J. CARROLL
H. KISILEVSKY
On the Iwasawa invariants of certain $\mathbb{Z}_p$-extensions


<http://www.numdam.org/item?id=CM_1983__49_2_217_0>
ON THE IWASAWA INVARIANTS OF CERTAIN
$Z_p$-EXTENSIONS

J. Carroll and H. Kisilevsky*

Let $k$ be a finite extension of the rational number field, $\mathbb{Q}$. For prime $p$, let $K/k$ be a $Z_p$-extension, i.e. $K/k$ is a Galois extension and $\text{Gal}(K/k) = \Gamma$ is topologically isomorphic to the additive group of the ring, $Z_p$, of all $p$-adic integers. Let $L$ be the maximal abelian unramified $p$-extension of $K$, and denote by $X$ the group $\text{Gal}(L/K)$. The $X$ has a natural action of $\Gamma$ and by fixing a topological generator $\sigma$ of $\Gamma$, $X$ becomes a $A = Z_p[[T]]$ module under the correspondence $\sigma \leftrightarrow 1 + T$. From the theory of $Z_p$-extensions ([3]) it follows that $X$ is pseudo-isomorphic to an elementary $A$-module $E$ of the form

$$E \cong A/T^{a_1} + \ldots + A/T^{a_r} + \sum A/(f_i)^{n_i}$$

where $f_i = p$ or $f_i$ is a distinguished irreducible polynomial in $Z_p[T]$ such that $f_i(0) \neq 0$. If $g(T) = T^s p^a f(T)$ where $s = a_1 + \ldots + a_r$, $f(T) = \prod f_i^n$, then $\mu = \mu(K/k)$ and the degree of $g(T) = \lambda(K/k)$ are the Iwasawa invariants of the $Z_p$-extension $K/k$. In this paper we study the invariants $a_1, \ldots, a_r$ of the module $X$ for certain $Z_p$-extensions introduced in [4]. We note that it is easy to prove that any $Z_p$-extension $K/k$ such that $K/\mathbb{Q}$ is normal, is the compositum of such a $Z_p$-extension with $k$.

Let $k$ be a totally complex abelian extension of $\mathbb{Q}$ with Galois group $\text{Gal}(k/\mathbb{Q}) = \Delta$. Let $p$ be an odd prime such that $p^{r-1} = 1$ for every element $\tau \in \Delta$, i.e. $p - 1$ is divisible by the exponent of the group $\Delta$. Denote by $\hat{\Delta}$ the group of all homomorphisms of $\Delta$ into the group $W$ of all $(p - 1)^{st}$ roots of unity in $Z_p$. Finally denote by $J$ the automorphism of $k$

* Research sponsored in part by an NSERC grant.
given by complex conjugation under some fixed embedding of an algebraic closure $\mathbb{Q}$ into the complex field, $\mathbb{C}$.

Then as is shown [4] for every character $\chi \in \hat{\Delta}$ such that either $\chi = \chi_0$ the trivial character, or $\chi(J) = -1$, there exists a uniquely define $\mathbb{Z}_p$-extension $K_\chi/k$, such that $K_\chi/Q$ is normal. In fact $\text{Gal}(K_\chi/Q)$ is isomorphic to a semi-direct product $\Delta \cdot \Gamma$, where $\Gamma = \text{Gal}(K_{\chi_0}/k)$ and $\Delta$ is the fixed lifting of $\text{Gal}(k/Q)$ to $\text{Gal}(K_\chi/Q)$ which contains $J$, and such that $\tau \gamma^{-1} = \gamma^{x_0}$ for each $\tau \in \Delta$, $\gamma \in \Gamma$. Hence $K_{\chi_0}/k$ is the cyclotomic $\mathbb{Z}_p$-extension and for $\chi \nmid \chi_0$, $K_\chi/Q$ is a non-abelian extension. It is shown in [4] for the polynomial $g(T) = T^s f(T)$ that $\deg(f(T))$ is congruent to 0 modulo the order of $\chi$ in $\hat{\Delta}$ so that $\lambda(K/k)$ is congruent to $s$ modulo the order of $\chi \in \hat{\Delta}$.

In section 1 we compute the number of factors in $X$ of the form $A/T^a$, and in section 2 we prove that $a = 1$ when the decomposition group $D(p)$ of $p$ in $\Delta$ is contained in the kernel of $\chi$.

We shall use the following conventions. If $A, B$ are profinite $p$-groups then $\phi: A \to B$ is a pseudo-isomorphism if $\phi$ has finite kernel and cokernel, and we write $A \sim B$. If $\{A_n\}, \{B_n\}$ are two sequences of finite groups then we shall write $A_n \sim B_n$ to mean that there are homomorphisms $\phi_n: A_n \to B_n$ whose kernels and cokernels have orders bounded independently of $n$. Such sequences shall arise naturally when $A = \lim_{\leftarrow} A_n$, $B = \lim_{\leftarrow} B_n$ and $A \sim B$. Finally if $|A_n|, |B_n|$ are the orders of $A_n$ and $B_n$ respectively we write $|A_n| \sim |B_n|$ to mean that the quotients $|A_n|/|B_n|$, $|B_n|/|A_n|$ are bounded independently of $n$, so for example if $A_n \sim B_n$, then $|A_n| \sim |B_n|$.

**Section 1**

Fix a character $\chi \in \hat{\Delta}$, such that $\chi = \chi_0$ or $\chi(J) = -1$, and let $K_\chi/k$ be the $\mathbb{Z}_p$-extension discussed above. Then $K_\chi = \bigcup_{n \geq 0} k_n$, where $k = k_0 \subseteq k_1 \subseteq \ldots \subseteq k_n \subseteq \ldots \subseteq K_\chi$, and each $k_n$ is a cyclic extension of $k$ of degree $p^n$. Denote by $A_n$ the $p$-primary subgroup of the ideal class group of $k_n$ so that $X \simeq \lim_{\leftarrow} A_n$, the inverse limit being taken with respect to the norm maps $N_{m,n}$ between the layers $k_m$ and $k_n$ of $K_\chi$.

Define $\tau X = \{x \in X| \tau(x) = 0\} = \{x \in X| \gamma(x) = x, \text{ for all } \gamma \in \Gamma\}$. Then it is easily seen that $\tau X \sim A/T + \ldots + A/T (r \text{ factors})$ where $X \sim A/T^{a_1} + \ldots + A/T^{a_r} + \sum_{f \neq T} A/(f)$. Since $\tau X = \lim_{\leftarrow} A_n^{\text{Gal}(k_n/k)}$, it is sufficient to compute the asymptotic order of the groups $A_n^{\text{Gal}(k_n/k)}$ where $A_n^{\text{Gal}(k_n/k)} = \{a \in A_n| \sigma(a) = a \text{ for all } \sigma \in \text{Gal}(k_n/k)\}$. Since $k_n/k$ is cyclic of degree $p^n$,
it follows from classical genus theory, that

$$|A_n^{\text{Gal}(k_n/k)}| = \frac{|A_0| \cdot \prod_{i=1}^{t} e_i}{p^n[E_0 : N(k_n^* \cap E_0)]}$$

where $A_0 = p$-primary part of the class group of $k$, $e_1, \ldots, e_t$ the ramification indices of the primes $p_1, \ldots, p_t$ of $k_0$ ramified in $k_n$, $E_0$ is the group of units of $k$, and $N(k_n^*)$ is the group $N_{n,0}(k_n^*)$ of elements of the multiplicative group $k^*$ which are norms from $k_n^*$.

Since $k_n/Q$ is a normal extension and all primes $p_1, \ldots, p_t$ of $k$ dividing $p$ eventually ramify in $k_n$, we see that

**Remark 1:** If there is exactly one prime of $k_0$ dividing $p$, $t = 1$ and it follows that $|A_n^{\text{Gal}(k_n/k)}|$ is bounded. Consequently $\tau X$ is finite and so $r = 0$, i.e. $X \sim \sum_{f \in \tau} A(f_i)$.

This occurs for the field $k = \mathbb{Q}(\zeta_p)$, the cyclotomic field of $p$th roots of unity.

**Remark 2:** If $k = \mathbb{Q}(\sqrt{D})$ is a complex quadratic field of discriminant $D < 0$, then $E_0$ is finite, hence $[E_0 : N(k_n^* \cap E_0)]$ is bounded. It follows that $|A_n^{\text{Gal}(k_n/k)}| \sim p^{(t-1)n}$ where $t$ is the number of primes of $k$ which divide $p$. Hence in this case, $r = t - 1$ (c.f. Iwasawa [3]). Explicitly $r = 1$ if $(D/p) = +1$ and $r = 0$ if $(D/p) = -1$ or $p$ divides $D$, where $(D/p)$ is the Kronecker symbol.

In general we must compute the asymptotic orders of the groups $E_0/N(k_n^* \cap E_0)$. Since $E_0$, and $N(k_n^*)$ are subgroups of $k_n^*$ which are stable under the action of $\Delta$, we shall obtain the orders of these groups by studying the $\mathbb{Z}_p[\Delta]$-module structure of certain associated groups.

For $\psi \in \hat{\Delta}$, let

$$\varepsilon_\psi = \frac{1}{|\Delta|} \sum_{\tau \in \Delta} \psi(\tau)^{-1}$$

Since the exponent of $\Delta$ divides $p - 1$, $\varepsilon_\psi$ belongs to $\mathbb{Z}_p[\Delta]$ for each $\psi \in \hat{\Delta}$ and together they form a complete set of primitive orthogonal idempotents of $\mathbb{Z}_p[\Delta]$. If $M$ is any $\mathbb{Z}_p[\Delta]$-module, $M$ can be decomposed
\[ M = \sum_{\psi \in \Delta} \epsilon_\psi M \]

where \( \epsilon_\psi M = \{ m \in M | \tau(m) = \psi(\tau)m, \text{ for all } \tau \in \Delta \} \).

Let \( p_1, \ldots, p_t \) be the primes of \( k_0 \) which divide \( p \), and let \( F_1, \ldots, F_t \) be the completions of \( k \) at \( p_1, \ldots, p_t \), respectively. Let \( U_i \subseteq F_i \) be the group of units of \( F_i \) congruent to 1 modulo \( p_i \), and let \( U = U_1 \times \ldots \times U_t \). Then \( U \) is a compact topological group which is a \( \mathbb{Z}_p[\Delta] \)-module in a natural way, namely if \( u = (u_1, \ldots, u_t) \in U \), and \( \tau \in \Delta \), then \( \tau(u) \) has \( \tau(u_i) \) in the \( p_i \) component if \( \tau(p_i) = p_i \). Furthermore we may embed \( E_0 \) into \( U \) diagonally so that \( E_0 \) is a \( \Delta \)-submodule of \( U \). Let \( \bar{E}_0 \) be the closure of \( E_0 \) in the topological group \( U \). Since \( \Delta \) is abelian, Brumer's theorem [1] on the Leopoldt conjecture implies that \( \bar{E}_0 \cong \mathbb{Z}_p[\Delta]^{-1} \). One can show that \( U \) contains a subgroup of finite index which is isomorphic to \( \mathbb{Z}_p[\Delta] \) as \( \mathbb{Z}_p[\Delta] \)-modules so that \( \epsilon_\psi U \cong \mathbb{Z}_p \) for every \( \psi \in \Delta \), (c.f. [4]). It is also known that there exists a totally real unit \( \eta \in E_0 \), such that the conjugates \( \tau(\eta) \) of \( \eta \), \( \tau \in \Delta \), generate a subgroup of finite index of \( E_0 \). If follows that the closed submodule of \( \bar{E}_0 \) generated by the elements \( \tau(\eta), \tau \in \Delta \), has finite index in \( \bar{E}_0 \) and is a cyclic \( \mathbb{Z}_p[\Delta] \)-module. Furthermore, since \( \eta \) is totally real, and \( \prod \tau(\eta) = 1 \), one sees that

\[
\epsilon_\psi \bar{E}_0 \cong \mathbb{Z}_p \quad \text{if } \psi(J) = +1, \psi = \chi_0
\]

\[
\epsilon_\psi \bar{E}_0 \cong 1 \quad \text{if } \psi(J) = -1 \text{ or } \psi = \chi_0
\]

Hence \( \bar{E}_0 \cong \sum_\psi \epsilon_\psi U \), the sum taken over \( \psi \in \Delta \), \( \psi(J) = +1 \) and \( \psi \equiv \chi_0 \).

Let \( D = D(p) \subseteq \Delta \) be the decomposition group of the prime \( p \) in \( \Delta \). If \( \psi \in \Delta \), we denote by \( \psi|D \) the character of \( D \) obtained by restricting \( \psi \) to \( D \). Let \( \bar{N}_n \) be the closure in \( U \) of the group \( N(k_0^*) \cap E_0 \).

**Lemma 1:**

\[ \bar{N}_n \cong \sum_{\psi_1} \epsilon_{\psi_1} U + \sum_{\psi_2} p^r \epsilon_{\psi_2} U \]

where the first sum runs over \( \psi_1 \in \Delta \) such that \( \psi_1(J) = +1, \psi_1 \equiv \chi_0 \) and \( \psi_1|D \equiv \chi|D \), and the second sum is taken over \( \psi_2 \in \Delta \), such that \( \psi_2(J) = +1, \psi_2 \equiv \chi_0 \), and \( \psi_2|D = \chi|D \).

**Proof:** We first note that \( k_n/k_0 \) is a cyclic extension of degree \( p^n \) which is unramified at all primes \( q \neq p_1, \ldots, p_t \). Hence by the Norm theorem an element \( \alpha \in k_0 \) is a norm from \( k_n \) if and only if it is a local norm at all completions of \( k \). In particular since \( k_n/k \) is unramified at all primes of \( k \) not dividing \( p \), a unit \( \mu \) is a norm from \( k_n \) if and only if \( \mu \) is a
local norm at the completion of $k_n/k$ at the primes $p_1, \ldots, p_t$. For each such prime $p_i$, let $F_{n,i} \supseteq F_i$ be a fixed completion of $k_n$ at some prime of $k_n$ dividing $p_i$. Let $M_n$ be the subgroup of $U$ which in the $p_i$ component is the group $N_n(U_{n,i})$ where $U_{n,i}$ is the group of units of $F_{n,i}$ congruent to 1 modulo the maximal ideal and $N_n$ denotes the norm map from $F_{n,i}$ to $F_i$ so

$$M_n = N_n(U_{n,1}) \times \cdots \times N_n(U_{n,t}).$$

By local class field theory $M_n \subseteq U$ is a closed and open subgroup of $U$, and $N(k^*_n) \cap E_0 \subseteq M_n$. On the other hand let $\alpha \in M_n \cap E_0$, and let $O_\alpha$ be any neighborhood of $\alpha$ in $U$. Since $M_n \subseteq U$ is open, we may suppose $O_\alpha \subseteq M_n$. As $\alpha \in E_0$, there is an $\epsilon \in O_\alpha \cap E_0 \subseteq M_n \cap E_0$. But the norm theorem then implies that $\epsilon \in N_n(k^*_n) \cap E_0$ and so $\alpha$ must be in $N_n$. Since $E_0 \sim \sum \epsilon_{\psi} U$ the sum taken over $\psi \in A$, such that $\psi(J) = +1, \psi \neq \chi_0$, it suffices to compute $M_n$.

Note that for each $p_i$ dividing $p$, the extension $k_n/k$ is ramified at $p_i$ (for $n$ sufficiently large) and the ramification index of $p_i$ in $k_n$ is asymptotically equal to $p^n$, so that the local extension $F_{n,i}/F_i$ is essentially totally ramified. Furthermore $k/Q_p$ is a galois extension with $\text{Gal}(k/Q_p) \simeq D = D(p)$. In addition $F_{n,i}/Q_p$ is a normal extension satisfying

$$\tau \sigma \tau^{-1} = \sigma^{\tau(t)} \text{ for } \sigma \in \text{Gal}(F_{n,i}/F_i),$$

$$\tau \in \text{Gal}(F_i/Q_p) = D(p)$$

Therefore by local class field theory, we see that

$$\text{Gal}(F_{n,i}/F_i) \simeq F_i^*/N_n(F_i^*) \text{ as } D(p)	ext{-modules}$$

$$\sim U_i/N_n(U_{n,i}) \text{ since } F_{n,i}/F_i \text{ is almost totally ramified}.$$

Now, as before, we can write

$$U_i = \sum \epsilon_{\psi'} U_i$$

where $\epsilon_{\psi'}$ are the primitive idempotents in $Z_p[D]$, and $\psi'$ run over the characters of $D \subseteq \Delta$. As before one sees that $\epsilon_{\psi'} U_i \sim Z_p$ for each character $\psi'$ of $D$ so that it follows that

$$N_n(U_{n,i}) \sim \sum_{\psi \notin \chi} \epsilon_{\psi'} U_i + p^n \epsilon_{\chi} U_i$$
where $\chi'$ is the character of $D$ given by $\chi' = \chi | D$. Hence

$$M_n \sim \sum_{\psi_1} \psi_1 U + \sum_{\psi_2} p^n \psi_2 U$$

where the first sum is taken over characters $\psi_1$ of $\Lambda$ such that $\psi_1 | D \not\cong \chi | D$ and the second sum is over characters $\psi_2$ of $\Lambda$ such that $\psi_2 | D \not\cong \chi | D$. Finally since $\bar{N}_n = M_n \cap \bar{E}_0$, the statement of the lemma follows.

To compute the group order $[E_0 : N(k^n) \cap E_0]$ we note that $\bar{E}_0 = E_0 \cdot \bar{N}_n$ and that $N(k^n) \cap E_0 \subseteq \bar{N}_n \cap E_0 \subseteq M_n \cap \bar{E}_0 \cap E_0 \subseteq M_n \cap E_0 \subseteq N(k^n) \cap E_0$, the last inequality being given by the norm theorem. Therefore $E_0 / N(k^n) \cap E_0 \cong E_0 / \bar{N}_n$. From the lemma, it follows that $|E_0 / \bar{N}_n| \sim p^n$ where $a$ is the number of characters $\psi_2$ of $\Lambda$ such that $\psi_2(J) = +1$, $\psi_2 \not\cong \chi_0$, and $\psi_2 | D = \chi | D$. Therefore, we see that $|A_n^{\text{Gal}(k^n/k)}| \sim p(t-a-1)n$ and so we have proved the following theorem:

**THEOREM 1:** Let $K_\chi/k$ be the $\mathbf{Z}_p$-extension defined in the introduction, and let $X$ be the galois group of the maximal abelian unramified $p$-extension of $K_\chi$. Then $|X| \sim Z_p^r$ where $r$ is given below:

(a) $\chi \cong \chi_0$, \hspace{1cm} $J \in D(p)$ \hspace{1cm} then $r = t - 1$

(b) $\chi \not\cong \chi_0$, \hspace{1cm} $J \in D(p), \chi | D = \chi_0 | D$ \hspace{1cm} then $r = t/2$

(c) $\chi = \chi_0$, \hspace{1cm} $J \in D(p)$, \hspace{1cm} then $r = 0$

(d) $\chi = \chi_0$, \hspace{1cm} $J \in D(p)$, \hspace{1cm} then $r = t/2$.

---

**Section 2**

In this section we again consider the $\mathbf{Z}_p$-extension $K_\chi/k$, for a character $\chi \in \Lambda$, with $\chi(J) = -1$ or $\chi = \chi_0$. In §1 we investigated the submodule $X_0$ of $X$, $X_0 = \{x \in X | T^k x = 0 \text{ some } k \geq 1\}$. In this section we prove:

**THEOREM 2:** Let $K_\chi/k$ be the $\mathbf{Z}_p$-extension described above. If $D(p)$ (= the decomposition group of $p$ in $\Lambda$) is contained in the kernel of $\chi$ then $X_0$ is a semi-simple $\Lambda$-module.

Note: The case $\chi = \chi_0$ is treated in [2].

To this end we consider the extension $L/K$, the maximal abelian unramified $p$-extension of $K$ such that every prime of $K$ dividing $p$ splits completely in $L$. Then $K \subseteq L \subseteq L$ and it is shown (Iwasawa [3]) that $\text{Gal}(L/L) \sim \Lambda/\xi_1 \times \ldots \times \Lambda/\xi_k$, where each $\xi_i$ is a distinguished irre-
ducible polynomial, and \( \xi_i(T) \) divides \( (T + 1)^{n_0} - 1 \) for some integer \( n_0 \).

It follows that \( \text{Gal}(L/L) \) has no submodule pseudo-isomorphic to \( \Lambda/T^2 \).

Hence in order to prove the theorem, it is sufficient to prove that the divisor of \( X' = \text{Gal}(L/K) \) is prime to \( (T) \), or equivalently that \( \tau X' \) is finite.

Consider in \( k_n \), the subgroup \( D_n \subseteq A_n \) of all ideal classes of \( p \)-power order which are represented, modulo principal ideals, by a product of primes dividing \( p \). Let \( A'_n = A_n/D_n \) so that by class field theory, \( A'_n \) corresponds to the maximal abelian unramified \( p \)-extension of \( k_n \) in which all primes dividing \( p \) are completely split. Therefore \( \lim_{n} A'_n \cong X' \), the inverse limit again taken with respect to the norm maps. It is therefore sufficient to prove that the orders

\[
|A'^{\text{Gal}(k_n/k_0)}|
\]

remain bounded for all \( n \).

We shall need the following version of the classical results of genus theory. Let \( F \) be a number field and let \( S \) be a finite set of primes of \( F \) including the Archimedean primes. Denote by \( I_S = I_{F,S} \) the (multiplicative) group of ideals of \( F \) generated by the finite primes of \( S \), so that \( I_S \subseteq I_F \) is a subgroup of the group of all ideals \( I_F \). Denote by \( I_F = I_F/I_S \), \( P'_F = P_F I_S/I_S \) where \( P_F \) is the group of principal ideals of \( F \) and \( C'_F = I_F/P'_F \) the \( S \)-class group of \( F \). Finally let \( E'_F = \{ \alpha \in F* | (\alpha) \in I_S \} \) where \( (\alpha) \) is the principal ideal generated by \( \alpha \). For an extension \( M/F \) we again let \( S \) denote the set of all primes of \( M \) which divide primes of \( S \).

**Lemma 2:** Let \( M/F \) be a cyclic extension of degree \( d \), then

\[
|C_M^{\text{Gal}(M/F)}| = \frac{|C'_F| \prod n_p \prod e_p}{d[E'_F : E' \cap N(M*)]}
\]

where \( \prod n_p \) is the product of the local degrees of primes \( p \in S \), \( \prod e_p \) is the product of the ramification indices of those primes of \( F \) not in \( S \).

**Proof:** Let \( G = \text{Gal}(M/F) \). From the exact \( G \)-sequence,

\[
0 \to P'_M \to I'_M \to C'_M \to 0
\]

we obtain the exact sequence

\[
0 \to (P'_M)^G \to (I'_M)^G \to (C'_M)^G \to H^1(G, P'_M) \to 0
\]
since $H^1(G, I_M) = 0 = H^1(G, I_M)$. Hence

$$|(C'_M)^G| = |(I'_M)^G : (P'_M)^G| \cdot |H^1(G, P'_M)|$$

We then have

$$|(C'_M)^G| = \frac{|(I'_M)^G : I'_F| \cdot |I'_F : P'_F|}{|(P'_M)^G : P'_F|} \cdot |H^1(G, P'_M)|$$

Now $[I'_F : P'_F] = |C'_F|$. To compute $(I'_M)^G/I'_F$, we let $a' \in (I'_M)^G$, and let $a$ be an ideal of $M$, representing $a'$. Since $\sigma(a') = a'$ for $\sigma \in G$, we must have

$$\sigma(a)/a \in I_{M,S}$$

So that there exists an ideal $b \in I_{M,S}$

$$\sigma(a)/a = b$$

This implies that $N_{M/F}(b) = 1$. Since $H^{-1}(G, I_{M,S}) = 0$, there is an ideal $c \in I_{M,S}$ such that $b = c/\sigma(c)$, so that $a \cdot c \in I_M^G$. It now follows that $(I'_M)^G = I_M^G I_{M,S}/I_{M,S}$ so that the following sequence is exact:

$$0 \to I_F^G I_{M,S}/I_F \to (I'_M)^G/I_F \to (I'_M)^G/I_M \to 0$$

But $[(I'_M)^G : I_F]$ is the product of the ramification indices over all primes of $F$ ramified in $M$, and $[I_F I_{M,S}^G : I_F]$ is equal to the product of the ramification indices over all primes of $S$ (in $F$) ramified in $M$, hence $[(I'_M)^G : I_F^G]$ is the product of ramification indices over all primes of $F$, not in $S$, ramified in $M$.

From the exact $G$ sequence

$$0 \to E'_M \to M^* \to P'_M \to 0$$

we obtain the exact sequence of cohomology groups

$$0 \to (E'_M)^G \to F^* \to (P'_M)^G \to H^1(G, E'_M) \to 0 \to H^1(G, P'_M)$$

$$\to H^2(G, E'_M) \to H^2(G, M^*)$$

Thus we obtain $H^1(G, E'_M) \cong (P'_M)^G/P'_F$ and

$$H^1(G, P'_M) \cong \ker(E'_F/N(E'_M) \to F^*/N(M^*))$$

$$= E'_F \cap N(M^*)/N(E'_M)$$
Now

\[ [E_F \cap N(M^*) : N(E'_M)] = \frac{|H^0(G, E_M)|}{[E'_F : E_F \cap N(M^*)]} \]

and the Herbrand quotient

\[ \frac{|H^0(G, E_M)|}{|H^1(G, E'_M)|} \]

is known to be equal to \( \frac{1}{d} \prod_{p \in S} n_p, \)

where \( n_p \) = local degree of the prime \( p \) for the extension \( M/F \). Therefore

\[ |(C'_M)^G| = \frac{|C'_F|}{d} \prod_{p \in S} n_p \prod_{p \in S} e_p \left[ N(E'_0 : E'_0 \cap N(k^*_p)) \right]. \]

We shall be interested in the case that \( M = k_n, F = k_0, \) and \( S \) will be the set of primes of \( k_0 \), which divide \( (p) \), and the Archimedean primes. In this situation only primes of \( S \) ramify in \( k_n \) so that \( [(I'_k)_n : I'_k] = 1 \). We note also in this case that for \( p \in S \), the decomposition group of \( p \) has bounded index in \( \text{Gal}(k_n/k_0) \) so that

\[ |(A'_n)^G| \sim |(C'_k)^0| \sim \frac{p^{nt(1)}}{[E'_0 : E'_0 \cap N(k^*_p)]}. \]

where \( t \) is the number of primes of \( k_0 \) dividing \( (p) \). Thus, in order to prove that \( |(A'_n)^G| \) is bounded we must show that

\[ [E'_0 : E'_0 \cap N(k^*_p)] \sim p^{nt(1)}. \]

As in [2], we reduce this computation to the case that \( p \) is totally split in \( k \). We can do this under the assumption that the decomposition group \( D = D(p) \) of \( p \) in \( \Delta \) is a subgroup of the kernel of \( \chi \).

**Proof of Theorem 2:** Let \( \bar{k} \) be the subfield of \( k \) fixed by \( D \), and let \( \bar{K} \) be the subfield of \( K = K_\chi \) fixed by a lifting of \( D \) to \( \text{Gal}(K_\chi/Q) \) (c.f. [4], where one sees that there is a unique lifting of \( \Delta \) to \( \text{Gal}(K_\chi/Q) \) containing \( J \)). Since \( D \subseteq \ker \chi \), we see that \( D \) is a subgroup of the center of \( \text{Gal}(K_\chi/Q) \) and hence \( \bar{K}_\chi/Q \) is normal, and \( \bar{K}/k \) is the \( \mathbb{Z}_p \)-extension corresponding to the character \( \bar{\chi} \) of \( \Delta/D \) induced by \( \chi \). Let \( \bar{k}_n \) be the \( n^{th} \) layer of the \( \mathbb{Z}_p \)-extension \( \bar{K}/k \), so \( \bar{k}_n \) is the subfield of \( k_n \) fixed by \( D \). Denote by \( \bar{p}_1, \ldots, \bar{p}_r \) the primes of \( \bar{k} \) dividing \( (p) \), such that \( \bar{p}_i \subseteq \bar{p}_i, i = 1, \ldots, t \). We may choose \( \alpha \in \bar{p}_1 \) so that \( \alpha \equiv 1 \pmod{\bar{p}_i}, i = 2, \ldots, t \) and \( \alpha \in E_{\bar{k}} \). (For example if \( \bar{p}_1^h = (\alpha_1) \) in \( \bar{k} \), we may choose \( x^1_i \).)
Let $B$ be the subgroup of $k^* \subseteq k^*$ generated by the conjugates of $\alpha$ under $\text{Gal}(\bar{k}/\mathbb{Q}) \cong \Delta/D$. Then $B$ has a free $\mathbb{Z}$-basis consisting of the conjugates of $\alpha$, and is isomorphic to $\mathbb{Z}[\Delta/D]$ as $\mathbb{Z}[\Delta/D]$-modules. By choice of $\alpha$, we have $B \subseteq E_k' \subseteq E_k$.

We show that

$$B/B \cap N_{k_n/k}(k_n^*) \sim B/B \cap N_{k_n/k}(\bar{k}_n^*)$$

and that the latter group has order $\sim p^{(t-1)n}$. From this we may conclude that the subgroup of $E_0'/E_0' \cap N(k_n^*)$ represented by elements of $B$ already has order $\sim p^{(t-1)n}$ so that $|A_n^\text{Gal}(k_n/k)|$ is bounded for all $n$.

To prove these statements, let $\beta \in B$ with $\beta = N_{k_n/k}(\gamma)$, then if $|D| = b$, $\beta^b = N_{k_n/k}(\gamma)$.

It follows that

$$\beta^b = N_{k_n/k}(N_{k_n/k}(\gamma)) \in N_{k_n/k}(\bar{k}_n^*).$$

Therefore

$$(B \cap N_{k_n/k}(k_n^*))^b \subseteq B \cap N_{k_n/k}(\bar{k}_n^*) \subseteq B \cap N_{k_n/k}(k_n^*)$$

Since $B$ is a finitely-generated group of rank $t$, we have

$$[B \cap N_{k_n/k}(k_n^*): B \cap N_{k_n/k}(\bar{k}_n^*)]$$

is bounded (by $t^b$) for all $n$ so that

$$B/B \cap N_{k_n/k}(k_n^*) \sim B/B \cap N_{k_n/k}(\bar{k}_n^*)$$

We may now assume that $k = \bar{k}$, and that $(p)$ is totally split in $k$. Also $B$ has as free basis $\{\sigma(\alpha) | \sigma \in \Delta\}$ and so $B \simeq \mathbb{Z}[\Delta]$ as a $\mathbb{Z}[\Delta]$-module. We prove that $[B:B \cap N_{k_n/k}(k_n^*)] \sim p^{(t-1)n}$ to conclude the theorem, by a method similar to that of section 1.

As in section 1, let $F_{n,i}$ be the completion of $k_n$ at a prime (of $k_n$) over $p_i$. Then $F_{n,i}/F_i$ is a cyclic extension of degree $\sim p^n$ for each $i = 1, \ldots, t$, and has ramification index also $\sim p^n$. Since $(p)$ is totally split in $k$, $F_i \simeq \mathbb{Q}_p$ for each $i$. Let $N_n(F_{n,i})$ be the subgroup of $F_i^*$ of norms from $F_{n,i}$ so that $\{N_n(F_{n,i})\}$ form a decreasing sequence of closed subgroups of finite index in $F_i^*$. Since the ramification index of $p_i$ in $k_n$, $\sim p^n$, we have

$$F_i^*/N_n(F_{n,i}^*) \sim U_i/N_n(U_{n,i}) \sim \mathbb{Z}/p^n\mathbb{Z}$$
It is clear that there is an integer $m_0 > 0$ independent of $n$ such that $N_n(F_{n,i}^*)$ contains an element of $p$-adic order $m_0$ for each $n$. Since sets of elements in $N_n(F_{n,i}^*)$ of order $m_0$ form a decreasing sequence of compact sets, it follows that there is an element $\pi_i \in \bigcap_{n \geq 0} N_n(F_{n,i}^*)$, ord$_p(\pi_i) = m_0 > 0$, and we may write $\pi_i = p^{m_0} \epsilon_i$ for some unit $\epsilon_i \in U_i$.

(Note that if $\chi = \chi_0$, $F_{n,i}/F_i$ is a cyclotomic extension of $\mathbb{Q}_p$ obtained by adjoining a $p^{n+1}$-st root of unity to $\mathbb{Q}_p$. In this case, $\pi_i = p$ and $\epsilon_i = 1$.)

By replacing $\alpha$ by $\alpha^{m_0}$ if necessary, we may assume that ord$_{p_1}(\alpha)$ is divisible by $m_0$, so we write ord$_{p_1}(\alpha) = m_0 c$, for some integer $c$.

Define a map $\phi : B \to U$ as follows

$$\phi(\alpha) = \begin{pmatrix} \alpha \\ \pi_1 \\ \ldots \\ \pi_{t-1} \end{pmatrix}$$

We may make $\phi$ into a $\Delta$-map by defining $\phi(\sigma(\alpha)) = \sigma(\phi(\alpha))$ for $\sigma \in \Delta$. Since $B$ is a free $\mathbb{Z}[\Delta]$-module this defines a $\mathbb{Z}[\Delta]$-homomorphism $\phi : B \to U$.

Let $\bar{B}$ be the closure of $\phi(B)$ in $U$, and let $Q_n$ be the closure of $\phi(B \cap N_{k_n/k}(k_n^*))$ in $U$, then

$$[B : B \cap N_{k_n/k}(k_n^*]) \geq [\phi(B) : \phi(B \cap N_{k_n/k}(k_n^*))] \geq [ar{B} : Q_n].$$

We show that asymptotically $[\bar{B} : Q_n] \geq p^{(t-1)n}$.

Firstly, $\beta \in B$ is a norm from $k_n^*$ if and only if $\beta$ is a local norm at all completions by primes of $k$. As in section 1, since $\beta$ is a unit at all primes not dividing $(p)$, and $k_n/k$ is ramified only at primes dividing $(p)$, $\beta$ is a norm from $k_n$ if and only if it is a local norm at the primes $p_1, \ldots, p_t$ of $k$.

Let $\beta = \prod_{\sigma \in \Delta} \sigma(\alpha)^{a_\sigma}$, $a_\sigma \in \mathbb{Z}$, then at the prime $p_i = \sigma(p_1)$, $\sigma \in \Delta$, $\beta$ is a local norm if and only if $\beta \sigma(\pi_1)^{-ca_\sigma}$ is a norm from $F_{n,i}^*$ (since $\pi_1$ is a norm from all $F_{n,i}$, $\sigma(\pi_1)$ is a norm from all $F_{n,i}$, where $\sigma(\pi_1) \in F_i$ is the image of $\pi_1 \in F_1$ under the natural map $\sigma : F_1 \to F_i$ induced by $\sigma \in \Delta$, $\sigma(p_1) = p_j$). However, as in section 1, since $F_{n,i}/F_i$ is “almost” totally ramified, we see that

$$[U_i : N_n(U_{n,i})] \sim p^n.$$
Since $\phi(\beta)$ has $\beta \sigma(\pi_i)^{-ca}$ in the $p_i$ co-ordinate, it follows that $[Q_n : B \cap U^{p^n}]$ is bounded for all $n$. However $[B : B^{p^n}] \sim [B : B \cap U^{p^n}]$ so we see that $[B : Q_n] \sim [B : B^{p^n}] \sim p^{sn}$ where $s$ is the $Z_p$-rank of $\bar{B}$. We show that $s \geq t - 1$ (and so $s = t - 1$).

Now $\bar{B} \subseteq U$ as a $Z_p[A]$-sub-module. Furthermore $U \sim Z_p[A]$, so that $e_\psi U \sim Z_p$ for each character $\psi \in \hat{A}$. Hence $e_\psi \bar{B}$ is either $\sim Z_p$ or $\sim 0$ for each character $\psi \in \hat{A}$. We prove that $e_\psi \bar{B} = 0$ for at most one character $\psi \in \hat{A}$ using the $p$-adic version of Baker's theorem on linear forms of logarithms.

Suppose that for distinct characters $\psi_1 \neq \psi_2 \in \hat{A}$, we had $e_{\psi_1} \bar{B} = e_{\psi_2} \bar{B} = 0$. Then we would have $\phi(x)^{d_\psi_1} = 1 = \phi(x)^{d_\psi_2}$ where $d = |\Delta|$.

Comparing co-ordinates at $p = p_1$ we have, in $F_1$ the equations

$$\frac{\alpha}{\pi_1} \prod_{\psi \neq 1} \tau(x)^{\psi_1(\tau^{-1})} = 1 = \frac{\alpha}{\pi_1} \prod_{\psi \neq 1} \tau(x)^{\psi_2(\tau^{-1})}$$

Taking $p_1$-adic logarithms we have

$$\sum_{\psi \neq 1} (\psi_1(\tau^{-1}) - \psi_2(\tau^{-1})) \log_{p_1} \tau(x) = 0$$

Since $p_1, \ldots, p_t$ are $Z$-independent in the group of ideals of $I$, it is clear that $\{\tau(x)\}_{x \in k^*}$ are $Z$-independent elements of $k^*$. If we had

$$\sum_{x \in d} a_x \log_{p_1} \tau(x) = 0, \quad a_x \in Z$$

Then $\prod_{x \in d} \tau(x)^{a_x}$ would be an element in $F_1$, in the kernel of $\log_{p_1}$, and so it would follow that

$$\prod_{x \in d} \tau(x)^{a_x} = p^a \zeta^b \quad \text{for some integers}$$

$a, b$, and a root of unity $\zeta$ in $F_1$. But taking ideals (in $k$) we would then have

$$a_\tau = a_1 \quad \text{for all } \tau \in \Delta.$$ 

Hence $\{\log_{p_1} \tau(x)\}_{x \neq 1}$ are linearly independent over $Z$ (resp. $Q$) and by Brumer's theorem [1], we see that they are linearly independent over the algebraic closure of $Q$ and this is a contradiction as $\psi_1 \neq \psi_2$. Hence $\bar{B} \sim Z_p^{-1}$ as a $Z_p$-module, and it follows that $[B : N(k^*_p) \cap B] \sim p^{(t-1)n}$
so that \([E'_0 : N(k_n^*) \cap E'_0] \sim p \pi^{(t-1)}\) and \(|(A'_n)^{\text{Gal}(k_n/k)}|\) is bounded. This establishes the theorem stated at the beginning of section 2.

**REMARK:**

1. If \(\chi = \chi_0\), then as noted \(\varepsilon = 1\) and \(\pi = p\). In this case \(\varepsilon_{\chi_0} B = 0\), and \(\varepsilon_{\psi} B \simeq \mathbb{Z}_p\) for all \(\psi \neq \chi_0\).

2. The proof shows that \(B \simeq \mathbb{Z}_p^s\) with \(s \geq t - 1\) but by the inequality from the genus theory, \(s \leq t - 1\) and so \(s = t - 1\).

3. Theorem 2 establishes the semi-simplicity of \(X_0\) in the case \(D(p) \subseteq \ker \chi\). This applies in cases (b), (d), (e) of Theorem 1. It can be shown using the methods of J.F. Jaulent \([5]\) that this may fail to be true in cases (a) and (c). (See \([5, 6]\)).

**REFERENCES**


(Oblatum 13-VIII-1980 & 22-II-1982)

J. Carroll
13474 Edgewater Drive
Lakewood, Ohio 44107
U.S.A.

&

H. Kisilevsky
Department of Mathematics
Concordia University
Sir George Williams Campus
1455 De Maisonneuve Blvd. West
Montreal
Quebec H3G 1M8
Canada