References

[1] J. Cassels and A. Fröhlich, *Algebraic Number Theory*, Thompson Book Co., Washington, D.C., 1967.
[2] R. Dedekind, *Ueber die Anzahl der Idealklassen in reinen kubischen Zahlkörpern*, J. Reine Angew. Math. 121 (1900), pp. 40–123.
[3] F. Gerth, *On 3-class groups of pure cubic fields*, ibid. 278/279 (1975), pp. 52–62.
[4] — *Ranks of 3-class groups of non-Galois cubic fields*, Acta Arith. 30 (1976), pp. 307–322.
[5] — *Counting certain number fields with prescribed l-class numbers*, J. Reine Angew. Math. 337 (1982), pp. 195–207.
[6] — *An application of matrices over finite fields to algebraic number theory*, Math. Comp. 41 (1983), pp. 229–234.
[7] — *Densities for ranks of certain parts of p-class groups*, to appear.
[8] H. Hasse, *Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper, II*, Jahresber. Deutsch. Math.-Verein. 39 (1930), pp. 1–204.
[9] E. Inaba, *Über die Struktur der l-Klassengruppe zyklischer Zahlkörper von Primzahlgrad l*, J. Fac. Sci. Imp. Univ. Tokyo, Sect. I, 4 (1940), pp. 61–115.
[10] G. Landsberg, *Ueber eine Anzahlbestimmung und eine damit zusammenhängende Reihe*, J. Reine Angew. Math. 111 (1893), pp. 87–88.

DEPARTMENT OF MATHEMATICS
UNIVERSITY OF TEXAS
AUSTIN, TEXAS 78712
U.S.A.

Received on 3.9.1984
and in revised form on 31.1.1985 (1449)

ACTA ARITHMETICA
XLVI (1986)

Galois representations of Iwasawa modules

by

ROBERT GOLD and MANOHAR MADAN (Columbus, Ohio)

1. Introduction. A finite group of automorphisms of an algebraic function field of one variable over the complex numbers operates in a natural way on the space of holomorphic differentials. The representation thus obtained was given by Chevalley and Weil [1]. Iwasawa [5] obtained analogous results for p-adic galois representations in number fields. In his situation, L/K is a finite p-extension of Z_p-fields of CM-type and $\mathrm{Gal}(L/K)$ operates on A_L^-, the minus part of the p-class group of L. Iwasawa determined the representation on $A_L^- \otimes_{Z_p} Q_p$ (Th. 4, Th. 5). His immediate object was to give a proof of a theorem of Kida [6]. The classical Riemann–Hurwitz genus formula and the well-known orthogonality relations on characters are the critical tools in the treatment of Chevalley and Weil. Kida's theorem is an analogue of the genus formula and it can be proved easily. In Section 2, we give a unified proof of Iwasawa's two theorems in the spirit of Chevalley and Weil. This is Theorem 2. In the special case when $[L:K] = p$, we determine even the integral representations, i.e. the structure of A_L^- as a $Z_p[G]$-module, $G = \mathrm{Gal}(L/K)$. This gives in particular the basis for induction in the proof of Theorem 2.

In Section 3, we determine the modular representations in the case when L/K is a cyclic p-extension and the module consists of elements of order dividing p in A_L^-. This result is analogous to the one proved in [4] for function fields.

To generalize Theorem 1 to arbitrary p-extensions is an interesting open problem. For the special case when G is cyclic of order p^2, the indecomposable $Z_p[G]$-modules have been classified. Using this, we have been able to extend Theorem 1 to this case, Theorem 4 in Section 4.

We are particularly indebted to Alfredo Jones for the information summarized in Table 1.

2. Let p be an odd prime. Let Q_n be the unique cyclic extension of degree p^{n-1} contained in the cyclotomic field of p^n-th roots of unity and $Q_\infty = \bigcup_{n>0} Q_n$. A Z_p-field is the composite of Q_∞ with a finite extension of Q.

A Z_p-field of CM-type is a totally imaginary Z_p-field which is a quadratic extension of a totally real Z_p-field. Let L/K be a cyclic extension of degree p of Z_p-fields of CM-type. Let $G = \mathrm{Gal}(L/K)$ and A_K^- (resp. A_L^-) be the minus part of the p-primary ideal class group of K (resp. L). As in [5] we let A_1 denote the trivial G-module Q_p/Z_p, A_p denotes the divisible regular representation

$$(Q_p/Z_p)[X]/X^p-1,$$

and A_{p-1} denotes the divisible faithful representation

$$(Q_p/Z_p)[X]/(X^{p-1}+X^{p-2}+\ldots+X+1).$$

Any divisible $Z_p[G]$-module of finite rank is isomorphic to a direct sum of indecomposable modules

$$A_1^{a_1} \oplus A_{p-1}^{a_{p-1}} \oplus A_p^{a_p}$$

for uniquely determined a_1, a_{p-1}, a_p.

THEOREM 1. *Assume that L/K are as described above, $\mu(A_K^-) = 0$, and τ is the number of non-p-primes of K^+ which ramify in L^+/K^+ and split in K/K^+. As a $Z_p[G]$-module, A_L^- is isomorphic to*

$$A_p^{\lambda_K^-} \oplus A_{p-1}^{(\tau-\delta)} \quad \textit{if} \quad \tau > 0$$

and

$$A_p^{(\lambda_K^- -\delta)} \oplus A_1^{\delta} \quad \textit{if} \quad \tau = 0$$

where $\lambda_K^- = \lambda(A_K^-)$ and $\delta = 1$ if K contains a primitive p-th root of unity, $\delta = 0$ otherwise.

Proof. It is known (e.g. [6]) that $\mu(A_K^-) = 0$ implies that $\mu(A_L^-) = 0$ and consequently that A_L^- is Z_p-divisible. Thus

$$A_L^- \cong A_1^{a_1} \oplus A_{p-1}^{a_{p-1}} \oplus A_p^{a_p} \tag{1}$$

and we need to compute the exponents.

Let $H^i(G, A_j)$, $i = -1, 0$; $j = 1, p-1, p$, denote the usual reduced or Tate cohomology groups. It is straightforward to compute the entries in the following table:

$A =$	A_1	A_{p-1}	A_p
$H^0(G, A) =$	0	Z_p/pZ_p	0
$H^{-1}(G, A) =$	Z_p/pZ_p	0	0

The exponents in (1) can therefore be determined from the p-ranks of A_L^-, $H^0(G, A_L^-)$, and $H^1(G, A_L^-)$.

The rank of A_L^- is $\lambda(A_L^-) = \lambda_L^-$ which by Kida's Theorem ([6]) is

$$p \cdot \lambda_K^- + (p-1)(\tau-\delta).$$

Next we look at the cohomology groups. We start with the canonical short exact sequences

$$\begin{array}{ccccccccc} 0 & \to & P_L & \to & I_L & \to & C_L & \to & 0, \\ 0 & \to & E_L & \to & L^\times & \to & P_L & \to & 0 \end{array} \tag{2}$$

whose terms are defined as in [5]. As usual $H^{-1}(G, I_L) = 0$, giving rise to

$$0 \to H^{-1}(G, C_L) \to H^0(G, P_L) \to H^0(G, I_L) \to H^0(G, C_L) \to H^{-1}(P_L) \to 0. \tag{3}$$

In addition $H^{-1}(G, L^\times) = 0$ and, since L/K is an extension of Z_p-fields, and p is odd, $H^0(G, L^\times) = 0$ (see [5], [3]). Hence $H^0(G, P_L) \cong H^{-1}(G, E_L)$ and $H^{-1}(G, P_L) \cong H^0(G, E_L)$. Since L and K are of CM-type and p is odd, we may take minus parts. Letting $W =$ the p-power roots of unity in K, we have

$$\begin{aligned} H^0(P_L)^- &\cong H^{-1}(E_L)^- \cong H^{-1}(W) \cong (Z/pZ)^\delta, \\ H^{-1}(P_L)^- &\cong H^0(E_L)^- \cong H^0(W) = \{0\}. \end{aligned} \tag{4}$$

Take minus parts of (3) and replace C_L by its p-primary component to obtain

$$0 \to H^{-1}(G, A_L^-) \to (Z/pZ)^\delta \xrightarrow{f} H^0(G, I_L)^- \to H^0(G, A_L^-) \to 0. \tag{5}$$

Recall next that every non-p-prime of K which is not ramified in L/K is completely decomposed in L/K (see [3]). Therefore

$$H^0(G, I_L)^- \cong (I_L^G/N(I_L))^- = (I_L^G/I_K)^- \cong (Z/pZ)^\tau.$$

Next we will show that f is injective if $\tau > 0$:

$$\begin{array}{cccc} f\colon & H^0(G, P_L)^- & \to & H^0(G, I_L)^- \\ & \| & & \| \\ & (Z/pZ) & & (Z/pZ)^\tau. \end{array}$$

Of course, we assume that $\delta = 1$.

Let $\alpha \in L$ be such that $(\alpha) \in \mathrm{Ker}(f)$, i.e. $(\alpha) \in N(I_L) = I_K$. By Kida's Proposition 1 in [6] we see that if $\tau > 0$ then (α) as an element of I_K is already principal: $(\alpha) = (\beta)$ with $\beta \in K^\times$. As noted above, $K^\times = N(L^\times)$. Therefore $\beta \in N(L^\times)$ and $(\alpha) = (\beta)$ is trivial in $H^0(G, P_L) = P_L^G/N(P_L)$.

We conclude that if $\tau > 0$, then $H^{-1}(A_L^-) = 0$ and $H^0(A_L^-) \cong (Z/pZ)^{\tau-\delta}$. If $\tau = 0$ then clearly $H^{-1}(A_L^-) \cong (Z/pZ)^\delta$ and $H^0(A_L^-) = 0$. Thus all necessary p-ranks have been determined and the proof is completed.

For any divisible Z_p-module M of finite rank, we let

$$V(M) = \mathrm{Hom}_{Z_p}(M, Q_p/Z_p) \otimes_{Z_p} Q_p,$$

a finite dimensional Q_p-vector space. If M is a $Z_p[G]$-module for any p-group G, then $V(M)$ is naturally a $Q_p[G]$-module.

THEOREM 2 (Iwasawa). *Let p be an odd prime and L/K a p-extension of Z_p-fields of CM-type such that $\mu_K^- = 0$. Let $G = \mathrm{Gal}(L/K)$, $V_L = V(A_L^-)$, and $\pi_{L/K}^-$ the p-representation of G on $\mathrm{GL}(V_L)$. Then*

$$(*)\qquad \pi_{L/K}^- = \delta\cdot\pi_1 \oplus (\lambda_K^- - \delta)\cdot\pi_G \oplus \Big(\bigoplus_{v^+/K^+} \pi'_{v^+}\Big),$$

where π_1 is the trivial one-dimensional representation, π_G is the regular representation of G, and π'_{v^+} is the complement in π_G of the representation induced from the trivial 1-dimensional representation on the inertia subgroup of v^+ in $G(L^+/K^+) \cong G(L/K)$ for every non-p-prime v^+ split in K/K^+.

Proof. Assume first that G has order p. From Theorem 1, the fact that $V(A_1)$ affords π_1, $V(A_{p-1})$ affords $\pi_G - \pi_1$, and $V(A_p)$ affords π_G, and for any ramified prime $\pi'_{v^+} = \pi_G - \pi_1$, we see that $(*)$ holds in this case.

Now assume that G is cyclic of order p^n and that $(*)$ is true for cyclic p-extensions of degree $\leqslant p^{n-1}$. Let $\Phi_i(x)$ be the cyclotomic polynomial of the p^i-th roots of unity and let $V_i = Q_p[x]/(\Phi_i(x))$. Then V_i may be viewed as an irreducible $Q_p[G]$-module by means of the maps

$$Q_p[G] \cong Q_p[x]/(x^{p^n}-1) \to Q_p[x]/\Phi_i(x).$$

As a $Q_p[G]$-module, V_L has a unique expression as a direct sum of irreducible modules: $V_L = \bigoplus_{i=0}^{n} V_i^{a_i}$.

Let G_j be the subgroup of G of index p^j and for any $Q_p[G]$-module V, let $V^{(j)}$ denote the subspace pointwise invariant under action of G_j. It is not hard to see that

$$\dim(V_i^{(j)}) = \begin{cases} 0, & i > j, \\ \varphi(p^i), & i \leqslant j \end{cases} \qquad \begin{cases} i = 0, \ldots, n, \\ j = 0, \ldots, n. \end{cases}$$

It follows that

$$\dim(V_L^{(j)}) = \sum_{i=0}^{j} a_i\,\varphi(p^i).$$

Solving for a_i we get

$$(6)\qquad a_i = \frac{1}{\varphi(p^i)}\big(\dim V_L^{(i)} - \dim V_L^{(i-1)}\big).$$

LEMMA 1. $\dim(V_L^{(i)}) = \lambda_i^- = \lambda(A_{K_i}^-)$ *where K_i is the fixed field of G_i.*

Proof. Since $V_L = V(A_L^-)$ is finite dimensional, $\dim V_L^{G_i}$ equals the rank of the maximal divisible submodule of $(A_L^-)^{G_i}$. Using (2) we have

$$0 \to E_L^{G_i} \to L^{G_i} \to P_L^{G_i} \to H^1(G_i, E_L) \to 0$$

and

$$0 \to P_L^{G_i} \to I_L^{G_i} \to C_L^{G_i} \to H^1(G_i, P_L).$$

This gives in turn

$$P_L^{G_i}/P_{K_i} \cong H^1(G_i, E_L); \quad 0 \to P_L^{G_i}/P_{K_i} \to I_L^{G_i}/P_{K_i} \to C_L^{G_i} \to H^1(G_i, P_L).$$

Taking p-primary and minus parts we obtain (cf. (4))

$$(7)\qquad 0 \to H^1(G_i, W) \to (I_L^{G_i}/P_{K_i})^- \to (A_L^-)^{G_i} \to 0.$$

In view of the sequence

$$0 \to A_{K_i}^- \to (I_L^{G_i}/P_{K_i})^- \to (I_L^{G_i}/I_{K_i})^- \to 0$$

and the finiteness of $H^1(G_i, W)$ and $I_L^{G_i}/I_{K_i}$ we see that $A_{K_i}^-$ and $(A_L^-)^{G_i}$ have the same maximal divisible rank, $\lambda(A_{K_i}^-)$.

Let T be an inertia subgroup of G for some prime v^+. Assume $T = G_j$, the subgroup of index p^j. The representation of G induced from the trivial one dimensional representation of T is the sum $\bigoplus_{i=0}^{j} V_i$, i.e. the representation of G arising from the regular representation of G/T. Since the regular representation of G is realized on $V_G = \bigoplus_{i=0}^{n} V_i$, the representation π'_{v^+} is afforded by

$$\bigoplus_{i=j+1}^{n} V_i = \bigoplus_{i=n-\mathrm{ord}_p e(v^+)+1}^{n} V_i.$$

We can now rewrite $(*)$ as

$$(**)\qquad V_L = V_0^{\delta} \oplus V_G^{\lambda_K^- - \delta} \oplus \bigoplus_{v^+} \bigoplus_{i=n-\mathrm{ord}_p e(v^+)+1}^{n} V_i.$$

If we let τ_i, $i = 0, \ldots, n-1$, denote the number of v^+ with ramification degree exactly p^{n-1} (i.e. inertia field equal to K_i), this becomes

$$(8)\qquad V_L = V_0^{\delta} \oplus V_G^{\lambda_K^- - \delta} \oplus \bigoplus_{i=1}^{n} V_i^{\sum_{j=0}^{i-1}\tau_j} = V_0^{\lambda_K^-} \oplus \bigoplus_{i=1}^{n} V_i^{\lambda_K^- - \delta + \sum_{j<i}\tau_j}$$

By the results of Kida we may write

$$\lambda_{K_i}^- = p^i(\lambda_K^- - \delta) + \sum_{w^+} \big(e(w^+, K_i^+/K^+) - 1\big) + \delta.$$

Consequently

$$\lambda_{K_i}^- - \lambda_{K_{i-1}}^- = \varphi(p^i)(\lambda_K^- - \delta) + \tau_{i-1}\, p^{i-1}(p-1) + \sum_{j=0}^{i-2} \tau_j\, p^j (p^{i-j} - p^{i-j-1}), \quad i \geqslant 1.$$

From (6) and Lemma 1, we have

$$a_i = \lambda_K^- - \delta + \frac{1}{\varphi(p^i)}\sum_{j=0}^{i-1} \tau_j p^j (p^{i-j} - p^{i-j-1}), \qquad i \geqslant 1$$

$$= \lambda_K^- - \delta + \frac{1}{\varphi(p^i)}\sum_{j=0}^{i-1}\tau_j(p^i - p^{i-1}) = \lambda_K^- - \delta + \sum_{j=0}^{i-1}\tau_j$$

while $a_0 = \lambda_K^- = \lambda_{K_0}^-$.

These are precisely the exponents occurring in (8), thus confirming the theorem for cyclic G.

Now let $G = G(L/K)$ be an arbitrary finite p-group. We will show that (*) is valid for such G as a consequence of its validity for cyclic G. Let χ_x be the character of the representation π_x. It will suffice to show that

$$\chi_{L/K}^-(g) = \delta_K\cdot\chi_1(g) + (\lambda_K^- - \delta_K)\chi_G(g) + \sum_{v^+/K^+} \chi'_{v^+}(g)$$

for every $e \neq g \in G$.

Fix $g\neq e$, let $S=\langle g\rangle \subseteq G$, and let E be the fixed field of S: $K\subseteq E\subseteq L$. Then we know

$$\chi_{L/K}^-(g) = \chi_{L/E}^-(g) = \delta_E\chi_1(g) + (\lambda_E^- - \delta_E)\chi_S(g) + \sum_{v^+/E^+}\chi'_{v^+,S}(g)$$

with $\chi'_{v^+,S}$ taken with respect to the extension L/E. Note that

$$\delta_K=\delta_E,\qquad \chi_G(g)=\chi_S(g)=0\quad (g\neq e),\qquad \chi'_{v^+} = \chi_G - \mathrm{Ind}_{T_{v^+}}^G(\chi_{0,T_{v^+}}),$$

and

$$\chi'_{v^+,S} = \chi_S - \mathrm{Ind}^S_{T_{v^+}\cap S}(\chi_{0,T_{v^+}\cap S}).$$

Furthermore,

$$\mathrm{Ind}_T^G(\chi_{0,T})(g) = \frac{1}{|T|}\sum_{h\in G}\chi_0'(h^{-1}gh) \quad \text{when } \chi_0'(h) = \begin{cases}0, & h\notin T,\\ \chi_0(h)=1, & h\in T,\end{cases}$$

(9)

$$= \frac{1}{|T|}\cdot|T|\cdot\#\{w \mid w \text{ place of } L,\ w|v,\ w \text{ totally ramified in } L/E\}$$

since

$$\#\{h \mid h^{-1}gh\in T_{w^+}\} = \#\{h\mid g\in hT_{w^+}h^{-1}\} = \#\{h \mid (w^+)^{h^{-1}} \text{ ramified in } L/E\}$$

$$= |T|\cdot\#\{w^+ \text{ totally ramified in } L/E\}.$$

A similar analysis shows that

$$\mathrm{Ind}^S_{T\cap S}(\chi_{0,T\cap S})(g)$$
$$= \#\{u^+ \mid u^+ \text{ place of } E,\ u^+|v^+,\ u^+ \text{ totally ramified in } L/E\}$$
$$= \#\{w\}$$

as in (9). This ends the proof of Theorem 2.

3. We continue to assume that p is an odd prime and L/K a p-extension of Z_p-fields of CM-type. We assume in this section that $G=\mathrm{Gal}(L/K)$ is cyclic of order p^n and we let X_L denote the subgroup of elements of order dividing p in A_L^-. We will describe the modular representation type of G on X_L; i.e. the structure X_L as a $F_p[G]$-module.

For $i = 1, 2, \ldots, p^n$, let $L(i)$ be the indecomposable $F_p[G]$-module of F_p-dimension i, so $L(i)\cong F_p[x]/(x-1)^i$. As above, τ_i is the number of non-p-places of K^+ with ramification degree p^{n-i} in L^+/K^+ and split in K/K^+, $i=0, 1,\ldots,n-1$.

THEOREM 3. *Let* $m = \max\{j \mid i<j \Rightarrow \tau_i = 0\}$; $0\leqslant m\leqslant n$, *then*

(10)
$$X_L \cong (\lambda_K^- - \delta)L(p^n)\oplus\delta L(p^n - p^{n-m}+1)\oplus (\tau_m-\delta)L(p^n-p^{n-m})\oplus\bigoplus_{i=m+1}^{n-1}\tau_i L(p^n-p^i).$$

Proof. Let g be a generator of G. We define

$${}_jX_L = \{x\in X_L \mid x^{(1-g)^j} = 1\},\qquad j=0, 1,\ldots,p^n.$$

Thus

$${}_{p^n}X_L = X_L,\qquad {}_1X_L = X_L^G,\qquad {}_0X_L=\{1\}.$$

Let d_i, $i = 1,\ldots,p^n$, be the number of times $L(i)$ occurs in the decomposition of X_L. It is easy to see that

$$d_{p^n} = \dim_{F_p}({}_pX_L/{}_{(p^n-1)}X_L)$$

and

(11)
$$d_j = \dim_{F_p}({}_jX_L/{}_{(j-1)}X_L) - \dim_{F_p}({}_{(j+1)}X_L/{}_jX_L),$$

for $j=1, 2,\ldots,p^n-1$.

Note that this last equation implies that

(12)
$$[{}_jX_L : {}_{(j-1)}X_L] \geqslant [{}_{(j+1)}X_L : {}_jX_L] \qquad\text{for}\qquad j=1,\ldots,p^n-1.$$

As earlier, we let G_i be the subgroup of G of index p^i and K_i its fixed field. Thus G_i is generated by g^{p^i} and $[K_i:K]=p^i$. We will need the facts listed in

LEMMA 2. *Given the notation described above*

(a) $(1-g)^{p^n-p^j} = N_{G_j} = \sum_{i=0}^{p^{n-j}-1}(g^{p^j})^i$,

(b) ${}_{p^i}X_L = X_L^{G_i}$,

(c) *If L/K is unramified, then* $\dim {}_pX_L^{G_i} = \lambda^-_{K_i}$,

(d) *If $i \geqslant m$, then the map $X_L \to X_{K_i}$, induced by the norm, is surjective. The extension map $e\colon X_{K_i} \to X_L$ is injective and $e(X_{K_i}) = N_{G_i}(X_L)$.*

(e) *If L/K is ramified of degree p then X_L^G has* $\dim \lambda_K - \delta + \tau$.

Proof of Lemma 2.

(a) $(1-g)^{p^n-p^j} = (1-g^{p^j})^{p^{n-j}-1}$, on X_L

$$= \frac{(1-g^{p^j})^{p^{n-j}}}{(1-g^{p^j})} = \frac{1-(g^{p^j})^{p^{n-j}}}{1-g^{p^j}} = \sum_{i=0}^{p^{n-j}-1} (g^{p^j})^i$$

$$= N_{G_j}.$$

(b) ${}_{p^j}X_L = \mathrm{Ker}(1-g)^{p^j} = \mathrm{Ker}(1-g^{p^j}) = X_L^{G_j}$.

(c) For unramified L/K, (7) reads

$$0 \to C^{\delta}_{p^{n-i}} \to A^-_{K_i} \to (A^-_L)^{G_i} \to 0.$$

Therefore, since $A^-_{K_i}$ is divisible,

$$A^-_{K_i} \cong (A^-_L)^{G_i}.$$

Consequently,

$$X_{K_i} = {}_pA^-_{K_i} = {}_p[(A^-_L)^{G_i}] = X_L^{G_i}.$$

(d) It suffices to prove the assertion for K_j/K_{j-1} of degree p. By Kida's Proposition 1 [6], e is injective. As shown in Theorem 1 for a ramified extension of degree p, $H^{-1}(A^-_{K_j}) = 0$ and $H^0(A^-_{K_j}) \cong C_p^{\tau-\delta}$. Taking the cohomology of the sequence

$$0 \to X_{K_j} \to A^-_{K_j} \xrightarrow{p} A^-_{K_j} \to 0$$

we deduce that

$$H^{-1}(X_{K_j}) \cong H^0(X_{K_j}) \cong H^0(A^-_{K_j}) = C_p^{\tau-\delta}.$$

In particular $\dim(X^G_{K_j}/N(X_{K_j})) = \tau - \delta$. But

$$\dim(X^G_{K_j}/e(X_{K_{j-1}})) = \dim X^G_{K_j} - \dim e(X_{K_{j-1}}) = (\lambda^-_K + \tau - \delta) - \lambda^-_K.$$

Thus $\dim N(X_{K_j}) = \dim e(X_{K_{j-1}})$ and, since clearly $N(X_{K_j}) \subseteq e(X_{K_{j-1}})$, they are equal. Since $N = e \circ \eta$ where $\eta\colon X_{K_j} \to X_{K_{j-1}}$ is induced by taking norms, η is surjective.

(e) We rewrite the sequence (7) as

$$0 \to C_p^{\delta} \to A^-_K \oplus C_p^{\tau} \xrightarrow{e} (A^-_L)^G \to 0.$$

Again by Kida, $e|_{A^-_K}$ is injective. So

$$(A^-_L)^G \cong A^-_K \oplus C_p^{\tau-\delta} \quad \text{and} \quad X_L^G = {}_p(A^-_L)^G \cong C_p^{\lambda^-_K - \delta + \tau}.$$

We treat first the case L/K unramified, i.e. all $\tau_i = 0$. Consider the chain of subspaces for $n \geqslant 1$,

$$(13) \quad {}_{p^n}X_L \supseteq {}_{(p^n-1)}X_L \supseteq \dots {}_{p^{n-1}}X_L \supseteq \dots \supseteq {}_{p^{n-2}}X_L \supseteq \dots \supseteq {}_pX_L \dots \supseteq {}_1X_L \supseteq 1.$$

By Lemma 2 parts (b) and (c)

$$\dim {}_{p^i}X_L = \lambda^-_{K_i} = (p^i-1)(\lambda^-_K - \delta) + \lambda^-_K,$$

this second equality by Kida's formula. Since by (12) the dimension of consecutive quotient spaces is nonincreasing from right to left, the only possibility to satisfy this formula for $\dim {}_{p^i}X_L$ for $i = 0, 1, \dots, n$ is

$$\dim({}_1X_L) = \lambda^-_K \quad \text{and} \quad \dim({}_iX_L/{}_{(i-1)}X_L) = \lambda^-_K - \delta \quad \text{for } i = 2, 3, \dots, p^n.$$

By (11) then $d_j = 0$ for $1 < j < p^n$ while $d_1 = \delta$ and $d_{p^n} = \lambda^-_K - \delta$. Therefore

$$X_L \cong (\lambda^-_K - \delta)\, L(p^n) \oplus \delta \cdot L(1),$$

confirming (10).

Next assume L/K is ramified at some non-p-prime which splits in K/K^+ or, in other words, some τ_i is nonzero. Consider the chain (13) from a different point of view:

$$(14) \quad {}_{p^n}X_L \dots \supseteq {}_{(p^n-p^m)}X_L \dots \supseteq {}_{(p^n-p^{m+1})}X_L \dots \supseteq {}_{(p^n-p^{n-1})}X_L \supseteq {}_{p^{n-1}}X_L \supseteq \dots {}_pX_L \dots \supseteq {}_1X_L \supseteq 1.$$

By Lemma 2 (a) we see that

$${}_{(p^n-p^j)}X_L = \mathrm{Ker}(N_{G_j}) \quad \text{on } X_L.$$

By (d) we see that $0 \to \mathrm{Ker}(N_{G_j}) \to X_L \to X_{K_j} \to 0$ is exact for $j \geqslant m$. So we have

$$\dim {}_{(p^n-p^j)}X_L = \dim X_L - \dim X_{K_j} \quad \text{for} \quad j \geqslant m,$$

or, better yet,

$$\dim {}_{(p^n-p^j)}X_L = \lambda^-_L - \lambda^-_{K_j}, \quad j \geqslant m.$$

By Kida's formula we can write this difference as

$$(15) \quad \dim {}_{(p^n-p^j)}X_L = \lambda^-_L - \lambda^-_{K_j} = (p^n-p^j)\Big(\lambda^-_K - \delta + \sum_{i=m}^{j-1} \tau_i\Big) + \sum_{i=j}^{n-1} \tau_i (p^n - p^i).$$

Next consider the space

$$_{(p^n-p^j+p^{j-1})}X_L \quad \text{for} \quad j \geqslant m.$$

This is the set of $x \in X_L$ annihilated by

$$(1-g)^{p^n-p^j}(1-g)^{p^{j-1}} = (1-g)^{p^n-p^j}(1-g^{p^{j-1}}).$$

In other words, it is the set (Lemma 2 (a)) of $x \in X_L$ such that $N_{G_j}(x)$ is fixed by G_{j-1}. Since N_{G_j} is surjective for $j \geqslant m$ (Lemma 2 (d)) and has kernel $_{(p^n-p^j)}X_L$, we have

$$[{}_{(p^n-p^j+p^{j-1})}X_L : {}_{(p^n-p^j)}X_L] = |X_{K_j}^{G_{j-1}}|, \quad j = m, \ldots, n.$$

Furthermore, we know that

$$\text{(16)} \quad \dim X_{K_j}^{G_{j-1}} = \begin{cases} \lambda_{K_{j-1}}^-, & j = m \text{ (Lemma 2 (c))}, \\ \lambda_{K_{j-1}}^- - \delta + \tau(K_j/K_{j-1}), & j > m \end{cases}$$

and

$$\tau(K_j/K_{j-1}) = \sum_{i=m}^{j-1} \tau_i p^i.$$

So for instance, let $j = n-1$. By (15) we have

$$\text{(17)} \quad \dim {}_{(p^n-p^{n-1})}X_L = (p^n-p^{n-1})(\lambda_K^- - \delta + \sum_{i=m}^{n-2} \tau_i) + \tau_{n-1}(p^n-p^{n-1})$$
$$= (p^n-p^{n-1})(\lambda_K^- - \delta + \sum_{i=m}^{n-1} \tau_i).$$

By (16) with $j = n$, we get

$$\dim {}_{(p^n-1)}X_L = \lambda_{K_{n-1}}^- - \delta + \sum_{i=m}^{n-1} \tau_i p^i$$
$$= (p^{n-1}(\lambda_K^- - \delta) + \delta + \sum_{i=m}^{n-1} \tau_i(p^{n-1}-p^i)) - \delta + \sum_{i=m}^{n-1} \tau_i p^i$$
$$= p^{n-1}(\lambda_K^- - \delta + \sum_{i=m}^{n-1} \tau_i).$$

Recalling that in (14), consective quotient spaces have nonincreasing dimension, we see that

$$= \dim({}_iX_L/{}_{(i-1)}X_L) = \lambda_K^- - \delta + \sum_{i=m}^{n-1} \tau_i$$

for all $0 < i \leqslant p^n - p^{n-1}$.

In the same manner one can show that

$$\dim({}_iX_L/{}_{(i-1)}X_L) = \lambda_K^- - \delta + \sum_{i=m}^{j-1} \tau_i$$

for $p^n - p^j + 1 \leqslant i \leqslant p^n - p^{j-1}$; $j = m+1, \ldots, n-1$.

It remains to determine $\dim({}_iX_L/{}_{(i-1)}X_L)$ for $p^n - p^m \leqslant i \leqslant p^n$.

By (15) we have

$$\dim({}_{(p^n-p^m)}X_L) = \lambda_L^- - \lambda_{K_m}^-$$

while by (16),

$$\dim({}_{(p^n-p^m+p^{m-1})}X_L/{}_{(p^n-p^m)}X_L) = \lambda_{K_{m-1}}^- = (p^{m-1}-1)(\lambda_K^- - \delta) + \lambda_K^-.$$

Since $\dim({}_{p^n}X_L) = \lambda_L^-$,

$$\dim({}_{p^n}X_L/{}_{(p^n-p^m)}X_L) = \lambda_{K_m}^- = (p^m-1)(\lambda_K^- - \delta) + \lambda_K^-.$$

Since (1) there are p^m consecutive quotients from $_{p^n}X_L$ to $_{(p^n-p^m)}X_L$ and p^{m-1} consecutive quotients from $_{(p^n-p^m+p^{m-1})}X_L$ to $_{(p^n-p^m)}X_L$, (2) the dimension of consecutive quotients is nonincreasing, and (3) $0 \leqslant \delta \leqslant 1$, it follows that

$$\dim({}_iX_L/{}_{(i-1)}X_L) = \begin{cases} \lambda_K^- - \delta & \text{for} \quad p^n - p^m + 1 < i \leqslant p^n, \\ \lambda_K^- & \text{for} \quad i = p^n - p^m + 1. \end{cases}$$

Thus we have determined d_i for $i = 1, \ldots, p^n$:

$d_{p^n} = \lambda_K^- - \delta$,

$d_{p^n-p^j} = \tau_j$; $j = m+1, \ldots, n-1$,

$d_{p^n-p^m} = \tau_m - \delta$,

$d_{p^n-p^m+1} = \delta$,

$d_i = 0$ otherwise

from which (10) follows.

4. In Section 2 we determined the integral representation type of A_L^- over $G = \mathrm{Gal}(L/K)$ for $G \cong C_p$. In this section, we will do the same for $G \cong C_{p^2}$. So assume $G \cong C_{p^2}$ and let $H \subseteq G$ be the subgroup of order p and let E be the fixed field of H. The decomposition of A_L^- as a $\mathbf{Z}_p[H]$-module is given by Theorem 1, as is the decomposition of A_E^- as a $\mathbf{Z}_p[G/H]$-module. The following lemma is crucial to the analysis of A_L^- as a $\mathbf{Z}_p[G]$-module. Let h generate H.

LEMMA 3. *As modules over $\mathbf{Z}_p[G/H]$, A_E^- and $A_L^-/(A_L^-)^{1-h}$ are isomorphic.*

Proof. Let $\eta = \eta_H$: $A_L^- \to A_E^-$ be induced by taking norms of ideals from L to E. Since A_E^- is divisible and $Im(\eta)$ clearly has finite index in A_E^-, η must be surjective. Let $\mathfrak{a} \in I_L$ be such that the class of $\mathfrak{a}$ is in the kernel of η.

Thus $\eta(\mathfrak{a}) = (a)$ for $a \in E^\times$. Recall that every element of $E^\times$ is a norm from $L^\times$ (e.g. [3]) and let $a = \eta(b)$. Replacing $\mathfrak{a}$ by $(b^{-1})\mathfrak{a}$, we see that every class in $\mathrm{Ker}(\eta)$ is represented by an $\mathfrak{a}$ such that $\eta(\mathfrak{a}) = (1)$. Consequently, $\mathfrak{a} = \mathfrak{b}^{1-h}$ for some $\mathfrak{b} \in I_L$ and the class of $\mathfrak{a}$ is in $(A_L^-)^{1-h}$. So $\mathrm{Ker}(\eta) \subseteq (A_L^-)^{1-h}$ and the converse is obvious. Hence η induces an isomorphism $A_L^-/(A_L^-)^{1-h} \to A_E^-$ and commutes with the action of G/H.

Let us pass again to the duals $Y_L = \mathrm{Hom}_{\mathbf{Z}_p}(A_L^-, \mathbf{Q}_p/\mathbf{Z}_p)$ and the same for Y_E, Y_K. Also let $Y_i = \mathrm{Hom}_{\mathbf{Z}_p}(A_i, \mathbf{Q}_p/\mathbf{Z}_p)$ for $i = 1, p-1, p$. Then Lemma 3 asserts that Y_E and Y_L^H are isomorphic as G/H-modules. Theorem 1 tells us the H-structure of Y_L^H and the G/H-structure of $Y_L \cong Y_E$. We can determine the G-structure of Y_L in terms of Reiner's classification of C_{p^2}-indecomposables ([2]). Let us summarize that classification. Let $Z = \mathbf{Z}_p$ with trivial G-action; $\mathscr{E} = \mathbf{Z}_p[G/H]$; $R_i = \mathbf{Z}_p[x]/\Phi_{p^i}(x)$, $i = 1, 2$; where $\Phi_{p^i}(x)$ is the cyclotomic polynomial and a generator of G acts on R_i via multiplication by x. Up to isomorphism, the $4p+1$ indecomposable $\mathbf{Z}_p$-free $\mathbf{Z}_p[G]$-modules are given in column 1 of Table 1. The notation $(N, L; r)$ denotes a module M determined by $L = M^H$, $0 \to L \to M \to N \to 0$ is exact, and $r \in \mathrm{Ext}^1_{\mathbf{Z}_p[G]}(N, L)$ is the extension class of M.

Column 2 of Table 1 gives the structure of M/pM as an $\mathbf{F}_p[G]$-module; $L(n)$ denotes the module $\mathbf{F}_p[x]/(x-1)^n$. (We are indebted to Alfredo Jones for the data in this column.) From this information it is easy to compute the form of M/pM over $\mathbf{F}_p[H]$ and, subsequently, the decomposition of M over $\mathbf{Z}_p[H]$. This last is given in column 3.

THEOREM 4. *Let L/K be a cyclic extension of degree p^2 of $\mathbf{Z}_p$-fields, p odd, of CM-type. Let $G = \mathrm{Gal}(L/K)$, τ_0 (resp. τ_1) = number non-p-primes of K^+ which are split in K/K^+ and totally (resp. partially) ramified in L/K. Assume that $\mu_K^- = 0$. As a $\mathbf{Z}_p[G]$-module, A_L^- is isomorphic to*

$$R_2^{\tau_1} \oplus (R_2, R_1;\ \lambda^0)^{\tau_0 - \delta} \oplus (R_2, \mathscr{E};\ \lambda^0)^{\lambda_K^-} \quad \textit{for} \quad \tau_0 > 0,$$

$$R_2^{\tau_1 - \delta} \oplus (R_2, Z;\ 1)^{\delta} \oplus (R_2, \mathscr{E};\ \lambda^0)^{\lambda_K^- - \delta} \quad \textit{for} \quad \tau_0 = 0,\ \tau_1 > 0,$$

and

$$Z^{\delta} \oplus (R_2, \mathscr{E};\ \lambda^0)^{\lambda_K^- - \delta} \quad \textit{for} \quad \tau_0 = \tau_1 = 0.$$

Remark. $(R_2, \mathscr{E};\ \lambda^0) \cong \mathbf{Z}_p[G]$.

Proof. We sketch out only the first case: $\tau_0 > 0$. By Theorem 1 and the dual of Lemma 3, we see that as a $\mathbf{Z}_p[H]$-module

$$Y_L \cong Y_p^{\lambda_E^-} \oplus Y_{p-1}^{\tau - \delta} \tag{18}$$

where $\tau = \tau_0 + p\tau_1$ while as a $\mathbf{Z}_p[G/H]$-module

$$Y_L^H \cong Y_p^{\lambda_K^-} \oplus Y_{p-1}^{\tau_0 - \delta}. \tag{19}$$

Now we search Table 1 for those indecomposable M for which M^H does not involve X_1 and which over H do not involve X_1. There are only three possibilities: R_2, $(R_2, R_1;\ \lambda^0)$, $(R_2, \mathscr{E};\ \lambda^0)$.

From $Y_L \cong R_2^x \oplus (R_2, R_1;\ \lambda^0)^y \oplus (R_2, \mathscr{E};\ \lambda^0)^z$ we deduce that

$$Y_L^H \cong R_1^y \oplus \mathscr{E}^z = Y_{p-1}^y \oplus Y_p^z$$

while over H,

$$Y_L \cong Y_{p-1}^{px} \oplus (Y_p^{p-1} \oplus Y_{p-1}^1)^y \oplus Y_p^{pz}.$$

Comparing these expressions with (18) and (19) (recalling that $\lambda_E^- = p\lambda_K^- + (p-1)(\tau_0 - \delta)$), we determine x, y, z to be as stated in the theorem.

Table 1

M/G	M/pM over $\mathbf{F}_p[G]$	$M/H \cong Y_p^a \oplus Y_{p-1}^b \oplus Y_1^c$ $(a, b, c) =$
R_2	$L(p^2-p)$	$(0, p, 0)$
R_1	$L(p-1)$	$(0, 0, p-1)$
Z	$L(1)$	$(0, 0, 1)$
$\mathscr{E}$	$L(p)$	$(0, 0, p)$
(R_2, Z)	$L(p^2-p+1)$	$(1, p-1, 0)$
$(R_2, R_1;\ \lambda^i)$, $0 \leqslant i \leqslant p-2$	$L(p^2-i-1) \oplus L(i)$	$(p-i-1, i+1, i)$
$(R_2, \mathscr{E};\ \lambda^i)$, $0 \leqslant i \leqslant p-1$	$L(p^2-i) \oplus L(i)$	$(p-i, i, i)$
$(R_2, Z \oplus R_1;\ \lambda^i)$, $0 \leqslant i \leqslant p-2$	$L(p^2-i-1) \oplus L(i+1)$	$(p-i-1, i+1, i+1)$
$(R_2, Z \oplus \mathscr{E};\ \lambda^i)$, $1 \leqslant i \leqslant p-2$	$L(p^2-i) \oplus L(i+1)$	$(p-i, i, i+1)$

References

[1] C. Chevalley and A. Weil, *Über das Verhalten der Integrale erster Gattung bei Automorphismen des Funktionenkörpers*, Hamburger Abhandlungen 10 (1934), pp. 358–361.

[2] C. W. Curtis and I. Reiner, *Methods of Representation Theory*, Vol. I, John Wiley & Sons, New York 1981.

[3] J. D'Mello and M. Madan, *Class group rank relations in Z_l-extensions*, Manuscripta Math. 41 (1983).

[4] R. Gold and M. Madan, *An application of a theorem of Deuring and Shafarevich*, Mat. Z. 191 (1986), pp. 247–251.

[5] K. Iwasawa, *Riemann–Hurwitz formula and p-adic Galois representations for number fields*, Tôhoku Math. J. (2) 33 (1981), pp. 263–288.

[6] Y. Kida, *l-extensions of CM-fields and cyclotomic invariants*, J. Number Theory 12 (1980), pp. 519–528.

DEPARTMENT OF MATHEMATICS
OHIO STATE UNIVERSITY
COLUMBUS, OHIO

Received on 13.9.1984
and in revised form on 7.3.1985 (1453)