . For each natural number  $n$ , let  $\Gamma_n$  be the subgroup generated by  $g_1^{p^n}, \dots, g_r^{p^n}$ , and let  $K_n$  be the fixed field of  $\Gamma_n$ . We will abbreviate the notation of the previous section by writing  $\mathcal{O}_{K_n} = \mathcal{O}_n$  and so on.

Given a compatible system of  $\text{Gal}(F/K)$ -modules  $Z_F$  and the corresponding  $\Lambda$ -module  $Z = \varprojlim_F Z_F$ , we have natural projections  $Z \rightarrow Z_n = Z_{K_n}$  which factor through  $Z/(\omega_n(T_1), \dots, \omega_n(T_r))$ , and hence we obtain maps

$$H^{r+1}(\mathbf{x}_n, Z) \rightarrow Z_n/p^n Z_n.$$

Let  $E_F = \mathcal{O}_F^{\times} \otimes \mathbb{Z}_p$ , and let  $Y_F$  be the Galois group of the maximal abelian pro- $p$ -extension of  $F$  unramified outside  $p$ . Then  $E = \varprojlim_F E_F$ , and  $Y = \varprojlim Y_F$ . So we have natural maps

$$H^{r+1}(\mathbf{x}_n, E) \rightarrow E_n/p^n E_n \subset \mathfrak{M}_n[p^n]$$

and

$$H^{r+1}(\mathbf{x}_n, Y) \rightarrow Y_n/p^n.$$

Thus the Kummer pairing of the previous section yields a natural pairing

$$\langle \cdot, \cdot \rangle_n : H^{r+1}(\mathbf{x}_n, E) \times H^{r+1}(\mathbf{x}_n, Y) \rightarrow \mu_{p^n}.$$

Hence, using Theorem 1, we obtain a natural pairing of  $\Lambda$ -modules

$$(4) \quad \langle \cdot, \cdot \rangle : E \times Y \rightarrow \Lambda(1).$$

Explicitly, this pairing is defined by the formula

$$\langle e, y \rangle \equiv \sum_{\sigma \in \text{Gal}(K_n/K)} \langle e_n, y_n^\sigma \rangle_n \sigma^{-1} \pmod{(\omega_n(T_1), \dots, \omega_n(T_r))}.$$

**THEOREM 5.** *The map*

$$e_1 : E \rightarrow \text{Hom}_\Lambda(Y, \Lambda(1)),$$

*induced by the pairing (4), is an isomorphism if  $r > 2$ . If  $r = 1$  there is an exact sequence*

$$0 \rightarrow \mathbb{Z}_p(1) \rightarrow E \xrightarrow{e_1} \text{Hom}_\Lambda(Y, \Lambda(1)) \rightarrow 0,$$

*and if  $r = 2$  there is an exact sequence*

$$0 \rightarrow E \xrightarrow{e_1} \text{Hom}_\Lambda(Y, \Lambda(1)) \rightarrow \mathbb{Z}_p(1).$$

*Proof:* Let  $\iota_n$  denote the isomorphism

$$(5) \quad H^1(\mathcal{O}'_\infty, \mu_{p^n}) \xrightarrow{\iota_n} H^1(\mathcal{O}'_\infty, \mathbb{Q}_p/\mathbb{Z}_p(1))[p^n]$$

coming from the Kummer sequence

$$(6) \quad 0 \rightarrow \mu_{p^n} \rightarrow \mathbb{Q}_p/\mathbb{Z}_p(1) \xrightarrow{p^n} \mathbb{Q}_p/\mathbb{Z}_p(1) \rightarrow 0.$$

Define

$$(7) \quad E_n \rightarrow H^{r+1}(\mathbf{x}_n, Y)^\wedge(1)$$

to be the composition

$$E_n \rightarrow H^1(\mathcal{O}'_n, \mu_{p^n}) \xrightarrow{\text{res}} H^1(\mathcal{O}'_\infty, \mu_{p^n})^{\Gamma_n} \xrightarrow{\iota_n^{\Gamma_n}} H^1(\mathcal{O}'_\infty, \mathbb{Q}_p/\mathbb{Z}_p(1))^{\Gamma_n}[p^n] = H^{r+1}(\mathbf{x}_n, Y)^\wedge(1).$$

Here the last equality may be seen from the following series of transformations:

$$\begin{aligned} H^{r+1}(\mathbf{x}_n, Y)^\wedge &= (H^1(\mathcal{O}'_\infty, \mathbb{Q}_p/\mathbb{Z}_p)^\wedge / (\mathbf{x}_n))^\wedge \\ &= (H^1(\mathcal{O}'_\infty, \mathbb{Q}_p/\mathbb{Z}_p)^\wedge / (\mathbf{x}'_n, p^n))^\wedge \\ &= H^1(\mathcal{O}'_\infty, \mathbb{Q}_p/\mathbb{Z}_p)^{\Gamma_n}[p^n]^\wedge \\ &= H^1(\mathcal{O}'_\infty, \mathbb{Q}_p/\mathbb{Z}_p)^{\Gamma_n}[p^n]. \end{aligned}$$

Twisting both sides by  $\mu_{p^n}$  (which is fixed by  $\Gamma_n$ ), we get the required isomorphism.

In the inverse limit the map (7) yields a map  $E \rightarrow \text{Hom}_\Lambda(Y, \Lambda(1))$ , and it is clear from the definitions that this map is  $e_1$ . Further, the first map in the composition yields an isomorphism  $E \simeq \varprojlim_n H^1(\mathcal{O}'_n, \mu_{p^n})$  in the limit, and  $\iota_n$  is an isomorphism. Thus it remains to consider the kernel and cokernel of restriction. The kernel is  $H^1(K_\infty/K_n, \mu_{p^n})$  and the cokernel injects into  $H^2(K_\infty/K_n, \mu_{p^n})$ . Thus the statements about the cokernel and kernel of  $e_1$  follow from the following lemma.

**LEMMA 6.** *Let  $\Gamma$  be an abelian pro- $p$ -group isomorphic to  $\mathbb{Z}_p^r$ , and let  $M$  be a finitely generated  $\mathbb{Z}_p$ -module with a continuous action of  $\Gamma$ . Then*

$$\varprojlim_n H^i(p^n \Gamma, M/p^n M) \simeq \begin{cases} M & i = r \\ 0 & i \neq r \end{cases}$$

*Proof:* The group  $\Gamma$  is a (trivial example of) a Poincaré group of cohomological dimension  $n$ , with dualizing module  $\mathbb{Q}_p/\mathbb{Z}_p$  (see [S], Chapter 4). Thus the inverse limit in question is the Pontriagin dual of

$$\varinjlim_n H^{r-i}(p^n \Gamma, \text{Hom}(M/p^n M, \mathbb{Q}_p/\mathbb{Z}_p)).$$

Here the direct limit is with respect to the restriction maps, thus it is zero unless  $i = r$ , and in that case it is  $\text{Hom}(M, \mathbb{Q}_p/\mathbb{Z}_p)$ . ■

■

## 5. Class Field Theory and the Leopoldt Kernel.

Much of the technical difficulty in proving Theorem B comes from the need to take account of the possible failure of Leopoldt's conjecture. In this section we review some basic facts about class field theory and Leopoldt's conjecture.

Let  $K$  be a number field, let  $S$  be a finite set of places of  $K$ , containing the infinite places, let  $\Omega/K$  be the maximal extension of  $K$  unramified outside  $S$ , and let  $G = \text{Gal}(\Omega/K)$ . For an intermediate field  $K \subset F \subset \Omega$ , let  $\mathbb{I}_F$  be the idèle group of  $K$ ,  $\mathbb{I}_{S,F}$  the subgroup of idèles supported on places above  $S$ ,  $F_S$  the ring of  $S$ -integers in  $F$ , and let  $C_{S,F} = \mathbb{I}_{S,F}/F_S^\times$ . We denote  $C_{S,\Omega}$  simply by  $C_S$ . Define

$$C_S(F) = C_S^{\text{Gal}(\Omega/F)}.$$

Let  $U_{S,F}$  be the unit idèles supported outside  $S$ . Then  $C_S(K) = \mathbb{I}_K/K^\times U_{S,K}$  ([Mi] Lemma 4.4). Let  $D_S(K)$  be the connected component of the identity in  $C_S(K)$ . Then  $D_S(K)$  is a) the divisible subgroup of  $C_S(K)$ , b) the closure in  $C_S(K)$  of the idèles supported on the infinite places, and c) the universal norm subgroup from  $\Omega$ , i.e., the intersection of the groups  $N_{F/K}C_S(F)$  as  $F$  ranges over all finite subextensions of  $\Omega/K$ . (See [AT], IX, and [Mi], I.4). The reciprocity map gives an exact sequence

$$(8) \quad 0 \rightarrow D_S(K) \rightarrow C_S(K) \rightarrow G^{\text{ab}} \rightarrow 0.$$

Let  $M$  be a finitely generated  $G$ -module. Then cup product into  $H^2(G, C_S) = \mathbb{Q}/\mathbb{Z}$  induces an isomorphism

$$(9) \quad \hat{H}^i(\text{Hom}(M, C_S)) \simeq \hat{H}^{2-i}(G, M)^\wedge, \quad i \leq 0.$$

Tate [Ta] showed this for torsion modules, and Uchida generalized it to finitely generated modules. For a proof, see [U], Theorem 1.

Now, let  $p$  be an odd prime, let  $S_p = S_{K,p}$  be the set of primes of  $K$  above  $p$ , and  $S = S_p \cup S_\infty$ . To construct the Ext duality in Theorem B, we will need a concrete representation of  $H^2(G, \mathbb{Z}/p^n\mathbb{Z})^\wedge$ . By (9), we have a surjective map

$$C_S(K)[p^n] \twoheadrightarrow H^2(G, \mathbb{Z}/p^n\mathbb{Z})^\wedge,$$

whose kernel is the intersection of the norm of  $C_S(F)[p^n]$  as  $F/K$  ranges over all subextensions of  $\Omega/K$ . Now, the universal norm subgroup of  $C_S(K)$  is  $D_S(K)$ , thus the universal norm subgroup of  $C_S(K)[p^n]$  is contained in  $D_S(K)[p^n]$ . Further, since  $D_S(K)$  is the divisible subgroup of  $C_S(K)$ ,  $D_S(K)[p^n] = T_p(C_S(K))/p^n$ . Here  $T_p(A)$  for an abelian group  $A$  is the Tate module  $\varprojlim A[p^n]$ . So our next step is to identify the infinitely  $p$ -divisible elements in  $C_S(K)$ .

The answer is complicated by the possible failure of Leopoldt's conjecture. We define the Leopoldt kernel,  $\mathcal{E} = \mathcal{E}_K$ , to be the kernel of the map

$$\mathcal{O}_K[1/p]^\times \otimes \mathbb{Z}_p \rightarrow \prod_{v \in S_{K,p}} K_v^\times \otimes \mathbb{Z}_p.$$

Leopoldt's conjecture is that  $\mathcal{E} = 0$ .

LEMMA 7. We have an exact sequence

$$0 \rightarrow \prod_{v \in S_\infty} T_p(K_v) \rightarrow T_p(C_{S,K}) \rightarrow \mathcal{E} \rightarrow 0.$$

*Proof:* The exact sequence comes from taking  $T_p$  of

$$0 \rightarrow \prod_{v \in S_\infty} K_v^\times \rightarrow C_{S,K} \rightarrow C_{S_p,K} \rightarrow 0,$$

which yields an exact sequence of Tate modules because  $K_v$  is  $p$ -divisible if  $v \in S_\infty$ . We must show that

$$T_p(C_{S_p,K}) = \mathcal{E}.$$

An element of the group on the left may be represented by a compatible system of idèles  $(x_n)$ ,  $n \in \mathbb{N}$ , such that

$$(10) \quad x_n^{p^n} = u_n z_n$$

$$(11) \quad x_m^{p^{m-n}} = u_{m,n} z_{m,n} x_n \quad m > n$$

where the  $u$ 's are in  $U_{K,S_p}$  and the  $z$ 's are in  $K^\times$ . Let  $[x_n]$  be the class of  $x_n$  in the ideal class group of  $K$ . Then  $[x]$  is  $p$ -divisible by (10), hence is zero, i.e.,  $x_n$  is a unit idèle times a principal idèle. Thus, replacing  $x_n$  with an equivalent idèle modulo  $K^\times U_{S,K}$ , we may assume  $x_n$  is supported on the places in  $S_p$ . It follows from (10) and (11) that  $z_n$  and  $z_{m,n}$  are  $S$ -units, and that

$$u_m z_m = u_{m,n}^{p^n} z_{m,n}^{p^n} u_n z_n.$$

Viewing this equation only at the places in  $S_p$  we see that

$$z_m = z_{m,n}^{p^n} z_n.$$

Thus the system  $(z_n)$  defines an element of  $E = \mathcal{O}_S^\times \otimes \mathbb{Z}_p$ . Further, it follows from (10) that this element is in fact in  $\mathcal{E}$ . Conversely, given an element  $(z_n) \in \mathcal{E}$ , we can reverse the construction above to get  $(x_n)$ . ■

Now, the archimedean contribution to  $T_p(C_{S,K})$  is clearly contained in the universal norms, but what about  $\mathcal{E}$ ? To answer this question, we use the Poitou-Tate long exact sequence to characterize  $\mathcal{E}$ . Part of this sequence is

$$\sum_{v \in S} H^0(G_v, \mathbb{Z}_p(1)) \rightarrow H^2(G, \mathbb{Q}_p/\mathbb{Z}_p)^\wedge \rightarrow H^1(G, \mathbb{Z}_p(1)) \rightarrow \sum_{v \in S} H^1(G_v, \mathbb{Z}_p(1)).$$

Now,  $H^0(G_v, \mathbb{Z}_p(1)) = 0$ ,  $H^1(G, \mathbb{Z}_p(1)) = \mathcal{O}_K[1/p]^\times \otimes \mathbb{Z}_p$ , and  $H^1(G_v, \mathbb{Z}_p(1)) = K_v^\times \otimes \mathbb{Z}_p$ , so

$$(12) \quad H^2(G, \mathbb{Q}_p/\mathbb{Z}_p)^\wedge = \mathcal{E}.$$

From this characterization we deduce a weak version of Leopoldt's conjecture.

LEMMA 8. Let  $K_n = K(\mu_{p^n})$ , and let  $\mathcal{E}_n$  be the Leopoldt kernel for  $K_n$ . Then  $\varprojlim \mathcal{E}_n = 0$ , where the limit is with respect to the norm maps.

*Proof:* The norm map is dual to the restriction map on cohomology. Thus, from (12),

$$\varprojlim \mathcal{E}_n = (\varprojlim H^2(\mathrm{Gal}(\Omega_S/K_n), \mathbb{Q}_p/\mathbb{Z}_p))^\wedge = H^2(\mathrm{Gal}(\Omega_S/K_\infty), \mathbb{Q}_p/\mathbb{Z}_p)^\wedge.$$

Now  $\mathbb{Q}_p/\mathbb{Z}_p \simeq \mathbb{Q}_p/\mathbb{Z}_p(1)$  over  $K_\infty$ , and

$$\begin{aligned} H^2(\mathrm{Gal}(\Omega_S/K_\infty), \mathbb{Q}_p/\mathbb{Z}_p(1)) &= \varprojlim H^2(\mathrm{Gal}(\Omega_S/K_n), \mathbb{Q}_p/\mathbb{Z}_p(1)) \\ &\hookrightarrow \varprojlim \mathrm{Br}(K_n)[p^\infty] = 0, \end{aligned}$$

where  $\mathrm{Br}(K_n)$  is the Brauer group of  $K_n$ , and the last equality follows from the fact that the restriction map on the Brauer group is multiplication by  $p^n$  under the canonical identification  $\mathrm{Br}(K_n) \hookrightarrow \bigoplus_v \mathbb{Q}/\mathbb{Z}$  coming from the invariant maps. ■

Finally, we are able to prove the following lemma.

LEMMA 9. Tate duality induces an isomorphism

$$C_{S_p, K}[p^n] \simeq H^2(G, \mathbb{Z}/p^n\mathbb{Z})^\wedge.$$

*Proof:* By (13), we have a surjective map

$$(13) \quad C_S(K)[p^n] \twoheadrightarrow H^2(G, \mathbb{Z}/p^n\mathbb{Z})^\wedge,$$

whose kernel is the universal norms. For each  $F$  we have an exact sequence

$$0 \rightarrow D_S(F)[p^n] \rightarrow C_S(F)[p^n] \rightarrow \mathrm{Gal}(\Omega_S/F)^{\mathrm{ab}}[p^n] \rightarrow 0.$$

The universal norms of the right hand groups are zero, so the kernel of (13) is the intersection of the groups  $N_{F/K}D_S(F)[p^n]$ . This clearly contains the image of  $\prod_{v \in S_\infty} \mu_{p^n}(K_v)$ . Further, we have an exact sequence

$$\prod_{v \in S_\infty} \mu_{p^n}(F_v) \rightarrow D_S(F)[p^n] \rightarrow D_{S_p}(F)[p^n] \rightarrow 0.$$

(Here surjectivity on the right follows from the fact that  $F_v$  is  $p$ -divisible if  $v$  is archimedean.) Since  $D_{S_p}(F)$  is divisible, the right hand group is  $\mathcal{E}_F/p^n$  by Lemma 7, and thus the universal norms of the right hand side are zero by Lemma 8. Thus the kernel of (13) is the image of  $\prod_{v \in S_\infty} \mu_{p^n}(K_v)$ . The quotient of  $C_S(K)[p^n]$  by this image is  $C_{S_p, K}[p^n]$ , as required. ■

Recall that  $Y_K$  is the pro- $p$ -completion of  $G^{\text{ab}}$ . Since  $D_S(K)$  is the closure of the archimedean idèles,

$$Y_K = \mathbb{I}_K / \overline{U_{K,S_p} K^\times},$$

where the bar denotes closure in the idèle topology followed by closure in the pro- $p$ -topology. Taking  $p^n$ -torsion in (8), factoring out by the archimedean primes, and using Lemma 7, we get an exact sequence

$$(14) \quad 0 \rightarrow \mathcal{E}/p^n \mathcal{E} \rightarrow C_{S_p, K}[p^n] \rightarrow Y_K[p^n] \rightarrow 0.$$

Finally, we note that (9) and (12) give

$$(15) \quad \hat{H}^{-1}(G, C_S \otimes \mathbb{Z}_p) \simeq H^3(G, \mathbb{Z}_p)^\wedge = H^2(G, \mathbb{Q}_p/\mathbb{Z}_p)^\wedge \simeq \mathcal{E}.$$

This map has the following simple description: given  $c = (c_n) \in C_{S, F} \otimes \mathbb{Z}_p$ , for some  $K \subset F \subset \Omega$ , such that  $N_{F/K}(c_n) \equiv 1 \pmod{p^n}$ , represent  $c_n$  by an idèle  $s_n$ . Then  $N_{F/K}(s_n) = u_n t_n z^{p^n}$  where  $u_n \in U_{S, F}$ ,  $t_n \in F^\times$ , and  $z \in \mathbb{I}_F$ . Then  $(t_n)$  defines an element in  $\mathcal{E}$ , and it is the image of  $c$  under the above map.

## 6. Construction of the Ext Duality.

In this section we will use Kummer theory and class field theory to define a map

$$X \rightarrow \text{Ext}_\Lambda^1(Y, \Lambda'),$$

where  $\Lambda' = \Lambda(1)$ . Ultimately we will extend this definition to  $H_\infty^2(\mathbb{Z}_p(1))$ , which contains  $X$  with a rather uninteresting cokernel by Lemma 4. However, for the sake of concreteness it is worthwhile seeing the simpler version first. Since

$$X = \text{Hom}_{\mathbb{Z}_p}(\varinjlim \mathfrak{L}_n, \mathbb{Q}_p/\mathbb{Z}_p(1))$$

and

$$\text{Ext}^1(Y, \Lambda') = \text{Hom}_{\mathbb{Z}_p}(\varinjlim H^r(\mathbf{x}_n, Y), \mathbb{Q}_p/\mathbb{Z}_p(1)),$$

it suffices to construct maps

$$\alpha_n : H^r(\mathbf{x}_n, Y) \rightarrow \mathfrak{L}_n$$

for each  $n$ , compatible with the direct limit.

The definition of  $\alpha_n$  is particularly simple if  $K_n$  satisfies Leopoldt's conjecture, so we give it in that case first. Let  $U_n = U_{S_p, K_n}$ . Class field theory gives an isomorphism  $Y_n \simeq \mathbb{I}_n / \overline{U_n K_n^\times}$ . Let  $c \in H^r(\mathbf{x}_n, Y)$  be represented by an  $(r+1)$ -tuple  $(y_0, \dots, y_r) \in Y^{r+1}$  such that

$$p^n y_0 + \omega_n(T_1)y_1 + \dots + \omega_n(T_r)y_r = 0.$$

Then the image of  $y_0$  in  $Y_n$  is killed by  $p^n$ . Choose an idèle  $s_0$  for  $K_n$  representing this element; thus  $s_0^{p^n} \in \overline{U_n K_n^\times}$ , and if we choose  $u \in U_n$ ,  $t \in K_n$  such that  $ut$  is sufficiently close to  $s_0^{p^n}$  then the class of  $t$  in  $\mathfrak{L}_n$  is well-defined (as we shall see below), and we set  $\alpha_n(c) = [t]$ .

What if Leopoldt's conjecture fails? Then  $\alpha_n(c)$  is well-defined only modulo  $\mathcal{E}_n$ . We solve this problem using the weak Leopoldt conjecture (Lemma 8) as follows. Since  $K_\infty$  contains  $\mu_{p^\infty}$ , we can and do choose  $m \geq n$  large enough so that

$$(16) \quad N_{m,n} \mathcal{E}_m \subset \mathcal{E}_n^{p^n}.$$

For each  $0 \leq i \leq r$ , choose an idèle  $s_i$  for  $K_m$  which represents the restriction of  $y_i$  to  $Y_m$  under the Artin map. Then

$$p^n s_0 + (g_1^{p^n} - 1)s_1 + \cdots + (g_r^{p^n} - 1)s_r = z \in \overline{U_m K_m^\times}.$$

Choose  $ut \in U_m K_m^\times$  sufficiently close to  $z$ , and let

$$\alpha_n(c) = N_{K_m/K_n} t \pmod{K_n^{\times p^n}}.$$

Note that  $N_{K_m/K_n} z = p^n N_{K_m/K_n} s_0$ , so if  $ut$  is sufficiently close to  $z$ , then

$$N_{K_m/K_n} t \in \mathfrak{L}_n.$$

This is part of what we mean by 'sufficiently close' in the definition. In addition,  $ut \in U_m K_m^\times$  must be chosen so that the image of  $t$  in  $K_m^*/K_m^{*p^m}$  is well defined modulo the image of  $\mathcal{E}_m$ . Then, by virtue of (16),  $N_{K_m/K_n} t$  is well-defined. To see that it is possible to choose  $ut$  in this way, let  $U_p$  be an open neighbourhood of the identity in  $\prod_{\mathfrak{p} \in S_p} (1 + \mathfrak{p}\mathcal{O}_{m,\mathfrak{p}})$  and let

$$U' = U_m \cdot U_p.$$

Then  $U'$  is a neighbourhood of the identity in the idèle group  $\mathbb{I}$  of  $K_m$ . Let  $N$  be a positive integer, to be fixed later. Choose

$$u \in U_m, \quad t \in K_m^\times$$

so that

$$utz^{-1} \in U' \cdot \mathbb{I}^{p^N},$$

and hence

$$tz^{-1} \in U' \cdot \mathbb{I}^{p^N}.$$

If  $t'$  is any other element of  $K_m^\times$  satisfying the same condition, then

$$t/t' \in U' \cdot \mathbb{I}^{p^N}.$$

Since the ideal class group of  $K_m$  is finite, we may choose  $N$  sufficiently large that so that the principle ideal  $(t/t')$  is the  $p^M$ -th power of a principle ideal, for arbitrarily large  $M$ , i.e.,

$$t = et'y^{p^M}$$

for some  $e \in E_m$ ,  $y \in K_m^\times$ . Thus

$$e \in U' \cdot \mathbb{I}^{p^M}.$$

Hence, choosing  $U_p$  small enough and  $M$  large enough, we can ensure that the image of  $e$  in  $\prod_{\mathfrak{p} \in S_m} K_{m,\mathfrak{p}} \otimes \mathbb{Z}_p$  is arbitrarily small, hence in particular that the image of  $e$  in  $K_m^*/K_m^{*p^m}$  is contained in the image of  $\mathcal{E}_m$ . We leave it the reader to check that the definition does not depend on the choice of idèles or on the choice of the representative for  $c$ .

Taking the direct limit of the maps  $\alpha_n$ , we get a map

$$X \rightarrow \text{Ext}_\Lambda^1(Y, \Lambda'),$$

as required.

Finally, we indicate the necessary modification to this definition to obtain a map

$$\alpha'_n : H_\infty^2(\mathbb{Z}_p(1)) \rightarrow \text{Ext}_\Lambda^1(Y, \Lambda').$$

By 9 we have

$$C_{S_p, K_n}[p^n] \simeq H^2(\mathcal{O}'_n, \mathbb{Z}/p^n\mathbb{Z})^\wedge.$$

Thus we want to define maps

$$\alpha'_n : H^r(\mathfrak{x}_n, Y) \rightarrow C_{S_p, K_n}[p^n].$$

Let  $c$  be a class in  $H^r(\mathfrak{x}_n, Y)$  represented by  $(y_0, y_1, \dots, y_r)$ , as above. We define  $\alpha'_n(c)$  to be the class represented by an idèle  $s$  satisfying

$$\begin{aligned} s^{p^n} &= \alpha_n(c)u && \text{for some } u \in U_{K_n} \\ s_v &= y_{0,v} && v \in S_p \end{aligned}$$

The exact sequence

$$0 \rightarrow \Omega_S^\times \rightarrow \mathbb{I}_{S,\Omega} \rightarrow C_S \rightarrow 0$$



yields an exact sequence

$$0 \rightarrow \mu_{p^n} \rightarrow \prod_{v \in S} \mu_{p^n} \rightarrow C_S[p^n] \rightarrow 0$$

and taking  $\text{Gal}(\Omega/K_m)$ -cohomology we get

$$0 \rightarrow \mu_{p^n} \rightarrow \prod_{v \in S} \mu_{p^n} \rightarrow C_S(K_n)[p^n] \rightarrow \mathfrak{L}_n \rightarrow 0,$$

or, factoring out by the archimedean contributions,

$$0 \rightarrow \mu_{p^n} \rightarrow \prod_{v \in S_p} \mu_{p^n} \rightarrow C_{S_p}(K_n)[p^n] \rightarrow \mathfrak{L}_n \rightarrow 0.$$

It is clear from the definitions that the triangle

$$\begin{array}{ccc} H^r(\mathbf{x}_n, Y) & & \\ \downarrow \alpha'_n & \begin{array}{c} \mathbf{4} \\ \mathbf{4} \\ \mathbf{4} \end{array} & \\ C_{S_p, K_n}[p^n] & \xrightarrow{\quad} & \mathfrak{L}_n \end{array}$$

commutes. It is also clear that

$$(17) \quad \alpha'_n(c) \equiv s_0 \pmod{\overline{U_n K_n^\times}}.$$

## 7. Structure of $Y$ .

In this section we recall some results on the structure of  $Y$ , due independently to Jannsen and Nguyen-Quang-Do. First, we introduce an auxiliary module  $Z$ , defined by Nguyen-Quang-Do [Ng], which is very convenient in studying  $Y$ . For this section, we let  $\Omega$  be the maximal pro- $p$ -extension of  $K$  which is unramified outside  $p$ ,  $G = \text{Gal}(\Omega/K)$ , and  $\mathcal{I}$  the augmentation ideal in  $\mathbb{Z}_p[[G]]$ . Nguyen-Quang-Do defines a  $\Lambda$ -module

$$Z_F = H_0(\Omega/F, \mathcal{I}).$$

We shall denote  $Z_{K_\infty}$  simply by  $Z$ . This module has the nice property that

$$(18) \quad H_0(\text{Gal}(K_\infty/F), Z) = Z_F.$$

**PROPOSITION 10** ([Ng], PROPOSITION 1.7). *There is an exact sequence*

$$(19) \quad 0 \rightarrow Y \rightarrow Z \rightarrow I \rightarrow 0,$$

where  $I$  is the augmentation ideal in  $\Lambda$ , and a resolution

$$(20) \quad 0 \rightarrow \Phi \rightarrow \Psi \rightarrow Z \rightarrow 0,$$

where  $\Phi$  and  $\Psi$  are free  $\Lambda$ -modules.

The first sequence is obtained simply by taking homology of the exact sequence

$$0 \rightarrow \mathcal{I} \rightarrow \mathbb{Z}_p[[\mathcal{G}]] \rightarrow \mathbb{Z}_p \rightarrow 0.$$

**COROLLARY 11.** *If  $i > 1$ , then*

$$\text{Ext}_\Lambda^i(Y, \Lambda) = \begin{cases} 0 & i \neq r-2 \\ \mathbb{Z}_p & i = r-2. \end{cases}$$

*Proof:* Since  $Z$  has a free resolution of length 2,  $\text{Ext}_\Lambda^i(Z, \Lambda) = 0$  if  $i > 1$ . Thus, taking Hom of (19), we see that  $\text{Ext}_\Lambda^i(Y, \Lambda) \simeq \text{Ext}_\Lambda^{i+1}(I, \Lambda)$  if  $i \geq 2$ . Now use the following lemma. ■

**LEMMA 12.** *If  $i > 1$ , then*

$$\text{Ext}_\Lambda^i(I, \Lambda) = \begin{cases} 0 & i \neq r-1 \\ \mathbb{Z}_p & i = r-1. \end{cases}$$

*Proof:* Taking Hom of

$$0 \rightarrow I \rightarrow \Lambda \rightarrow \mathbb{Z}_p \rightarrow 0,$$

we see that  $\text{Ext}_\Lambda^{i+1}(I, \Lambda) \simeq \text{Ext}_\Lambda^{i+2}(\mathbb{Z}_p, \Lambda)$ . But, using the Koszul resolution of  $\mathbb{Z}_p$ , one can see that this latter group is zero unless  $i+2 = r$ , in which case it is  $\mathbb{Z}_p$ . ■

## 8. Proof of Theorem B.

**THEOREM 13.** *If  $r \neq 2, 3$ , there is an isomorphism*

$$H_\infty^2 \simeq \text{Ext}^1(Y^1(\mathbb{Z}_p(1)), \Lambda).$$

*If  $r = 2$  there is an exact sequence*

$$\mathbb{Z}_p(1) \rightarrow H_\infty^2 \rightarrow \text{Ext}^1(Y^1(\mathbb{Z}_p(1)), \Lambda) \rightarrow 0,$$

*and if  $r = 3$ , there is an exact sequence*

$$0 \rightarrow H_\infty^2 \rightarrow \text{Ext}^1(Y^1(\mathbb{Z}_p(1)), \Lambda) \rightarrow \mathbb{Z}_p(1).$$

*Proof:* Our aim is to construct a commutative diagram

$$\begin{array}{ccccccc} 0 & \longrightarrow & \mathfrak{W}H^{r-1}(\mathbf{x}'_n, Y)/p^n & \longrightarrow & \mathfrak{W}H^r(\mathbf{x}_n, Y) & \longrightarrow & \mathfrak{W}H^r(\mathbf{x}'_n, Y)[p^n] \longrightarrow \mathfrak{W} \\ & & \gamma_n \downarrow \mathfrak{u} & & \alpha'_n \downarrow \mathfrak{u} & & \beta_n \downarrow \mathfrak{u} \\ 0 & \longrightarrow & \mathfrak{W}_n/\mathcal{E}_n^{p^n} & \longrightarrow & \mathfrak{W}_{S_p, K_n}[p^n] & \longrightarrow & \mathfrak{W}_n[p^n] \longrightarrow \mathfrak{W} \end{array}$$

Here the bottom sequence is (14) and  $\beta_n$  is the restriction to the  $p^n$ -torsion of the canonical map  $H^r(\mathbf{x}'_n, Y) \rightarrow Y_n$ . By (17) it commutes with  $\alpha'_n$ .

We define  $\gamma_n$  to be the restriction of  $\alpha'_n$  to  $H^{r-1}(\mathbf{x}'_n, Y)/p^n$ ; we must show that its image is  $\mathcal{E}_n/\mathcal{E}_n^{p^n}$ . We will factor  $\gamma_n$  into a series of maps, as follows.

First, we have an identification

$$(21) \quad H^{r-1}(\mathbf{x}'_n, Y) \simeq H_1(K_\infty/K_n, Y).$$

Next, we have

$$(22) \quad H_1(K_\infty/K_n, Y) = \varprojlim_m H_1(K_m/K_n, Y_m).$$

Now we concentrate on the individual terms in the inverse limit. The reciprocity isomorphism  $Y_m \simeq \hat{H}^0(\Omega/K_m, C_{S,\Omega})$  gives

$$(23) \quad H_1(K_m/K_n, Y_m) \simeq H_1(K_m/K_n, \hat{H}^0(\Omega/K_m, C_{S,\Omega})).$$

Now we take a coboundary with respect to the exact sequence

$$0 \rightarrow N_{\Omega/K_m} C_{S,\Omega} \rightarrow C_{S,K_m} \rightarrow \hat{H}^0(\Omega/K_m, C_{S,\Omega}) \rightarrow 0.$$

This yields

$$(24) \quad H_1(K_m/K_n, \hat{H}^0(\Omega/K_m, C_{S,\Omega})) \rightarrow \hat{H}^{-1}(K_m/K_n, N_{\Omega/K_m} C_{S,\Omega}).$$

Next, the exact sequence

$$\hat{H}^{-1}(\Omega/K_m, C_{S,\Omega}) \rightarrow \hat{H}^{-1}(\Omega/K_n, C_{S,\Omega}) \rightarrow \hat{H}^{-1}(K_m/K_n, N_{\Omega/K_m} C_{S,\Omega}) \rightarrow 0$$

yields an isomorphism

$$(25) \quad \hat{H}^{-1}(K_m/K_n, N_{\Omega/K_m} C_{S,\Omega}) \simeq \frac{\hat{H}^{-1}(\Omega/K_n, C_{S,\Omega})}{\hat{H}^{-1}(\Omega/K_m, C_{S,\Omega})}.$$

Finally, (15) gives

$$(26) \quad \frac{\hat{H}^{-1}(\Omega/K_n, C_{S,\Omega})}{\hat{H}^{-1}(\Omega/K_m, C_{S,\Omega})} \simeq \frac{\mathcal{E}_n}{N_{K_m/K_n} \mathcal{E}_m}.$$

Taking the inverse limit over  $m$ , using Lemma 8, we get, on composing (21)–(26), a map

$$H^{r-1}(\mathbf{x}'_n, Y) \rightarrow \mathcal{E}_n,$$

which, taken mod  $p^n$ , we claim is  $\gamma_n$ .

Indeed, an element  $c \in H^{r-1}(\mathbf{x}'_n, Y)$  is represented by an  $r$ -tuple  $(y_1, \dots, y_r)$  in  $Y^r$  such that

$$\omega_n(T_1)y_1 + \dots + \omega_n(T_r)y_r = 0.$$

The map (21) amounts to observing that this is the same as

$$(\sigma_1^{p^n} - 1)y_1 + \dots + (\sigma_r^{p^n} - 1)y_r = 0,$$

and so equally represents an element of  $H_1(K_\infty/K_n, Y)$ . Then (22) expresses the  $y_i$ 's as the inverse limit their restrictions to  $Y_m$ . The map (23) expresses these restrictions as idèle classes, say of idèles  $s_1, \dots, s_r$  in  $\mathbb{I}_{K_m}$ . Then

$$(\sigma_1^{p^n} - 1)[s_1] + \dots + (\sigma_r^{p^n} - 1)[s_r] = N_{L/K_m}[s],$$

for arbitrarily large  $L \subset \Omega$  and  $s \in \mathbb{I}_L$ , where the square brackets denote idèle classes. The map (24) takes us to  $N_{L/K_m}[s]$  and the map (25) takes us to  $[s]$  itself. Finally, in view of the remarks at the end of Sect. 5, (26) takes us to  $t_n \in \mathcal{E}_n/p^n\mathcal{E}_n$ , where  $u_n t_n$  is close to  $N_{L/K_n}s$  for some  $u_n \in U_{S, K_n}$ . This is the description of  $\alpha'_n(c)$ .

We now look at the kernel and cokernel of  $\varinjlim \beta_n$  and  $\varinjlim \gamma_n$ . First  $\beta_n$ . There is a commutative diagram

$$\begin{array}{ccc} H^r(\mathbf{x}'_n, Y)[p^n] & \xrightarrow{\quad} & \mathbf{w}H^r(\mathbf{x}'_n, Z)[p^n] \\ \beta_n \downarrow \mathbf{u} & & \downarrow \mathbf{u} \\ Y_n[p^n] & \xrightarrow{\quad} & \mathbf{w}Z_n[p^n]. \end{array}$$

The right map is an isomorphism by (18), and the bottom map is an isomorphism by (19), since  $I_n \subset \mathbb{Z}_p[\text{Gal}(K_n/K)]$  is torsion free. Hence the kernel and cokernel of  $\beta_n$  are the same as those of

$$H^r(\mathbf{x}'_n, Y)[p^n] \rightarrow H^r(\mathbf{x}'_n, Z)[p^n].$$

We claim that the cokernel of  $\varinjlim_n H^r(\mathbf{x}'_n, Y) \rightarrow \varinjlim_n H^r(\mathbf{x}'_n, Z)$  is torsion-free for all  $r$ , and that the kernel is  $p$ -divisible unless  $r = 2$ , and in that case it is isomorphic to  $\mathbb{Z}_p$ .

To verify the claim, consider the long exact sequence

$$0 \rightarrow H^{r-1}(\mathbf{x}'_n, I) \rightarrow H^r(\mathbf{x}'_n, Y) \rightarrow H^r(\mathbf{x}'_n, Z) \rightarrow H^r(\mathbf{x}'_n, I) \rightarrow 0.$$

The zero on the left is  $H^{r-1}(\mathbf{x}'_n, Z)$ . We may see that it is zero in the case  $n = 1$  by taking  $H^*(\mathbf{x}'_1, \cdot)$  of the resolution (20) for  $Z$  (assuming that the resolution is

minimal). The case of arbitrary  $n$  may be treated by regarding  $K_n$  as  $K$ . Since  $H^r(\mathbf{x}'_n, I) = I/(\omega_n(T_1), \dots, \omega_n(T_r))$  is torsion-free, its direct limit is. This proves the statement about the cokernel. As for the kernel, if  $r = 1$ , then  $H^{r-1}(\mathbf{x}'_n, I) = I[\omega_n(T)] = 0$ . If  $r > 1$ , the  $H^{r-1}(\mathbf{x}'_n, I)$  is generated by elements of the form

$$e_{i,j}^{(n)} = (0, \dots, 0, \omega_n(T_j), 0, \dots, 0, -\omega_n(T_i), 0, \dots, 0), \quad 1 \leq i < j \leq r,$$

where the non-zero terms occur at the  $i$ -th and  $j$ -th positions. The transition map in the direct limit takes  $e_{i,j}^{(n)}$  to  $p^{(r-2)(m-n)}e_{i,j}^{(m)}$ . This proves that the kernel is  $p$ -divisible unless  $r = 2$ , and in that case it is generated by the single element  $e_{1,2}^{(n)}$ .

It follows from the claim that that  $\varinjlim \beta_n$  is an isomorphism unless  $r = 2$ , and in that case it has a cokernel contained in  $\mathbb{Q}_p/\mathbb{Z}_p$ .

Now we consider the kernel and cokernel of  $\gamma_n$ . We expressed  $\gamma_n$  as the composite of a sequence of maps (21)–(26). The only map in the sequence that was not an isomorphism was (24), which is a coboundary with respect to the Tate cohomology  $\hat{H}^*(K_m/K_n, \cdot)$  of the short exact sequence

$$0 \rightarrow N_{\Omega/K_m} C_{S,\Omega} \rightarrow C_{S,K_m} \rightarrow Y_m \rightarrow 0.$$

In fact, it is the inverse limit over  $m$  that fits into  $\gamma_n$ . Now,  $H^{-1}(K_m/K_n, C_{S,K_m}) = 0$  by class field theory. Thus we have an exact sequence

$$\begin{aligned} \varinjlim_m \hat{H}^{-2}(K_m/K_n, C_{S,K_m}) &\rightarrow \varinjlim_m \hat{H}^{-2}(K_m/K_n, H^0(\Omega/K_m, C_{S,\Omega})) \xrightarrow{\gamma_n} \\ &\varinjlim_m \hat{H}^{-1}(K_m/K_n, N_{\Omega/K_m} C_{S,\Omega}) \rightarrow 0. \end{aligned}$$

Now, it is ultimately the direct limit over  $n$  of  $\gamma_n$  that counts. By class field theory and the cohomology theory of abelian groups, we see that

$$\varinjlim_n \varinjlim_m \hat{H}^{-2}(K_m/K_n, C_{S,K_m}) \simeq \begin{cases} \mathbb{Q}_p/\mathbb{Z}_p & r = 3 \\ 0 & \text{otherwise} \end{cases}$$

(The point is that the transition maps in the direct limit preserve the cohomology group only in the case  $r = 3$ .)

In summary, we have a cokernel contained in  $\mathbb{Q}_p/\mathbb{Z}_p$  for  $\varinjlim \beta_n$  when  $r = 2$ , a kernel which is a quotient of  $\mathbb{Q}_p/\mathbb{Z}_p$  for  $\varinjlim \gamma_n$  when  $r = 3$ , and otherwise both are isomorphisms. An application of the snake lemma now concludes the proof of the theorem. ■

#### BIBLIOGRAPHY

[AT] E. Artin & J. Tate, *Class Field Theory*, Benjamin, New York, 1968.

- [B] P. Billot, *Quelques aspects de la descente sur une courbe elliptique dan le cas de réduction supersingulière*, Compositio Mathematica **58** (1986), 341–369.
- [Br] K. S. Brown, *Cohomology of Groups*, Springer-Verlag, New York, 1982.
- [B-H] W. Bruns & J. Herzog, *Cohen-Macaulay rings, Cambridge studies in advanced mathematics* **39**, Cambridge University Press, Cambridge, 1993.
- [G] R. Greenberg, *On the Structure of Certain Galois Groups*, Inventiones math. **47** (1978), 85–99.
- [Gr] A. Grothendieck, *Local Cohomology*, Lecture Notes in Mathematics Vol. 41, Springer-Verlag, Berlin, 1967.
- [I] K. Iwasawa, *On  $\mathbb{Z}_\ell$ -extensions of algebraic number fields*, Annals of Math. **98** (1973), 246–326.
- [J1] U. Jannsen, *On the structure of Galois groups as Galois modules*, in Number Theory Noordwijkerhout 1983, Lecture Notes in Math. **1068**, Springer, Berlin, 1984, pp. 109–126.
- [J2] ———, *Iwasawa Modules up to Isomorphism*, in Advanced Studies in Pure Mathematics **17**, Academic Press, Orlando, 1989, pp. 171–207.
- [Mc] W. McCallum, *A duality theorem in the multivariable Iwasawa theory of local fields*, J. reine angew. Math. **464** (1995), 143–172.
- [Mi] J.S. Milne, *Arithmetic Duality Theorems*, Academic Press, Orlando, 1986.
- [Ng1] T. Nguyen-Quang-Do, *Sur la structure galoisienne des corps locaux et la théorie d’Iwasawa*, Compositio Math. **46** no. 1 (1982), 85–119.
- [Ng2] ———, *Sur la structure galoisienne des corps locaux II*, J. reine angew. Math. **333** (1982), 133–143.
- [Ng3] ———, *Formations de classes et modules d’Iwasawa*, Number Theory Noordwijkerhout, 1983, Lecture Notes in Math. **1068**, Springer, Berlin, 1984, pp. 167–185.
- [P-R] B. Perrin-Riou, *Astérisque*.
- [S] J.-P. Serre, *Cohomologie Galoisienne*, Springer-Verlag, Berlin, 1994.
- [Sch] P. Schneider, *Über gewisse Galoiscohomologiegruppen*, Math. Z **168** (1979), 181–205.
- [Ta] J. Tate, *Duality theorems in Galois cohomology over number fields*, Proc. Int. Congr., Stockholm, 1962, pp. 234–241.
- [U] K. Uchida, *On Tate duality theorems on Galois cohomology*, Tohoku Math. J. **21** (1969), 92–101.

Department of Mathematics, University of Arizona, Tucson, AZ, 85721