Conspectus materiae tomi XL, fasciculi 1

La revue est consacrée à la Théorie des Nombres
The journal publishes papers on the Theory of Numbers
Die Zeitschrift veröffentlicht Arbeiten aus der Zahlentheorie
Журнал посвящен теории чисел

L'adresse de la Rédaction et de l'échange | Address of the Editorial Board and of the exchange | Die Adresse der Schriftleitung und des Austausches | Адрес редакции и книгообмена

ACTA ARITHMETICA
ul. Śniadeckich 8, 00-950 Warszawa

Les auteurs sont priés d'envoyer leurs manuscrits en deux exemplaires
The authors are requested to submit papers in two copies
Die Autoren sind gebeten um Zusendung von 2 Exemplaren jeder Arbeit
Рукописи статей редакция просит предлагать в двух экземплярах

ISBN 83-01-01784-8 ISSN 0065-1036

PRINTED IN POLAND

WROCŁAWSKA DRUKARNIA NAUKOWA

On Iwasawa's λ-invariant for certain Z_l-extensions

by

JOSEPH E. CARROLL and H. H. KISILEVSKY (Pasadena, Calif.)

In this article we consider Z_l-extensions of certain abelian extensions of Q, the field of rational numbers. For the basic theory of Z_l-extensions we refer to Iwasawa [3].

Let k be a finite extension of Q, l a prime, and let K/k be a Z_l-extension, i.e. K/k is a Galois extension and $\mathrm{Gal}(K/k) = \Gamma$ is topologically isomorphic to the additive group of Z_l, the ring of l-adic integers. Let L be the maximal abelian unramified l-extension of K, and let $X = \mathrm{Gal}(L/K)$. Then X has the structure of a $Z_l[\Gamma]$-module in a natural way. If we fix a topological generator, σ, of Γ, X can be endowed with the structure of a $\Lambda = Z_l[[T]]$ module under the correspondence $\sigma \leftrightarrow 1+T$. It is known that X contains as a submodule of finite index an elementary module $E \approx \bigoplus_{i=1}^{r} \Lambda/(f_i)^{n_i}$ where $f_i = l$ or is a distinguished irreducible polynomial in $Z_l[T]$. (This follows from the existence of a pseudo-isomorphism $E \to X$, and the fact that E has no finite Λ-submodules.) Let $H_K(T) = \prod f_i^{n_i}$. Then the degree of H_K is λ_K, the Iwasawa λ-invariant for K/k.

Now suppose that l is odd and that k/Q is a totally complex abelian extension with $\mathrm{Gal}(k/Q) = \Delta$. We assume that every element of Δ has order dividing $l-1$. By using the action of Δ on $\mathrm{Gal}(F/k)$, where F is the composite of all Z_l-extensions of k, we single out a certain set of Z_l-extensions of k. We then obtain congruence conditions on corresponding λ's, and a functional equation for the corresponding H's.

1. Let l be an odd prime, and let k/Q be a totally complex abelian extension with $\mathrm{Gal}(k/Q) = \Delta$. Assume that the group Δ has exponent dividing $l-1$. Let W be the group of $(l-1)$st roots of unity in Z_l, and let $\hat{\Delta} = \mathrm{Hom}(\Delta, W)$. For each $\chi \in \hat{\Delta}$, let

$$\varepsilon_\chi = \frac{1}{|\Delta|} \sum_{\tau \in \Delta} \chi(\tau)^{-1}\tau \in Z_l[\Delta].$$

Then the ε_χ are a set of orthogonal idempotents with $\sum_\chi \varepsilon_\chi = 1$, and any topological $Z_l[\Delta]$-module M can be decomposed:

$$M = \bigoplus_{\chi\in\hat{\Delta}} \varepsilon_\chi M,$$

where

$$\tau(m) = \chi(\tau)\cdot m \quad \text{for all } m\in\varepsilon_\chi M \text{ and all } \tau\in\Delta.$$

Let F be the composite of all Z_l-extension of k, and denote by G the group $\mathrm{Gal}(F/k)$. Since Leopoldt's conjecture is valid for k, [1], it follows that $G \approx Z_l^{d/2+1}$, where $[k:Q] = d$. Furthermore, F/Q is a Galois extension, and $\mathrm{Gal}(F/Q) \approx G\cdot\Delta$, the semi-direct product, where Δ acts on G by group theoretic conjugation. We shall identify Δ with a lifting to $\mathrm{Gal}(F/Q)$ for which J = complex conjugation is an element of Δ under a fixed embedding of F into the field of complex numbers. We first determine the decomposition of G as a $Z_l[\Delta]$-module.

Let $G^- = \bigoplus_{\chi(J)=-1} \varepsilon_\chi G$ and let F^+ be the fixed field of G^-. If k^+ is the maximal real subfield of k, then F^+/k^+ is Galois with group $G/G^- \times\langle J\rangle$. Thus if F_0^+ is the subfield of F^+ fixed by J, $\mathrm{Gal}(F_0^+/k^+) \approx G/G^-$. Since Leopoldt's conjecture is true for k_0^+, F_0^+ is the cyclotomic Z_l-extension of k^+, implying that $\varepsilon_{\chi_0}G \approx Z_l$ and $\varepsilon_\chi G = 0$ for all other $\chi\in\hat{\Delta}$ such that $\chi(J) = 1$, where χ_0 is the principal character of Δ.

It shall be shown that each group $\varepsilon_\chi G$ has Z_l-rank at most one. Assuming this, it follows from the fact that $G\approx Z_l^{d/2+1}$ that $\varepsilon_\chi G\approx Z_l$ for all χ such that $\chi(J) = -1$ or $\chi = \chi_0$, and that $\varepsilon_\chi G = 0$ otherwise.

Suppose that $\mathfrak{p}_1, \ldots, \mathfrak{p}_m$ are the primes of k lying above the rational prime l. Let $k_{\mathfrak{p}_i}$ denote the completion of k at $\mathfrak{p}_i$, $\mathcal{O}_{\mathfrak{p}_i}$ the integers of $k_{\mathfrak{p}_i}$, and $U_{\mathfrak{p}_i}^{(t)}$ the units of $\mathcal{O}_{\mathfrak{p}_i}$ congruent to 1 modulo $\mathfrak{p}_i^t$, for t a non-negative integer. Choose t large enough, so that the $\mathfrak{p}_i$-adic exponential function maps $\mathfrak{p}_i^t\mathcal{O}_{\mathfrak{p}_i}$ isomorphically onto $U_{\mathfrak{p}_i}^{(t)}$. Let $Z\subset\Delta$ be the decomposition group of the prime l, so Z is naturally isomorphic with the groups $\mathrm{Gal}(k_{\mathfrak{p}_i}/Q_l)$. Choose coset representatives $\tau_1 = 1, \tau_2, \ldots, \tau_m$ of Δ/Z so that $\tau_i(\mathfrak{p}_1) = \mathfrak{p}_i$. Since the group Z has exponent dividing $l-1$, and the $(l-1)$st roots of unity are in Q_l, it follows that $k_{\mathfrak{p}_1}/Q_l$ is a Kummer extension. Furthermore if we denote by A_1 the multiplicative group of non-zero elements of $k_{\mathfrak{p}_1}$ whose $(l-1)$st powers are in Q_l, we have a perfect pairing $A_1\times\mathrm{Gal}(k_{\mathfrak{p}_1}/Q_l)\to W$ given by $(\alpha,\gamma)\mapsto\gamma(\alpha)\alpha^{-1}$. Hence $A_1/Q_l^\times$ is naturally isomorphic to the character group of $\mathrm{Gal}(k_{\mathfrak{p}_1}/Q_l)$.

Let $\chi\in\hat{\Delta}$, and define $\chi_Z = \chi|_Z$, the character of Z obtained by restricting the domain of χ to Z. Under the identification of Z with $\mathrm{Gal}(k_{\mathfrak{p}_1}/Q_l)$, we can view $\chi_Z\in\widehat{\mathrm{Gal}(k_{\mathfrak{p}_1}/Q_l)}$, so that there exists an element $a_1\in A_1$ such that $\chi_Z(\gamma) = \gamma(a_1)a_1^{-1}$ for every $\gamma\in Z$. Consider the product $P = \mathfrak{p}_1^t\mathcal{O}_{\mathfrak{p}_1}\times\ldots$

$\ldots\times\mathfrak{p}_m^t\mathcal{O}_{\mathfrak{p}_m}$ which is naturally a $Z_l[\Delta]$-module. Define $\beta\in P$ by

$$\beta = (a_1, \ldots, \chi(\tau_i)^{-1}\tau_i(a_1), \ldots).$$

Let $\varphi\in\Delta$ and we determine the $\mathfrak{p}_i$-coordinate of $\varphi(\beta)$ in P. There exists $\gamma\in Z$ so that $\varphi\tau_j = \tau_i\gamma$ for some index j.

Then

$$\begin{aligned}\varphi\big(\chi(\tau_j^{-1})\tau_j(a_1)\big) &= \chi(\tau_j^{-1})\varphi\tau_j(a_1) = \chi(\tau_j^{-1})\tau_i\gamma(a_1)\\ &= \chi(\tau_j^{-1})\tau_i\big(\chi(\gamma)a_1\big) = \chi(\tau_j^{-1}\gamma)\tau_i(a_1) = \chi(\varphi)\chi(\tau_i^{-1})\tau_i(a_1).\end{aligned}$$

Hence $\varphi(\beta) = \chi(\varphi)\beta$ in P, and so $\varepsilon_\chi P$ is non-trivial. Applying the exponential map in each component and noting that exp is a $Z_l[\Delta]$-map, we see that for any $\chi\in\Delta$, $\varepsilon_\chi(U^{(t)})$ is non-trivial, where $U^{(t)} = U_{\mathfrak{p}_1}^{(t)}\times\ldots\times U_{\mathfrak{p}_m}^{(t)}$. Since $U^{(t)}$ is a $Z_l[\Delta]$-module of Z_l-rank d, each eigenspace must have rank exactly one. Now by class field theory ([4], ch. 7, §11.5) G contains as a $Z_l[\Delta]$ submodule of finite index an isomorphic copy of $(U^{(t)}/\bar{E}\cap U^{(t)})/(\text{torsion})$ ([3], § 2), where $\bar{E}$ is the closure of the units, E, of k embedded diagonally in $U^{(0)}$. It follows that all the eigenspaces for G have Z_l-rank at most one.

For any $\chi\in\hat{\Delta}$, such that $\chi(J) = -1$ or $\chi = \chi_0$, let K_χ be the subfield of F fixed by $\bigoplus_{\chi'\neq\chi}\varepsilon_{\chi'}G$.

Thus we have proved:

THEOREM 1. *For any $\chi\in\hat{\Delta}$, $\chi(J) = -1$ or $\chi = \chi_0$, K_χ/k is a Z_l-extension. The set of such K_χ is an independent set of Z_l-extensions of k whose composite is F. Furthermore, K_χ/Q is Galois with group the semi-direct product $\mathrm{Gal}(K_\chi/k)\cdot\Delta$, where $\tau(\sigma) = \tau\sigma\tau^{-1} = \sigma^{\chi(\tau)}$ for every $\sigma\in\mathrm{Gal}(K_\chi/k)$, and $\tau\in\Delta$.*

COROLLARY 1. *If K/k is a Z_l-extension with K/Q Galois, then $K = K_\chi$ for some $\chi\in\Delta$.*

Proof. If M is any $Z_l[\Delta]$-submodule of G then $M = \bigoplus_{\chi\in\hat{\Delta}}\varepsilon_\chi M$ where $\varepsilon_\chi M = 0$ or $\varepsilon_\chi M = l^{a_\chi}\varepsilon_\chi G$ for some non-negative integer a_χ. As K/Q is Galois, $\mathrm{Gal}(K/k)$ is a $Z_l[\Delta]$-submodule of G. Since $\mathrm{Gal}(K/k)\approx Z_l$ it follows that $\mathrm{Gal}(F/K) = \bigoplus_{\chi'\neq\chi}\varepsilon_{\chi'}G$ for some $\chi\in\hat{\Delta}$. Hence $K = K_\chi$. It is easy to see that every sub-extension of F/k which is Galois over Q, is a composite of layers from the extensions K_χ.

2. We next consider the splitting of primes in the various fields K_χ.

THEOREM 2. *Let $p\neq l$ be a rational prime. Let $Z(p)$ be the decomposition group of p in Δ, and $\mathfrak{p}$ be a prime of k dividing p. If $Z(p)$ is not contained in $\ker\chi$, then $\mathfrak{p}$ splits completely in K_χ.*

Proof. Let $Z(\mathfrak{p})$ be the decomposition group of $\mathfrak{p}$ in G. Since $\mathfrak{p}$ does not split completely in K_{χ_0} (cf. [2]), it follows that $Z(\mathfrak{p})$ is non-trivial.

Since $p \neq l$, $\mathfrak{p}$ does not ramify in F, and hence $Z(\mathfrak{p}) \approx \mathbf{Z}_l$. Thus $Z(\mathfrak{p})$ is generated as a $\mathbf{Z}_l$-module by some

$$a = (a_{\chi_0}, \ldots, a_\chi, \ldots) \in \bigoplus_{\chi \in \hat{\Delta}} \varepsilon_\chi G, \quad \text{with } a_{\chi_0} \neq 0.$$

For $\tau \in Z(p) \subset \Delta$, $\tau\mathfrak{p} = \mathfrak{p}$, so that $\tau\big(Z(\mathfrak{p})\big) = Z(\mathfrak{p})$, and hence there is a unit $u \in \mathbf{Z}_l$, such that $\tau(a) = u \cdot a$. But $\tau(a) = \big(\ldots \chi(\tau) a_\chi \ldots\big)$ so we must have $u = 1$ comparing χ_0 components, and $\chi(\tau) = 1$ for each component with $a_\chi \neq 0$. But $a_\chi = 0$ if and only if $\mathfrak{p}$ splits completely in K_χ, and the theorem is proved.

Corollary 2. *For every $\chi \in \Delta$, $\chi(J) = -1$, infinitely many primes of k split completely in K_χ.*

3. In this section we consider the Iwasawa invariant $\lambda_\chi = \lambda_{K_\chi}$ of the extensions K_χ. We also derive a functional equation for $H_\chi = H_{K_\chi}$, when $\chi \neq \chi_0$.

Fix $\chi \in \hat{\Delta}$, $\chi(J) = -1$ or $\chi = \chi_0$ and let L be the maximal abelian unramified l-extension of K_χ. Let $X = \mathrm{Gal}(L/K_\chi)$. If $\Gamma = \mathrm{Gal}(K_\chi/k)$, then as noted in the introduction, X is a $\mathbf{Z}_l[\Gamma]$-module and so becomes a $\Lambda = \mathbf{Z}_l[[T]]$-module under the correspondence $\sigma \leftrightarrow 1+T$ where σ is a fixed topological generator of Γ. But also, as $K_\chi/\mathbf{Q}$ is Galois, so is $L/\mathbf{Q}$. Hence Δ acts on both Λ (via its action on Γ) and on X. Since these actions are induced by group theoretic conjugation, we have for $r \in \Lambda$, $x \in X$ and $\tau \in \Delta$, the equation

$$\tau(rx) = \tau(r) \cdot \tau(x).$$

Also since $\tau(\sigma) = \sigma^{\chi(t)}$, we see that $\tau(1+T) = (1+T)^{\chi(\tau)} \in \Lambda$, so for any $r \in \Lambda$ and $\tau \in \Delta$ we have $\tau\big(r(T)\big) = r\big((1+T)^{\chi(\tau)}-1\big)$.

Lemma 1. *Let $M \subset X$ be a Λ-submodule. Then $\tau(M)$ is a Λ-submodule of X for every $\tau \in \Delta$. Furthermore* $\mathrm{Ann}\big(\tau(M)\big) = \tau\big(\mathrm{Ann}(M)\big)$ *where* Ann *denotes the annihilator in Λ.*

Proof. Let $m \in M$, $r \in \Lambda$ and $\tau \in \Delta$. Then

$$r\tau(m) = \tau\tau^{-1}\big(r\tau(m)\big) = \tau\big(\tau^{-1}(r) \cdot m\big) \in \tau(M).$$

Secondly,

$$\begin{aligned} r \in \mathrm{Ann}\big(\tau(M)\big) &\Leftrightarrow r\tau(M) = 0 \\ &\Leftrightarrow \tau^{-1}\big(r\tau(M)\big) = 0 \\ &\Leftrightarrow \tau^{-1}(r) \cdot M = 0 \\ &\Leftrightarrow \tau^{-1}(r) \in \mathrm{Ann}(M) \\ &\Leftrightarrow r \in \tau\big(\mathrm{Ann}(M)\big). \end{aligned}$$

As mentioned in the introduction, X contains as a Λ-submodule of finite index an elementary module, E. E is a sum of cyclic modules, $E = \bigoplus_{i=1}^{r} \Lambda x_i$, where $\mathrm{Ann}(x_i) = (f_i^{n_i})$, the principal ideal of Λ generated by $f_i^{n_i}$. Here f_i is either l, or a distinguished irreducible polynomial. Now if f is any distinguished irreducible polynomial and $\tau \in \Delta$, we see by the Weierstrass preparation theorem, and the fact that τ is an automorphism of Λ that $\tau\big(f(T)\big) = u(T)g(T)$ uniquely, where $u(T)$ is a unit of Λ and $g(T)$ is a distinguished irreducible polynomial.

Lemma 2. *Let E be an elementary module of finite index in X, and let $\tau \in \Delta$. Suppose that*

$$E = \bigoplus_{i=1}^{u} \Lambda x_i \bigoplus_{j=1}^{t} \Lambda y_j,$$

where $\mathrm{Ann}(x_i) = (l^{\mu_i})$ and $\mathrm{Ann}(y_j) = (f_j^{n_j})$, f_j a distinguished irreducible polynomial. For each j, let $\tau(f_j) = u_j g_j$ as above. Then the set of $f_j^{n_j}$ is the same as the set $g_j^{n_j}$ counting multiplicities.

Proof. $\tau(E) = \bigoplus_{i=1}^{u} \Lambda\tau(x_i) \oplus \bigoplus_{j=1}^{t} \Lambda\tau(y_j)$ where $\mathrm{Ann}\big(\tau(x_i)\big) = (l^{\mu_i})$ and $\mathrm{Ann}\big(\tau(y_j)\big) = (g_j^{n_j})$ by Lemma 1. As $\tau(X) = X$, $\tau(E)$ is an elementary submodule of finite index in X. But this means that $\tau(E) \approx E$ as Λ-modules, and hence that the annihilators of the y_j's are the same as those of the $\tau(y_j)$'s after rearrangement.

Let χ have order a in $\hat{\Delta}$, and choose $\tau_\chi \in \Delta$ so that $\chi(\tau_\chi) = \eta$, where η is a primitive ath root of unity in W. We note that if $\tau \in \ker\chi$, then $\tau(T) = T$ and $\tau(r) = r$ for any $r \in \Lambda$.

Lemma 3. *Let $f \neq T$ be a distinguished irreducible polynomial in Λ. Suppose that $(\tau_\chi^m f) = (f)$. Then the order of η^m in W divides the degree of f.*

Proof. Let $u(T)f(T) = \tau_\chi^m f(T) = f\big((1+T)^{\eta^m}-1\big)$ where $u(T)$ is a unit of Λ. Let $\alpha-1$ be a zero of $f(T)$ in some extension field k' of $\mathbf{Q}_l$. Then $\alpha-1$ has positive valuation in k' since f is distinguished, so we can substitute $T = \alpha-1$ in the above equation to deduce that $\alpha^{\eta^m}-1$ is also a root of $f(T)$. Iterating we see that $\alpha^{\eta^{im}}-1$ is a root of $f(T)$ for $i = 0, 1, \ldots, O(\eta^m)-1$, where $O(\eta^m)$ is the order of η^m in W. Now suppose we had $\alpha^{\eta^{im}}-1 = \alpha^{\eta^{jm}}-1$ for some $0 \leqslant i < j < O(\eta^m)$. Then $\alpha^{\eta^{im}(\eta^{(j-i)m}-1)} = 1$, and taking $\mathscr{L}$-adic logarithms ($\mathscr{L}$ is the maximal ideal of k') we get $\eta^{im}(\eta^{(j-i)m}-1)\log\alpha = 0$. Since $0 < j-i < O(\eta^m)$, $\log\alpha = 0$, so α is an l-power root of 1, and hence, $\alpha-1$ is a root of $\omega_k = (1+T)^{l^k}-1$ for some k. Thus if $f(T)$ is prime to ω_k for all k, there are no such i and j. This implies that the roots of $f(T)$ are partitioned into disjoint orbits each with $O(\eta^m)$ elements. Hence $O(\eta^m)$ divides the degree of f. If $f(T) | \omega_k$ for some k, then either $f(T) = T$ or $f(T) = \xi_i = \omega_i/\omega_{i-1}$ for some positive integer i. As $l-1$

divides the degree of ξ_i we again have that $O(\eta^m)$ divides the degree of f if $f(T) \neq T$. We note that it can be verified that $(\tau(\xi_i)) = (\xi_i)$.

THEOREM 3. *Let $H_\chi(T) = H_{K_\chi}(T)$ be as defined in the introduction, and write $H_\chi(T) = T^s l^\mu g(T)$ where $g(0) \neq 0$. Then the order of χ in $\hat{\Delta}$ divides the degree of g, so that $\lambda_\chi \equiv s \pmod{a}$.*

Proof. Let $g'(T)$ be any distinguished polynomial of Λ, such that $(\tau_\chi(g'(T))) = (g'(T))$, and $g'(0) \neq 0$. Let $f(T)$ be a distinguished irreducible factor of $g'(T)$ and suppose $m > 0$ is the least integer such that $(\tau_\chi^m f(T)) = (f(T))$. By Lemma 3, $O(\eta^m)$ divides the degree of f. Since $(\tau_\chi(g')) = (g')$, we must have all the ideals (f), $(\tau_\chi f)$, ..., $(\tau_\chi^{m-1} f)$ appearing in the factorization of (g') to the same power. As τ_χ is an automorphism of Λ, the distinguished irreducible polynomials generating these ideals all have degree equal to degree of f. Hence $a = O(\eta) = mO(\eta^m)$ divides the degree of $g'(T)$. Noting that $(\tau_\chi(T)) = ((1+T)^\eta - 1) = (T)$ and that by Lemma 2, $(\tau_\chi(H_\chi(T))) = (H_\chi(T))$ we apply this argument to $g' = g(T)$ to finish the proof.

Remark. If $\chi \neq \chi_0$ this places some severe restrictions on the set of f_j's.

THEOREM 4. *Let $\chi \in \hat{\Delta}$, $\chi(J) = -1$. Then $H_\chi(T)$ satisfies the functional equation*

$$(-1-T)^{\deg H_\chi} \cdot H_\chi\left(\frac{-T}{1+T}\right) = H_\chi(T).$$

Also

$$H_\chi(-1) = (-1)^{\lambda_\chi} \cdot l^\mu.$$

Proof. It is clear that $(J(H(T))) = (H(T))$, and since $\chi(J) = -1$ $J(T) = -T/(1+T)$. Hence there is a unit $u(T)$ in Λ such that

$$l^\mu \left(\frac{-T}{1+T}\right)^s g\left(\frac{-T}{1+T}\right) u(T) = H_\chi\left(\frac{-T}{1+T}\right) u(T) = H_\chi(T) = l^\mu T^s g(T).$$

Clearing denominators, we obtain

$$(-1)^s (1+T)^{2m} g\left(\frac{-T}{1+T}\right) u'(T) = g(T),$$

where $u'(T) = \dfrac{u(T)}{(1+T)^{\deg H_\chi}}$ and $2m$ = degree of g (which is even by Theorem 3).

Let $g(T) = a_0 + \ldots + a_{2m-1} T^{2m-1} + T^{2m}$. Then $(1+T)^{2m} g\left(\frac{-T}{1+T}\right) = a_0(1+T)^{2m} + \ldots + a_{2m-1}(1+T)(-T)^{2m-1} + T^{2m}$, a polynomial of degree at

most $2m$. But as $g(T)$ is distinguished, $(1+T)^{2m} g\left(\frac{-T}{1+T}\right) \equiv T^{2m} \pmod{l}$ so there is a unit $v \in Z_l$, such that $v(1+T)^{2m} g\left(\frac{-T}{1+T}\right)$ is a (monic) distinguished polynomial. Thus by the Weierstrass Preparation Theorem, we see that $v(1+T)^{2m} g\left(\frac{-T}{1+T}\right) = g(T)$. Substituting $T = 0$, and noting that $g(0) \neq 0$, we see that $v = 1$.

The second statement now follows by evaluating the expression above for $(1+T)^{2m} g\left(\frac{-T}{1+T}\right)$ at $T = -1$.

We note that the proof is valid for any distinguished polynomial h satisfying $(J(h(T))) = (h(T))$.

4. We now discuss a sufficient condition for a Z_l-extension, so that T does not divide $H_K(T)$. As a consequence we derive divisibility properties for the λ_χ's when $k = Q(\zeta)$, ζ a primitive lth root of 1.

Let K be a Z_l-extension of a finite extension, k, of Q. Let k_n be the nth layer of K, $n = 1, 2, \ldots$ Let $G_n = \mathrm{Gal}(k_n/k)$, and let A_n be the l-primary part of the ideal class group of k_n.

LEMMA 4. *Let K/k, k_n, G_n, A_n be as above, and suppose there is a unique prime $\mathfrak{p}$ of k which ramifies in K. Then $(A_n)^{G_n}$ has bounded order as $n \to \infty$, where $(A_n)^{G_n}$ is the subgroup of elements of A_n fixed by G_n.*

Proof. Let σ generate G_n. Then $|(A_n)^{G_n}| = |(A_n)^{\langle\sigma\rangle}| = |A_n/(\sigma-1)A_n|$. It is well known from genus theory that $|A_n/(\sigma-1)A_n|$ is the power of l which divides $h \cdot e(\mathfrak{p})/([k_n:k](E:E \cap N_{k_n/k}k_n))$ where h is the class number and E the unit group of k, and $e(\mathfrak{p})$ is the ramification index of $\mathfrak{p}$ in k_n. Since $e(\mathfrak{p}) \leqslant [k_n:k_0]$, $|A_n/(\sigma-1)A_n| \leqslant h$.

LEMMA 5. *Let K/k be a Z_l-extension such that $|(A_n)^{G_n}|$ is bounded for all n. Then $T \nmid H_K(T)$.*

Proof. If $X = \mathrm{Gal}(L/F)$ for L the maximal abelian unramified l-extension of K then $X \approx \varprojlim A_n$ as Λ-modules, where the limit is taken with respect to norm maps, [3]. Thus if ${}_TX$ is the submodule of X annihilated by T, ${}_TX \approx \varprojlim (A_n)^{G_n}$ (recall $T \leftrightarrow \sigma - 1$), which is finite by assumption. This implies that ${}_TE$ is finite where E is the elementary module associated with X. Therefore, $T \nmid H_K(T)$.

THEOREM 5. *Let k/Q be a totally complex abelian extension with Galois group Δ having as exponent a divisor of $l-1$. Suppose only one prime of k lies above l. Then for any $\chi \in \hat{\Delta}$, $\chi(J) = -1$ or $\chi = \chi_0$, the order of χ in $\hat{\Delta}$ divides λ_χ.*

Proof. This follows from Theorem 3 and Lemmas 4 and 5.

COROLLARY 3. *For $k = Q(\zeta)$, ζ a primitive l-th root of 1, the order of χ in $\hat{\Delta}$ divides λ_χ for χ such that $\chi(J) = -1$ or $\chi = \chi_0$.*

We would like to point out that Theorem 4 has been proved independently by R. Gillard [5].

Added in proof: J.-F. Jaulent has recently obtained results similar to some of those in this article.

— *Théorie d'Iwasawa des tours métabeliennes*, Séminaire de théorie des Nombres de Bordeaux, exposée No. 21 (1980–81).

References

[1] A. Brumer, *On the units of algebraic number fields*, Mathematika 14 (1967), pp. 121–124.

[2] John Coates, *On K_2 and some classical conjectures in algebraic number theory*, Annals of Math. 95 (1972), pp. 99–116.

[3] K. Iwasawa, *On Z_l-extensions of algebraic number fields*, Annals of Math., series 2, 98 (1973), pp. 246–326.

[4] John Tate, *Global class field theory, algebraic number theory*, Thompson Book Company, Washington 1967, pp. 162–203.

[5] R. Gillard, *Remarques sur certaines extensions prodiédrales de corps de nombres*, C. R. Acad. Sci. Paris, Ser. A-B, 282 (1976).

CALIFORNIA INSTITUTE OF TECHNOLOGY
Pasadena, California

Current address
CONCORDIA UNIVERSITY
Montreal, Quebec, Canada

Received on 19.1.1976
and in revised form on 20.4.1979 (806)

ACTA ARITHMETICA
XL (1981)

On the rationality of periods of primitive forms

by

KAZUYUKI HATADA (Tokyo)

Introduction. In this paper, we give a new proof of the algebraic property of the periods of primitive forms F of Neben type. We also study p-adic Hecke series attached to the F, which take algebraic values.

Let Γ be a finite index subgroup of $\mathrm{SL}(2, \mathbf{Z})$, $w+2 \geqslant 2$ be a rational integer, $S_{w+2}(\Gamma)$ be the space of cusp forms of weight $w+2$ with respect to Γ, ϱ_w be the representation $\mathrm{GL}(2, \mathbf{R}) \to \mathrm{GL}(w+1, \mathbf{R})$ given by

$$\varrho_w\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}\right) dz_w = {}^t\big((cz+d)^w,\ (cz+d)^{w-1}(az+b),\ (cz+d)^{w-2}(az+b)^2,\ \ldots,\ (az+b)^w\big)dz$$

($dz_w = {}^t(dz, z\,dz, z^2dz, \ldots, z^w dz)$: the $\mathbf{C}^{w+1}$ valued differential form on the upper half plane H), $\varrho_w|_\Gamma$ be the restriction of ϱ_w to Γ, $\operatorname{Ind}_{\Gamma\uparrow \mathrm{SL}(2,\mathbf{Z})} \varrho_w|_\Gamma$ be the induced representation of $\varrho_w|_\Gamma$, P be the set consisting of all the parabolic elements in $\mathrm{SL}(2, \mathbf{Z})$ and $H^1_{P\cap\Gamma}(\Gamma, \varrho_w|_\Gamma, R)$ (resp. $H^1_P\big(\mathrm{SL}(2, \mathbf{Z}), \operatorname{Ind}_{\Gamma\uparrow \mathrm{SL}(2,\mathbf{Z})} \varrho_w|_\Gamma, R\big)$ be the parabolic cohomology group with the coefficients in a commutative ring R. Now let $j_2\big(H^1_{P\cap\Gamma}(\varrho_w|_\Gamma, \mathbf{Z})\big)$ (resp. $j_1\big(H^1_P(\operatorname{Ind} \varrho_w|_\Gamma, \mathbf{Z})\big)$) denote the image of the whole domain: Image (j_2) (resp. Image (j_1)) under the canonical homomorphism

$$j_2\colon H^1_{P\cap\Gamma}(\Gamma, \varrho_w|_\Gamma, \mathbf{Z}) \to H^1_{P\cap\Gamma}(\Gamma, \varrho_w|_\Gamma, \mathbf{R})$$

(resp. $j_1\colon H^1_P\big(\mathrm{SL}(2, \mathbf{Z}), \operatorname{Ind}_{\Gamma\uparrow \mathrm{SL}(2,\mathbf{Z})} \varrho_w|_\Gamma, \mathbf{Z}\big) \to H^1_P\big(\mathrm{SL}(2, \mathbf{Z}), \operatorname{Ind}_{\Gamma\uparrow \mathrm{SL}(2,\mathbf{Z})} \varrho_w|_\Gamma, \mathbf{R}\big)$) which is induced by the natural inclusion $\mathbf{Z} \hookrightarrow \mathbf{R}$. In § 2, we prove:

THEOREM 0.1 (1). (For details, see Theorems 2.2–2.4 in § 2.) *Let* sh *be the map of Shapiro*:

$$H^1\big(\mathrm{SL}(2, \mathbf{Z}), \operatorname{Ind}_{\Gamma\uparrow \mathrm{SL}(2,\mathbf{Z})} \varrho_w|_\Gamma, \mathbf{Z}\big) \to H^1(\Gamma, \varrho_w|_\Gamma, \mathbf{Z}).$$

(1) This theorem has some applications to congruence properties of eigenvalues of Hecke operators. (Cf. K. Hatada: *On the divisibility by 2 of the eigenvalues of Hecke operators*, Proc. Japan Acad. 53A, (1977), pp. 37–40, and K. Hatada: *Congruences of the eigenvalues of Hecke operators*, Proc. Japan Acad. 53A, (1977), pp. 125–128. Also cf. K. Hatada: *Eigenvalues of Hecke operators on* $\mathrm{SL}(2, \mathbf{Z})$, to appear in Math. Ann.)