COMPOSITIO MATHEMATICA

J. CARROLL
H. KISILEVSKY

On the Iwasawa invariants of certain $\mathbb{Z}_p$-extensions

Compositio Mathematica, tome 49, nº 2 (1983), p. 217-229
<http://www.numdam.org/item?id=CM_1983__49_2_217_0>

Compositio Mathematica 49 (1983) 217–229

ON THE IWASAWA INVARIANTS OF CERTAIN $\mathbb{Z}_p$-EXTENSIONS

J. Carroll and H. Kisilevsky*

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

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

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

Let k be a totally complex abelian extension of $\mathbf{Q}$ with Galois group $\mathrm{Gal}(k/\mathbf{Q}) = \Delta$. Let p be an odd prime such that $\tau^{p-1} = 1$ for every element $\tau \in \Delta$, i.e. $p - 1$ is divisible by the exponent of the group Δ. Denote by $\hat{\Delta}$ the group of all homomorphisms of Δ into the group W of all $(p-1)^{\text{st}}$ roots of unity in $\mathbf{Z}_p$. 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 $\bar{\mathbf{Q}}$ into the complex field, $\mathbf{C}$.

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 $\mathbf{Z}_p$-extension K_χ/k, such that $K_\chi/\mathbf{Q}$ is normal. In fact $\mathrm{Gal}(K_\chi/\mathbf{Q})$ is isomorphic to a semi-direct product $\Delta \cdot \Gamma$, where $\Gamma = \mathrm{Gal}(K_\chi/k)$ and Δ is the fixed lifting of $\mathrm{Gal}(k/\mathbf{Q})$ to $\mathrm{Gal}(K_\chi/\mathbf{Q})$ which contains J, and such that $\tau\gamma\tau^{-1} = \gamma^{\chi(\tau)}$ for each $\tau \in \Delta$, $\gamma \in \Gamma$. Hence K_{χ_0}/k is the cyclotomic $\mathbf{Z}_p$-extension and for $\chi \neq \chi_0$, $K_\chi/\mathbf{Q}$ is a non-abelian extension. It is shown in [4] for the polynomial $g(T) = T^s p^u f(T)$ that $\deg(f(T))$ is congruent to 0 modulo the order of χ 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 Λ/T^a, and in section 2 we prove that $a = 1$ when the decomposition group $D(p)$ of p in Δ is contained in the kernel of χ.

We shall use the following conventions. If A, B are profinite p-groups then $\phi: A \to B$ is a pseudo-isomorphism if ϕ 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 $A = \varprojlim A_n$, $B = \varprojlim B_n$ 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_χ/k be the $\mathbf{Z}_p$-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 $X \simeq \varprojlim A_n$, the inverse limit being taken with respect to the norm maps $N_{m,n}$ between the layers k_m and k_n of K_χ.

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

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

where $A_0 = p$-primary part of the class group of k, $e_1, \ldots, e_t$ the ramification indices of the primes $\mathfrak{p}_1, \ldots, \mathfrak{p}_t$ 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 $\mathfrak{p}_1, \ldots, \mathfrak{p}_t$ of k dividing p eventually ramify in k_n, we see that

$$|A_n^{\mathrm{Gal}(k_n/k)}| \sim \frac{p^{(t-1)n}}{[E_0 : N(k_n^*) \cap E_n]}$$

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

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

Remark 2: If $k = \mathbf{Q}(\sqrt{D})$ 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 $|A_n^{\mathrm{Gal}(k_n/k)}| \sim p^{(t-1)n}$ 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_0^* which are stable under the action of Δ, we shall obtain the orders of these groups by studying the $\mathbf{Z}_p[\Delta]$-module structure of certain associated groups.

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

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

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

$$M = \sum_{\psi \in \hat{\Delta}} \varepsilon_\psi M$$

where $\varepsilon_\psi M = \{m \in M \mid \tau(m) = \psi(\tau)m, \text{ for all } \tau \in \Delta\}$.

Let $\mathfrak{p}_1, \ldots, \mathfrak{p}_t$ be the primes of k_0 which divide p, and let $F_1, \ldots, F_t$ be the completions of k at $\mathfrak{p}_1, \ldots, \mathfrak{p}_t$, respectively. Let $U_i \subseteq F_i$ be the group of units of F_i congruent to 1 modulo $\mathfrak{p}_i$, and let $U = U_1 \times \ldots \times U_t$. Then U is a compact topological group which is a $\mathbf{Z}_p[\Delta]$-module in a natural way, namely if $u = (u_1, \ldots, u_t) \in U$, and $\tau \in \Delta$, then $\tau(u)$ has $\tau(u_j)$ in the $\mathfrak{p}_i$ component if $\tau(\mathfrak{p}_j) = \mathfrak{p}_i$. Furthermore we may embed E_0 into U diagonally so that E_0 is a Δ-submodule of U. Let $\bar{E}_0$ be the closure of E_0 in the topological group U. Since Δ is abelian, Brumer's theorem [1] on the Leopoldt conjecture implies that $\bar{E}_0 \sim \mathbf{Z}_p^{\frac{d}{2}-1}$. One can show that U contains a subgroup of finite index which is isomorphic to $\mathbf{Z}_p[\Delta]$ as $\mathbf{Z}_p[\Delta]$-modules so that $\varepsilon_\psi U \sim \mathbf{Z}_p$ for every $\psi \in \hat{\Delta}$, (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 η, $\tau \in \Delta$, 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 $\mathbf{Z}_p[\Delta]$-module. Furthermore, since η is totally real, and $\prod_\tau \tau(\eta) = 1$, one sees that

$$\varepsilon_\psi \bar{E}_0 \sim \mathbf{Z}_p \ \text{ if } \ \psi(J) = +1, \psi = \chi_0$$
$$\varepsilon_\psi \bar{E}_0 \sim 1 \quad \text{if } \ \psi(J) = -1 \text{ or } \psi = \chi_0$$

Hence $\bar{E}_0 \sim \sum_\psi \varepsilon_\psi U$, the sum taken over $\psi \in \hat{\Delta}$, $\psi(J) = +1$ and $\psi \neq \chi_0$.

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

Lemma 1:

$$\bar{N}_n \sim \sum_{\psi_1} \varepsilon_{\psi_1} U + \sum_{\psi_2} p^n \varepsilon_{\psi_2} U$$

where the first sum runs over $\psi_1 \in \hat{\Delta}$ such that $\psi_1(J) = +1$, $\psi_1 \neq \chi_0$ and $\psi_1 | D \neq \chi | D$, and the second sum is taken over $\psi_2 \in \hat{\Delta}$, such that $\psi_2(J) = +1$, $\psi_2 \neq \chi_0$, 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 $\mathfrak{q} \neq \mathfrak{p}_1, \ldots, \mathfrak{p}_t$. 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 μ is a norm from k_n if and only if μ is a local norm at the completion of k_n/k at the primes $\mathfrak{p}_1, \ldots, \mathfrak{p}_t$. For each such prime $\mathfrak{p}_i$, let $F_{n,i} \supseteq F_i$ be a fixed completion of k_n at some prime of k_n dividing $\mathfrak{p}_i$. Let M_n be the subgroup of U which in the $\mathfrak{p}_i$ 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

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

By local class field theory $M_n \subseteq U$ is a closed and open subgroup of U, and $N(k_n^*) \cap E_0 \subseteq M_n$, so that $\bar{N}_n \subseteq M_n \cap \bar{E}_0$. On the other hand let $\alpha \in M_n \cap \bar{E}_0$, and let O_α be any neighborhood of α in U. Since $M_n \subseteq U$ is open, we may suppose $O_\alpha \subseteq M_n$. As $\alpha \in \bar{E}_0$, there is an $\varepsilon \in O_\alpha \cap E_0 \subseteq M_n \cap E_0$. But the norm theorem then implies that $\varepsilon \in N_n(k_n^*) \cap E_0$ and so α must be in $\bar{N}_n$. Since $\bar{E}_0 \sim \sum \varepsilon_\psi U$ the sum taken over $\psi \in \hat{\Delta}$, such that $\psi(J) = +1$, $\psi \neq \chi_0$, it suffices to compute M_n.

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

$$\tau\sigma\tau^{-1} = \sigma^{\chi(\tau)} \text{ for } \sigma \in \mathrm{Gal}(F_{n,i}/F_i),$$
$$\tau \in \mathrm{Gal}(F_i/\mathbf{Q}_p) = D(p)$$

Therefore by local class field theory, we see that

$$\begin{aligned}\mathrm{Gal}(F_{n,i}/F_i) &\simeq F_i^*/N_n(F_{n,i}^*) \text{ as } D(p)\text{-modules}\\ &\sim U_i/N_n(U_{n,i}) \text{ since } F_{n,i}/F_i \text{ is almost totally ramified.}\end{aligned}$$

Now, as before, we can write

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

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

$$N_n(U_{n,i}) \sim \sum_{\psi' \neq \chi'} \varepsilon_{\psi'} U_i + p^n \varepsilon_{\chi'} U_i$$

where χ' is the character of D given by $\chi' = \chi | D$. Hence

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

where the first sum is taken over characters ψ_1 of Δ such that $\psi_1 | D \neq \chi | D$ and the second sum is over characters ψ_2 of Δ such that $\psi_2 | D \neq \chi | D$. 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 $E_0/N(k_n^*) \cap E_0 \simeq \bar{E}_0/\bar{N}_n$. From the lemma, it follows that $|\bar{E}_0/\bar{N}_n| \sim p^{an}$ where a is the number of characters ψ_2 of Δ such that $\psi_2(J) = +1$, $\psi_2 \neq \chi_0$, and $\psi_2 | D = \chi | D$. Therefore, we see that $|A_n^{\mathrm{Gal}(k_n/k)}| \sim p^{(t-a-1)n}$ and so we have proved the following theorem:

THEOREM 1: *Let K_χ/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_χ. Then ${}_{\mathrm{T}}X \sim Z_p^r$ where r is given below:*

(a)	$\chi \neq \chi_0$,	$J \in D(p)$	*then* $r = t - 1$
(b)		$J \notin D(p), \chi | D = \chi_0 | D$	*then* $r = t/2$
(c)		$J \notin D(p), \chi | D \neq \chi_0 | D$	*then* $r = t/2 - 1$
(d)	$\chi = \chi_0$	$J \in D(p)$,	*then* $r = 0$
(e)		$J \notin D(p)$.	*then* $r = t/2$.

Section 2

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

THEOREM 2: *Let K_χ/k be the $\mathbf{Z}_p$-extension described above. If $D(p)$ (= the decomposition group of p in Δ) is contained in the kernel of χ then X_0 is a semi-simple Λ-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 $\mathrm{Gal}(L/L') \sim \Lambda/\xi_1 \times \ldots \times \Lambda/\xi_k$, where each ξ_i is a distinguished irreducible polynomial, and $\xi_i(T)$ divides $(T+1)^{n_0}-1$ for some integer n_0. It follows that $\mathrm{Gal}(L/L')$ has no submodule pseudo-isomorphic to Λ/T^2. Hence in order to prove the theorem, it is sufficient to prove that the divisor of $X' = \mathrm{Gal}(L'/K)$ is prime to (T), or equivalently that ${}_TX'$ 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 $\varprojlim A'_n \cong X'$, the inverse limit again taken with respect to the norm maps. It is therefore sufficient to prove that the orders

$$|A'^{\mathrm{Gal}(k_n/k_0)}|$$

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 $E'_F =$ the set of S-units F, i.e. $E'_F = \{\alpha \in F^* \mid (\alpha) \in I_S\}$ where (α) is the principal ideal generated by α. 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*

$$|C_M'^{\mathrm{Gal}(M/F)}| = \frac{|C'_F| \prod n_{\mathfrak{p}} \prod e_{\mathfrak{p}}}{d[E'_F : E'_F \cap N(M^*)]}$$

where $\prod n_{\mathfrak{p}}$ is the product of the local degrees of primes $\mathfrak{p} \in S$, $\prod e_{\mathfrak{p}}$ is the product of the ramification indices of those primes of F not in S.

Proof: Let $G = \mathrm{Gal}(M/F)$. 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

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

We then have

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

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

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

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

$$\sigma(\mathfrak{a})/\mathfrak{a} = \mathfrak{b}$$

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

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

But $[(I_M)^G : I_F]$ is the product of the ramification indices over all primes of F ramified in M, and $[I_F I^G_{M,S} : I_F]$ is equal to the product of the ramification indices over all primes of S (in F) ramified in M, hence $[(I'_M)^G : I'_F]$ 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

$$\begin{aligned} &0 \to (E'_M)^G \to F^* \to (P'_M)^G \to H^1(G, E'_M) \to 0 \to H^1(G, P'_M) \\ &\quad \to H^2(G, E'_M) \to H^2(G, M^*) \end{aligned}$$

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

$$\begin{aligned} H^1(G, P'_M) &\simeq \ker(E'_F/N(E'_M) \to F^*/N(M^*)) \\ &= E'_F \cap N(M^*)/N(E'_M) \end{aligned}$$

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

$$\frac{|H^0(G, E'_M)|}{|H^1(G, E'_M)|} \text{ is known to be equal to } \frac{1}{d}\prod_{\mathfrak{p}\in S} n_{\mathfrak{p}},$$

where $n_{\mathfrak{p}}$ = local degree of the prime $\mathfrak{p}$ for the extension M/F. Therefore

$$|(C'_M)^G| = \frac{|C'_F|}{d} \frac{\prod_{\mathfrak{p}\in S} n_{\mathfrak{p}} \prod_{\mathfrak{p}\notin S} e_{\mathfrak{p}}}{[E'_F : E'_F \cap N(M^*)]}.$$

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 $[(I'_{k_n})^G : I'_{k_0}] = 1$. We note also in this case that for $\mathfrak{p} \in S$, the decomposition group of $\mathfrak{p}$ has bounded index in $\mathrm{Gal}(k_n/k_0)$ so that

$$|(A'_n)^G| \sim |(C'_{k_n})^G| \sim \frac{p^{n(t-1)}}{[E'_0 : E'_0 \cap N(k_n^*)]}$$

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 $[E'_0 : E'_0 \cap N(k_n^*)] \sim p^{n(t-1)}$.

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 Δ is a subgroup of the kernel of χ.

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 $\mathrm{Gal}(K_\chi/\mathbf{Q})$ (c.f. [4], where one sees that there is a unique lifting of Δ to $\mathrm{Gal}(K_\chi/\mathbf{Q})$ containing J). Since $D \subseteq \ker\chi$, we see that D is a subgroup of the center of $\mathrm{Gal}(K_\chi/\mathbf{Q})$ and hence $\bar{K}_\chi/\mathbf{Q}$ is normal, and $\bar{K}/\bar{k}$ is the $\mathbf{Z}_p$-extension corresponding to the character $\bar{\chi}$ of Δ/D induced by χ. Let $\bar{k}_n$ be the n^{th} layer of the $\mathbf{Z}_p$-extension $\bar{K}/\bar{k}$, so $\bar{k}_n$ is the subfield of k_n fixed by D. Denote by $\bar{\mathfrak{p}}_1, \ldots, \bar{\mathfrak{p}}_t$ the primes of $\bar{k}$ dividing (p), such that $\bar{\mathfrak{p}}_i \subseteq \mathfrak{p}_i$, $i = 1, \ldots, t$. We may choose $\alpha \in \bar{\mathfrak{p}}_1$ so that $\alpha \equiv 1 \pmod{\mathfrak{p}_i}$, $i = 2, \ldots, t$ and $\alpha \in E'_{\bar{k}}$. (For example if $\bar{\mathfrak{p}}_1^h = (\alpha_1)$ in $\bar{k}$, we may choose α_1^{p-1}.)

Let B be the subgroup of $\bar{k}^* \subseteq k^*$ generated by the conjugates of α under $\mathrm{Gal}(\bar{k}/\mathbf{Q}) \cong \Delta/D$. Then B has a free $\mathbf{Z}$-basis consisting of the conjugates of α, and is isomorphic to $\mathbf{Z}[\Delta/D]$ as $\mathbf{Z}[\Delta/D]$-modules. By choice of α, we have $B \subseteq E'_{\bar{k}} \subseteq E'_k$.

We show that

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

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 $|(A'_n)^{\mathrm{Gal}(k_n/k)}|$ is bounded for all n.

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

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

Therefore

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

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

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

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

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

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 $B \simeq \mathbf{Z}[\Delta]$ as a $\mathbf{Z}[\Delta]$-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 $\mathfrak{p}_i$. Then $F_{n,i}/F_i$ is a cyclic extension of degree $\sim p^n$ for each $i = 1, \dots t$, and has ramification index also $\sim p^n$. Since (p) is totally split in k, $F_i \simeq \mathbf{Q}_p$ 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 $\mathfrak{p}_i$ in k_n, $\sim p^n$, we have

$$F_i^*/N_n(F_{n,i}^*) \sim U_i/N_n(U_{n,i}) \sim \mathbf{Z}/p^n\mathbf{Z}$$

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 $\pi_i \in \bigcap_{n \geq 0} N_n(F^*_{n,i})$, $\text{ord}_p(\pi_i) = m_0 > 0$, and we may write $\pi_i = p^{m_0}\varepsilon_i$ for some unit $\varepsilon_i \in U_i$.

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

By replacing α by α^{m_0} if necessary, we may assume that $\text{ord}_{\mathfrak{p}_1}(\alpha)$ is divisible by m_0, so we write $\text{ord}_{\mathfrak{p}_1}(\alpha) = m_0 c$, for some integer c.

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

$$\phi(\alpha) = \left(\frac{\alpha}{\pi_1^c}, \alpha \ldots, \alpha\right)$$

We may make ϕ into a Δ-map be defining $\phi(\sigma(\alpha)) = \sigma(\phi(\alpha))$ for $\sigma \in \Delta$. Since B is a free $\mathbf{Z}[\Delta]$-module this defines a $\mathbf{Z}[\Delta]$-homomorphism

$$\phi : B \to \phi(B) \subseteq U$$

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

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

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 β is a local norm at all completions by primes of k. As in section 1, since β is a unit at all primes not dividing (p), and k_n/k is ramified only at primes dividing (p), β is a norm from k_n if and only if it is a local norm at the primes $\mathfrak{p}_1, \ldots \mathfrak{p}_t$ of k.

Let $\beta = \prod_{\tau \in \Delta} \tau(\alpha)^{a_\tau}$, $a_\tau \in Z$, then at the prime $\mathfrak{p}_i = \sigma(\mathfrak{p}_1)$, $\sigma \in \Delta$, β is a local norm if and only if $\beta\sigma(\pi_1)^{-ca_\sigma}$ is a norm from $F^*_{n,i}$ (since π_1 is a norm from all $F_{n,1}$, $\sigma(\pi_1)$ 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 $\sigma \in \Delta$, $\sigma(\mathfrak{p}_1) = \mathfrak{p}_i$). However, as in section 1, since $F_{n,i}/F_i$ is "almost" totally ramified, we see that

$$[U_i : N_n(U_{n,i})] \sim p^n.$$

Also, as $F_i \simeq \mathbf{Q}_p$, we see that $U_i \simeq \mathbf{Z}_p$ so that $[N_n(U_{n,i}) : U_i^{p^n}]$ is bounded for all n. Thus we see that β is a local norm at $\mathfrak{p}_i$ from k_n if and only if $\beta^{b_0}\sigma(\pi_1)^{-ca_\sigma b_0} \in U^{p^n}$ for some power b_0 independent of n.

Since $\phi(\beta)$ has $\beta\sigma(\pi_1)^{-ca_\sigma}$ in the $\mathfrak{p}_i$ co-ordinate, it follows that $[Q_n:\bar{B}\cap U^{p^n}]$ is bounded for all n. However $[\bar{B}:\bar{B}^{p^n}] \sim [\bar{B}:\bar{B}\cap U^{p^n}]$ so we see that $[\bar{B}:Q_n] \sim [\bar{B}:\bar{B}^{p^n}] \sim p^{sn}$ where s is the $\mathbf{Z}_p$-rank of $\bar{B}$. We show that $s \geq t-1$ (and so $s = t-1$).

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

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

Comparing co-ordinates at $\mathfrak{p} = \mathfrak{p}_1$ we have, in F_1 the equations

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

Taking $\mathfrak{p}_1$-adic logarithms we have

$$\sum_{\tau \neq 1} (\psi_1(\tau^{-1}) - \psi_2(\tau^{-1})) \log_{\mathfrak{p}_1} \tau(\alpha) = 0$$

Since $\mathfrak{p}_1, \ldots, \mathfrak{p}_t$ are $\mathbf{Z}$-independent in the group of ideals of I, it is clear that $\{\tau(\alpha)\}_{\tau \in \Delta}$ are $\mathbf{Z}$-independent elements of k^*. If we had

$$\sum_{\tau \in \Delta} a_\tau \log_{\mathfrak{p}_1} \tau(\alpha) = 0, \qquad a_\tau \in \mathbf{Z}$$

Then $\prod_{\tau \in \Delta} \tau(\alpha)^{a_\tau}$ would be an element in F_1, in the kernel of $\log_{\mathfrak{p}_1}$, and so it would follow that

$$\prod_{\tau \in \Delta} \tau(\alpha)^{a_\tau} = p^a \cdot \zeta^b \qquad \text{for some integers}$$

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

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

Hence $\{\log_{\mathfrak{p}_1} \tau(\alpha)\}_{\tau \neq 1}$ are linearly independent over $\mathbf{Z}$(resp. $\mathbf{Q}$) and by Brumer's theorem [1], we see that they are linearly independent over the algebraic closure of $\mathbf{Q}$ and this is a contradiction as $\psi_1 \neq \psi_2$. Hence $\bar{B} \sim \mathbf{Z}_p^{t-1}$ as a $\mathbf{Z}_p$-module, and it follows that $[B:N(k_n^*) \cap B] \sim p^{(t-1)n}$

so that $[E'_0 : N(k_n^*) \cap E'_0] \sim p^{n(t-1)}$ and $|(A'_n)^{\mathrm{Gal}(k_n/k)}|$ 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 $\varepsilon_{\chi_0}\bar{B} = 0$, and $\varepsilon_\psi \bar{B} \simeq \mathbf{Z}_p$ for all $\psi \neq \chi_0$.

2. The proof shows that $\bar{B} \sim \mathbf{Z}_p^s$ 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

[1] A. BRUMMER: On the Units of Algebraic Number Fields. *Mathematika 14* (1967) 121–124.
[2] R. GREENBERG: On a certain p-adic representation. *Inventiones Math. 21* (1973) 117–124.
[3] K. IWASAWA: On $\mathbf{Z}_p$-extensions of Algebraic Number Fields. *Annals of Math., ser (2)* 1973 (98) 187–326.
[4] J. CARROLL and H. KISILEVSKY: On Iwasawa's λ Invariant for Certain $\mathbf{Z}_p$-extensions. *Acta Arithmetica*, XL (1981) 1–8.
[5] J.F. JAULENT: Sur la théorie des genres dans une extension procyclique métabelienne sur un sous corps. To appear.
[6] H. KISILEVSKY: Some Non-Semi-Simple Iwasawa Modules. To appear in *Comp. Math. 49* (1983) vol. 3.

(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