Zeitschrift: Commentarii Mathematici Helvetici

Herausgeber: Schweizerische Mathematische Gesellschaft

Band: 63 (1988)

Artikel: A Riemann-Hurwitz formula for the Selmer group of an elliptic curve with complex multiplication.

Autor: Wingberg, Kay

DOI: https://doi.org/10.5169/seals-48221

Nutzungsbedingungen

Die ETH-Bibliothek ist die Anbieterin der digitalisierten Zeitschriften auf E-Periodica. Sie besitzt keine Urheberrechte an den Zeitschriften und ist nicht verantwortlich für deren Inhalte. Die Rechte liegen in der Regel bei den Herausgebern beziehungsweise den externen Rechteinhabern. Das Veröffentlichen von Bildern in Print- und Online-Publikationen sowie auf Social Media-Kanälen oder Webseiten ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. Mehr erfahren

Conditions d'utilisation

L'ETH Library est le fournisseur des revues numérisées. Elle ne détient aucun droit d'auteur sur les revues et n'est pas responsable de leur contenu. En règle générale, les droits sont détenus par les éditeurs ou les détenteurs de droits externes. La reproduction d'images dans des publications imprimées ou en ligne ainsi que sur des canaux de médias sociaux ou des sites web n'est autorisée qu'avec l'accord préalable des détenteurs des droits. En savoir plus

Terms of use

The ETH Library is the provider of the digitised journals. It does not own any copyrights to the journals and is not responsible for their content. The rights usually lie with the publishers or the external rights holders. Publishing images in print and online publications, as well as on social media channels or websites, is only permitted with the prior consent of the rights holders. Find out more

Download PDF: 11.04.2026

ETH-Bibliothek Zürich, E-Periodica, https://www.e-periodica.ch

Comment. Math. Helvetici 63 (1988) 587–592 0010–2571/88/040587–06$01.50 + 0.20/0
© 1988 Birkhäuser Verlag, Basel

A Riemann–Hurwitz formula for the Selmer group of an elliptic curve with complex multiplication

KAY WINGBERG

In 1981 Iwasawa considered p-adic Galois representations obtained by the action of the Galois group of a finite p-extension on a $\mathbf{Q}_p$-vector space defined by the ideal class group of the cyclotomic $\mathbf{Z}_p$-extension of a number field. More precisely his result is as follows [4]: Let p be an odd prime number and let L be a CM-field which is a finite Galois p-extension of the cyclotomic $\mathbf{Z}_p$-extension k_∞ of a CM-field k with Galois group $G = G(L/k_\infty)$ and ring of integers $\mathcal{O}(L)$. Assuming the Iwasawa-μ-invariant of k_∞ is zero the structure of the minus part of the Pontryagin dual of the flat cohomology group $H^1(\mathcal{O}(L), \mu_{p^\infty})$ as $\mathbf{Q}_p[G]$-module is given by the isomorphism

$$(H^1(\mathcal{O}(L), \mu_{p^\infty})^-)^* \otimes \mathbf{Q}_p \cong \mathbf{Q}_p^\delta \oplus \mathbf{Q}_p[G]^{\lambda^-(k_\infty)-\delta} \oplus \bigoplus_{\substack{v \nmid p \\ \mu_p \subset k_v^+}} \mathrm{Ind}_{G_v}^G (I(G_v))$$

where δ is equal to 1 if k contains the group μ_p of p-th roots of unity and 0 otherwise; $\lambda^-(k_\infty)$ denotes the λ-invariant of $(H^1(\mathcal{O}(k_\infty), \mu_{p^\infty})^-)^*$, G_v is the decomposition group of G relative to a prime v of k_∞^+ and $I(G_v)$ is the augmentation ideal of $\mathbf{Q}_p[G_v]$. (If $\lambda^-(k_\infty) = 0$ and $\delta = 1$ the isomorphism should be interpreted in the Grothendieck group of finitely generated $\mathbf{Q}_p[G]$-modules.) Observe that $H^1(\mathcal{O}(L), \mu_{p^\infty})^-$ is just the minus part of the p-component of the Picard group Pic $\mathcal{O}(L)$.

The corresponding identity between the dimensions on both sides is the Riemann–Hurtwitz formula proved by Kida [6].

Our aim is to show an analogous formula for the Selmer group of an elliptic curve E defined over a number field F which has complex multiplication by the ring of integers of an imaginary quadratic field K. In this case p has to be an odd prime number, which splits in K, i.e. $p = \mathfrak{p}\mathfrak{p}^*$, and where E has good (ordinary) reduction. Let F_∞ be the unique $\mathbf{Z}_p$-extension inside $F(E(\mathfrak{p}))$ and let L be a finite Galois p-extension of F_∞ with Galois group G unramified at all primes above $\mathfrak{p}^*$. For the Selmer group $H^1(\mathcal{O}(L), E(\mathfrak{p}))$ (we do not distinguish in the notations between the Néron model and its generic fiber) we will then show the following result,

THEOREM. *Assuming*

$$F(E_{\mathfrak{p}})/K \text{ is abelian} \tag{1.0}$$

then there is a $\mathbf{Q}_p[G]$*-isomorphism*

$$H^1(\mathcal{O}(L), E(\mathfrak{p}))^* \otimes \mathbf{Q}_p \cong \mathbf{Q}_p^\varepsilon \oplus \mathbf{Q}_p[G]^{\lambda_{\mathfrak{p}}(F_\infty)-\varepsilon} \oplus \bigoplus_{\substack{v \nmid \mathfrak{p} \\ F_v(E_{\mathfrak{p}})=F_v}} \mathrm{Ind}_{G_v}^G (I(G_v))$$

where ε *is equal to* 1 *if* $F = F(E_{\mathfrak{p}})$ *and* 0 *otherwise and* $\lambda_{\mathfrak{p}}(F_\infty)$ *denotes the* λ*-invariant of* $H^1(\mathcal{O}(F_\infty), E(\mathfrak{p}))^*$ *(if* $\lambda_{\mathfrak{p}}(F_\infty) - \varepsilon$ *is negative the isomorphism should be considered in the Grothendieck group). In particular, if* e_w *is the ramification index of* L/F_∞ *relative to a prime* w *of* L*, then*

$$\varepsilon - \lambda_{\mathfrak{p}}(L) = (\varepsilon - \lambda_{\mathfrak{p}}(F_\infty))[L:F_\infty] - \sum_{\substack{w \nmid \mathfrak{p} \\ L_w(E_{\mathfrak{p}})=L_w}} (e_w - 1).$$

Instead of assuming $\mathcal{F} = F(E_{\mathfrak{p}})$ to be an abelian extension of K we will prove the theorem under the more general conditions:

$\mathcal{F}_\infty$ satisfies the weak $\mathfrak{p}$-adic Leopold-conjecture, see [1] p. 124. (1.1)

The μ-invariant of $H^1(\mathcal{O}(\mathcal{F}_\infty), E(\mathfrak{p}))^*$ is zero. (1.2)

These assertions are true if $\mathcal{F}/K$ is abelian, [1] Proposition 15, [2] Theorem 3.4. As a consequence of (1.1) and (1.2) the following is true:

(2) The Pontryagin dual of

$$H^1(\mathcal{O}(F_\infty), E(\mathfrak{p})) \cong H^1(G(\mathcal{F}_{S_{\mathfrak{p}}}/\mathcal{F}_\infty), E(\mathfrak{p}))^\Delta$$

is a free $\mathbf{Z}_p$-module of finite rank $\lambda_{\mathfrak{p}}(F_\infty)$, [1] Theorem 12, Proposition 22, where L_S is the maximal p-extensions of a field L unramified outside a set S of primes of L, $S_{\mathfrak{p}} = \{v \mid \mathfrak{p}\}$ and $\Delta = G(\mathcal{F}/F)$. Furthermore, let S be a finite set of primes such that $S \cap S_p = S_{\mathfrak{p}}$ then according to [8], Theorem, the assertions (1.2) and (2) imply:

$G(F_S/F_\infty)$ is free pro-p-group of finite rank. (3.1)

For $T \supseteq S$ the canonical map (3.2)

$$*_{v \in T \setminus S(F_S)} T_v(F(p)/F_\infty) \xrightarrow{\sim} G(F_T/F_S)$$

from the free pro-p-product of inertia groups into $G(F_T/F_S)$ induced by the maps

$$T_v(F(p)/F_\infty) = T_v(F(p)/F_S) \hookrightarrow G(F(p)/F_S) \twoheadrightarrow G(F_T/F_S)$$

is an isomorphism.

LEMMA 4. *The assertions* (3.1) *and* (3.2) *are stable under base change by a finite Galois p-extension unramified at all primes above $\mathfrak{p}^*$.*

Proof. Let L/F_∞ be a finite Galois p-extension unramified at $S_{\mathfrak{p}^*}$ and let T be a finite set of primes such that $L \subset F_T$ and $T \cap S_p = S_{\mathfrak{p}}$. Then by (3.1) the Galois group $G(L_T/L)$ of $L_T = F_T$ over L is free of finite rank. Hence we obtain for the factor group $G(L_{S_{\mathfrak{p}}}/L)$

$$\mathrm{rank}_\Lambda G(L_{S_{\mathfrak{p}}}/L)^{ab} = 0,$$
$$\mu(G(L_{S_{\mathfrak{p}}}/L)^{ab}) = \mu(G(L_T/L)^{ab}) = 0.$$

Again by [8], Theorem, the assertions (3.1) and (3.2) are true for L.

LEMMA 5. *Let G and Δ be finite groups of p-power order and order prime to p, respectively. Let M be a $\mathbf{Z}_p$-torsion free $\mathbf{Z}_p[G \times \Delta]$-module with the properties*
(a) $H^1(G, M) = 0$,
(b) $H^2(G, M) \cong \mathbf{Z}/(G:1)\mathbf{Z}$,
(c) $H^2(G \times \Delta, M) \neq 0$.
Then for every $\mathbf{Z}_p$-irreducible character χ of Δ, i.e., $\mathbf{Z}_p[\Delta] = \bigoplus_\chi \mathbf{Z}_p[\Delta]^\chi$, there are numbers $m_\chi \geq 0$ and $\mathbf{Z}_p[G]$-isomorphisms

$$M^\chi \cong \mathbf{Z}_p[G]^{m_\chi} \quad \text{for} \quad \chi \neq \chi_0 := 1,$$
$$M^{\chi_0} \cong R_d^{ab} \oplus \mathbf{Z}_p[G]^{m_{\chi_0}},$$

where R_d is defined by a minimal presentation $1 \to R_d \to F_d \to G \to 1$ of the group G be a free pro-p-group F_d of rank d.

Proof. Let M^χ be the eigenspace of M with respect to χ, then

$$H^1(G, M) = \bigoplus_\chi H^1(G, M^\chi) = 0,$$

$$H^2(G, M) = \bigoplus_\chi H^2(G, M^\chi) \cong \mathbf{Z}/(G:1)\mathbf{Z}$$

Because $H^2(G, M^{\chi_0}) \cong H^2(G \times \Delta, M) \neq 0$ we obtain

$$H^2(G, M^{\chi}) \cong \begin{cases} \mathbf{Z}/(G:1)\mathbf{Z}, & \chi = \chi_0 \\ 0, & \chi \neq \chi_0. \end{cases}$$

This shows that for $\chi \neq \chi_0$ the $\mathbf{Z}_p[G]$-module M^{χ} is cohomologically trivial and therefore $\mathbf{Z}_p[G]$-free, as M is torsion free, [5] Lemma 1.6. According to [5] Korollar 1.8 we obtain the assertion for the eigenspace of the trivial character.

COROLLARY 6. *Let*

$$\begin{array}{ccccccccc}
1 & \longrightarrow & H & \longrightarrow & F & \longrightarrow & G & \longrightarrow & 1 \\
 & & \| & & \downarrow & & \downarrow & & \\
1 & \longrightarrow & H & \longrightarrow & \mathcal{F} & \longrightarrow & G \times \Delta & \longrightarrow & 1 \\
 & & & & \downarrow & & \downarrow & & \\
 & & & & \Delta & = & \Delta & &
\end{array}$$

be a commutative and exact diagram of profinite groups, where F is a free pro-p-group of finite rank and Δ is a finite group of order prime to p. Then for every $\mathbf{Z}_p$-irreducible character χ of Δ there is a $\mathbf{Q}_p[G]$-isomorphism

$$(H^{ab})^{\chi} \otimes \mathbf{Q}_p \cong \mathbf{Q}_p[G]^{n_\chi - \delta_\chi} \oplus \mathbf{Q}_p^{\delta_\chi}$$

where

$$\delta_\chi = \begin{cases} 1, & \chi = \chi_0 \\ 0, & \chi \neq \chi_0 \end{cases} \quad \textit{and} \quad n_\chi = \operatorname{rank}_{\mathbf{Z}_p} (F^{ab})^{\chi}$$

Proof. For the $\mathbf{Z}_p[G \times \Delta]$-module H^{ab} the conditions of Lemma 5 are fulfilled because $scd_p(F) \leq 2$, [3] Definition 10 and Proposition 11, and

$$H^2(G \times \Delta, H^{ab}) \xrightarrow[\sim]{\text{res}} H^2(G, H^{ab})^{\Delta} \xrightarrow[\sim]{} \hat{H}^0(G, \mathbf{Z}_p)_{\Delta} \cong \mathbf{Z}/(G:1)\mathbf{Z}.$$

Since

$$H^{ab} \otimes \mathbf{Q}_p \cong \mathbf{Q}_p[G]^{d-1} \oplus \mathbf{Q}_p, \qquad d = \operatorname{rank} F,$$

we obtain $\mathbf{Q}_p[G]$-isomorphisms

$$(H^{ab})^{\chi} \otimes \mathbf{Q}_p \cong \mathbf{Q}_p[G]^{m_\chi} \oplus \mathbf{Q}_p^{\delta_\chi}$$

for some $m_\chi \geq 0$. These numbers are easily calculated. Since G and Δ commute we get by taking G-coinvariants

$$\begin{aligned} m_\chi + \delta_\chi &= \operatorname{rank}_{\mathbf{Z}_p} ((H^{ab})^\chi)_G \\ &= \operatorname{rank}_{\mathbf{Z}_p} (H^{ab}_G)^\chi \\ &= \operatorname{rank}_{\mathbf{Z}_p} (F^{ab})^\chi = n_\chi . \end{aligned}$$

Proof of the Theorem. Let $L \mid F_\infty$ be a finite Galois p-extension unramified at all primes above $\mathfrak{p}^*$ and contained in F_S, S a finite set with $S \cap S_p = S_\mathfrak{p}$. Let $\mathscr{L} = L(E_\mathfrak{p})$, $\Delta = G(\mathscr{L}/L)$ and $G = G(L/F_\infty)$. Then we obtain a commutative and exact diagram

$$\begin{array}{ccccccccc} 1 & \longrightarrow & G(\mathscr{F}_S/\mathscr{L}) & \longrightarrow & G(\mathscr{F}_S/\mathscr{F}_\infty) & \longrightarrow & G & \longrightarrow & 1 \\ & & \| & & \downarrow & & \downarrow & & \\ 1 & \longrightarrow & G(\mathscr{F}_S/\mathscr{L}) & \longrightarrow & G(\mathscr{F}_S/F_\infty) & \longrightarrow & G \times \Delta & \longrightarrow & 1 \\ & & & & \downarrow & & \downarrow & & \\ & & & & \Delta & = & \Delta & & \end{array}$$

From Corollary 6 it follows that

$$\begin{aligned} (H^1(G(\mathscr{F}_S/\mathscr{L}), E(\mathfrak{p}))^\Delta)^* \otimes \mathbf{Q}_p &= (H^1(G(\mathscr{F}_S/\mathscr{L}), \mathbf{Q}_p/\mathbf{Z}_p)^\chi(1))^* \otimes \mathbf{Q}_p \\ &\cong \mathbf{Q}_p[G]^{\lambda_\mathfrak{p}(F_\infty) + \#\{v \in S \setminus S_\mathfrak{p} \mid F_v(E_\mathfrak{p}) = F_v\} - \varepsilon} \oplus \mathbf{Q}_p^\varepsilon , \end{aligned}$$

where (1) denotes the twist with $E(\mathfrak{p})$ and χ is the character given by the action of Δ on $E_\mathfrak{p}$. Here we use (3.1) and (3.2) which give

$$\begin{aligned} \operatorname{corank}_{\mathbf{Z}_p} H^1(G(\mathscr{F}_S/\mathscr{F}_\infty), \mathbf{Q}_p/\mathbf{Z}_p)^\chi &= \operatorname{corank}_{Z_p} H^1(G(\mathscr{F}_{S_\mathfrak{p}}/\mathscr{F}_\infty), \mathbf{Q}_p/\mathbf{Z}_p)^\chi \\ &\quad + \sum_{v \in S \setminus S_\mathfrak{p}} \operatorname{corank}_{\mathbf{Z}_p} H^1(T_v(\mathscr{F}(p)/\mathscr{F}_\infty), \mathbf{Q}_p/\mathbf{Z}_p)^\chi \\ &= \lambda_\mathfrak{p}(F_\infty) + \#\{v \in S \setminus S_\mathfrak{p} \mid F_v(E_\mathfrak{p}) = F_v\} \end{aligned}$$

Again with (3.1) and (3.2) and Lemma 4 we obtain

$$\begin{aligned} (H^1(G(\mathscr{F}_S/\mathscr{L}), E(\mathfrak{p}))^\Delta)^* \otimes \mathbf{Q}_p &\cong (H^1(G(\mathscr{L}_{S_\mathfrak{p}}/\mathscr{L}), E(\mathfrak{p}))^\Delta)^* \otimes \mathbf{Q}_p \\ &\quad \oplus \bigoplus_{v \in S \setminus S_\mathfrak{p}(L)} (H^1(T_v(\mathscr{F}(p)/\mathscr{L}), \mathbf{Q}_p/\mathbf{Z}_p)^\chi(1))^* \otimes \mathbf{Q}_p \\ &\cong (H^1(G(\mathscr{L}_{S_\mathfrak{p}}/\mathscr{L}), E(\mathfrak{p}))^\Delta)^* \otimes \mathbf{Q}_p \\ &\quad \oplus \bigoplus_{\substack{w \in S \setminus S_\mathfrak{p}(L) \\ L_w(E_\mathfrak{p}) = L_w}} \mathbf{Q}_p \end{aligned}$$

Thus we get an isomorphism

$$(H^1(\mathcal{O}(L), E(\mathfrak{p}))^* \otimes \mathbf{Q}_p \oplus \mathbf{Q}_p^{\#\{w \in S\setminus S_{\mathfrak{p}}(L) \mid L_w(E_{\mathfrak{p}})=L_w\}}$$
$$\cong \mathbf{Q}_p^{\varepsilon} \oplus \mathbf{Q}_p[G]^{\lambda_{\mathfrak{p}}(F_\infty)-\varepsilon} \oplus \bigoplus_{\substack{v \in S\setminus S_p(F_\infty) \\ F_v(E_{\mathfrak{p}})=F_v}} \mathrm{Ind}_{G_v}^{G} \mathbf{Q}_p[G_v]$$

which proves the theorem.

Acknowledgement

I would like to thank the Mathematical Sciences Research Institute for its hospitality and the DFG for support while this work was done.

REFERENCES

[1] COATES, J., *Infinite descent on elliptic curves in: Arithmetic and Geometry, papers dedicated to I. R. Shafarevich on the occasion of his 60th birthday, Vol. I,* Progress in Math *35* (1983), 107–137.

[2] GILLARD, R., *Functions L p-adiques des corps quadratiques imaginaires et de leur extensions abéliennes.* J. reine u. angew. Math *358* (1985), 76–91.

[3] HABERLAND, K., "Galois cohomology of algebraic number fields," VEB Verlag der Wissenschaften, Berlin, 1978.

[4] IWASAWA, K., *Riemann–Hurwitz formula and p-adic Galois representations for number fields,* Tohoku. Math. J. *33* (1981), 263–288.

[5] JANNSEN, U. and WINGBERG, K., *Die p-Vervollständigung der multiplikativen Gruppe einer p-Erweiterung eines irregulären p-adischen Zahlkörpers,* J. reine u. angew. Math. *307/308* (1979), 399–410.

[6] KIDA, Y., *ℓ-extension of CM-fields and cyclotomic invariants,* J. Number theory. *12* (1980), 519–528.

[7] WINGBERG, K., *Ein Analogon zur Fundamentalgruppe einer Riemann'schen Fläche im Zahlkörperfall,* Invent. Math. *77* (1984), 557–584.

[8] WINGBERG, K., *Galois groups of number fields generated by torsion points of elliptic curves,* Nagoya Math. J. *104* (1986), 43–53.

Mathematisches Institut,
Universität Erlangen-Nürnberg,
Bismarckstraße 1 1/2,
D 8520 *Erlangen, West-Germany*

Received March 3, 1987