Trends in Mathematics
Information Center for Mathematical Sciences
Volume 3, December 2000, Pages 108–111

IWASAWA INVARIANTS

JANGHEON OH

ABSTRACT. We survey various results of Iwasawa invariants of ideal class groups and of Selmer groups of elliptic curves.

1. IDEAL CLASS GROUPS

Let F be a number field and let p be a prime number. Consider a tower of number fileds

$$F = F_0 \subset F_1 \subset \cdots \subset F_n \subset \cdots$$

such that F_n/F is a cyclic extension of degree p^n. Let $F_\infty = \cup_{n\geq 0} F_n$. Iwasawa proved the following now famous theorem [10].

Theorem 1. *Let p^{e_n} be the highest power of p dividing the class number of F_n. Then there exist integers λ, μ and ν such that $e_n = \lambda n + \mu p^n + \nu$ for all sufficiently large n.*

Iwasawa's proof of this theorem is based on studying the Galois group $X = Gal(L_\infty/F_\infty)$ as a $\Lambda = \mathbb{Z}_p[[T]]$-module, where $L_\infty = \cup_{n\geq 0} L_n$ and L_n is the p-part of the Hilbert class field of F_n. If $x \in X$, one defines $(1+T)\cdot x = \gamma \cdot x = \tilde{\gamma} x \tilde{\gamma}^{-1}$, where $\tilde{\gamma} \in Gal(L_\infty/F)$ is an extension of a topological generator $\gamma \in Gal(F_\infty/F)$. By analyzing p-adic L-functions constructed by Iwasawa, Ferrero and Washington [4] proved that the Iwasawa invariant μ vanishes when $F/\mathbb{Q}$ is abelian and F_∞/F is the cyclotomic $\mathbb{Z}_p$-extension. But it is still an open problem that the μ-invariant vanishes for the cyclotomic $\mathbb{Z}_p$-extension over arbitrary number field F. The Kronecker-Webber theorem and Iwasawa's construction of p-adic L-functions play a very important role in the case of $F/\mathbb{Q}$ abelian. By a different approach to p-adic L-functions, Sinnott [19] gave a new proof of the Ferrero-Washington theorem($\mu = 0$) . We can construct an "elliptic" $\mathbb{Z}_p$-extension of an imaginary quadratic field k, which is not cyclotomic $\mathbb{Z}_p$-extension. Let E be an elliptic curve with complex multiplication $\mathfrak{o}_k$, the ring of integers of k and let $p = \mathfrak{p}\mathfrak{p}^*$ split in k. Then there exist an infinite extension $k_\infty \subset k(E[\mathfrak{p}^\infty])$ such that $Gal(k_\infty/k) \simeq \mathbb{Z}_p$, where $k(E[\mathfrak{p}^\infty])$ is an infinite extension of k obtained by adding $\mathfrak{p}$-power torsion points of E to k. By using Sinnott's method, Schneps [18] proved that the μ-invariant for the $\mathbb{Z}_p$-extension k_∞/k vanishes. By class field theory, the compositum of all $\mathbb{Z}_p$-extensions over an imaginary quadratic field is $\mathbb{Z}_p{}^2$. Among the $\mathbb{Z}_p$-extensions, there is an anti-cyclotomic $\mathbb{Z}_p$-extension on which the complex conjugation acts inversely. It is easy to see that if p stays prime in k, then it splits completely in

2000 *Mathematics Subject Classification.* 11R23, 11G05.
Key words and phrases. Iwasawa theory, class numbers, selmer groups, elliptic curves.
Received August 31, 2000.

the anti-cyclotomic $\mathbb{Z}_p$-extension. It is believed that the μ-invariant for the anti-cyclotomic $\mathbb{Z}_p$-extension vanishes. Iwasawa [11] constructed a $\mathbb{Z}_p$-extension with $\mu > 0$, in which infinitely many primes split completely.

In a paper [13], Oh proved that the zeta function ζ_k for any number field k determines the λ-invariant of the cyclotomic $\mathbb{Z}_p$-extension of k. But it is still an open problem that the μ-invariant is also determined by a zeta function. When the base field F is a totally real field and F_∞/F is the cyclotomic $\mathbb{Z}_p$-extension(the cyclotomic $\mathbb{Z}_p$-extension is the only $\mathbb{Z}_p$-extension of a totally real field F if Leopoldt conjecture is true), Greenberg [7] conjectured that μ and λ-invariants vanish. See [1, 3, 5, 6, 12, 14, 17] for many partial results on the Greenberg conjecture. It should be noted that Greenberg's conjecture is closely related to capitulation problem. See [2, 5, 14] for this topic. When the base field is an imaginary quadratic field, $\lambda \geq 1$ for the cyclotomic $\mathbb{Z}_p$-extension if p splits in k or the class number $h_k > 1$. Following a method of Sinnott [19], we [15] can compute λ-invariants of the cyclotomic $\mathbb{Z}_3$-extension of imaginary quadratic fields. It is an open question whether λ is unbounded as imaginary quadratic fields k vary. We do not have any results on the explicit computation of the λ-invariants of non-cyclotomic $\mathbb{Z}_p$-extensions.

The $\ell \neq p$ part of the class number of the cyclotomic $\mathbb{Z}_p$-extensions of abelian number fields is bounded. See [21, 16].

2. Selmer groups

Let E be an elliptic curve defined over a number field F and let M be any algebraic extension of F. If η is any prime of M, we define M_η to be the union of the η-adic completions of all finite extensions of F contained in M. We will let κ_η denote the Kummer homomorphism for E :

$$\kappa_\eta : E(M_\eta) \otimes (\mathbb{Q}_p/\mathbb{Z}_p) \to H^1(M_\eta, E[p^\infty]).$$

If $\alpha = a \otimes (m/n + \mathbb{Z}_p) \in E(M_\eta) \otimes (\mathbb{Q}_p/\mathbb{Z}_p)$, then $\kappa_\eta(\alpha)$ is the class of the 1-cocycle ϕ_α given by $\phi_\alpha(g) = g(b) - b$ for all $g \in G_{M_\eta}$. Here $b \in E(\overline{M_\eta})$ satisfies $nb = ma$ on $E(\overline{M_\eta})$. We define the p-primary subgroup of the Selmer group for E over M.

$$Sel_E(M)_p = ker(H^1(M, E[p^\infty]) \to \prod_\eta H^1(M_\eta, E[p^\infty])/Im(\kappa_\eta)),$$

where η runs over all primes of M. We say that $Sel_E(F_\infty)_p$ is Λ-cotorsion if $X_E(F_\infty) = Hom(Sel_E(F_\infty)_p, \mathbb{Q}_p/\mathbb{Z}_p)$ is Λ-torsion, i.e., $X_E(F_\infty) \sim \bigoplus_i \Lambda/f_i^{a_i}$. Here F_∞ is the cyclotomic $\mathbb{Z}_p$-extension of F and $f_i \in \mathbb{Z}_p[[T]]$ is non-unit. By the p-adic Weierstrass Preparation Theorem, we may uniquely write $\prod_i f_i^{a_i} = f(T) = p^{\mu_E} P_E(T) U_E(T)$ with $\mu_E \geq 0$, $P_E(T)$ distinguished, and $U_E(T) \in \Lambda^*$. Kato proved that if $E/\mathbb{Q}$ is modular and E has good, ordinary ,or multiplicative reduction at p, and $F/\mathbb{Q}$ is abelian, then $Sel_E(F_\infty)_p$ is Λ-torsion. One [8] can prove that if $Sel_E(F_\infty)_p$ is Λ-torsion, then the rank of the Mordell-Weil group $E(F_n)$ is bounded above by λ_E(=degree of $P_E(T)$). We denote the maximal rank of Mordell-Weil group of $E(F_n)$ by λ_E^{M-W}. Now we [8]have the following analogue of Iwasawa's theorem.

Theorem 2. *Assume that E has good, ordinary reduction at all primes of F lying over p. Assume that $Sel_E(F_\infty)_p$ is Λ-cotorsion and that $III_E(F_n)_p$ is finite for all $n \geq 0$. Then there exist λ, μ and ν such that $|III_E(F_n)_p| = p^{e_n}$, where $e_n = \lambda n + \mu p^n + \nu$. Here $\lambda = \lambda_E - \lambda_E^{M-W}$ and $\mu = \mu_E$.*

Each of the invariants λ_E^{M-W}, λ and μ_E can be strictly positive [8]. Let $E = X_0(11), p = 5, F = \mathbb{Q}$, and $F_\infty = \mathbb{Q}_\infty$ = the cyclotomic $\mathbb{Z}_5$-extension of $\mathbb{Q}$. Then $\mu_E = 1$.(In fact, $(F_E(T)) = (p)$.) For more examples, see [8]. It is conjectured that if $E[p]$ is irreducible as a $(\mathbb{Z}/p\mathbb{Z})$-representation of $G_{\mathbb{Q}}$, then $\mu_E = 0$ under the assumption that $Sel_E(\mathbb{Q}_\infty)_p$ is Λ-cotorsion. Recently, Greenberg and Vatsal [9] proved that $\mu_E = 0$ under the assumption that $E/\mathbb{Q}$ has good ordinary reduction at an odd prime p and E admits a $\mathbb{Q}$-isogeny of degree p with kernel Φ, and the action of $G_{\mathbb{Q}}$ on Φ is either ramified at p and even, or unramified at p and odd.

Let E be any one of the elliptic curves of conductor 11, and let ξ be a nontrivial character of an imaginary quadratic field $\mathbb{Q}(\sqrt{d})$ with $\xi(5) \neq 0$ and $p = 5$. Then one finds the following formula [8]:

$$\lambda_{E^\xi} = 2\lambda_\xi + \epsilon_\xi,$$

where E^ξ is the quadratic twist of E and λ_ξ is the lambda invariant(of ideal class group) of the cyclotomic $\mathbb{Z}_5$-extension of $\mathbb{Q}(\sqrt{d})$ and where $\epsilon_\xi = 1$ if 11 splits in $\mathbb{Q}(\sqrt{d})/\mathbb{Q}$, $\epsilon_\xi = 0$ if 11 is inert or ramified. Note that λ_ξ is conjecturally unbounded as ξ varies. Using this formula , one can prove [8] that $\lambda_{E^\xi}^{M-W} = 0$ when ξ corresponds to $\mathbb{Q}(\sqrt{-1})$, which means that the rank of Mordell-Weil group of $E(F_n)$ is zero for any n. Here F_n is the n-th layer of the cyclotomic $\mathbb{Z}_5$-extension of $\mathbb{Q}(\sqrt{-1})$.

References

[1] D.Byeon, Iwaswa λ-invariants of real quadratic fields, To appear in Compositio Math..

[2] A.Candiotti, On capitulation in certain $\mathbb{Z}_\ell$-extensions of number fields, Mathematika, 30(1983), 58-60.

[3] H.Ichimura and H.Sumida, On the Iwasawa λ-invariants of certain real abelian fields II, Internat.J.Math., 7(1996), 721-744.

[4] B.Ferrero and L.Washington, The Iwasawa invariant μ_p vanishes for abelian number fields, Ann. of Math.,109(1979), 377-395.

[5] T.Fukuda, K.Komatsu, M.Ozaki and H.Taya, Iwasawa λ_p-invariants of relative cyclic extensions of degree p, Tokyo J. Math., 20(1997), 475-480.

[6] T.Fukuda and H.Taya, The Iwasawa λ-invariants of $\mathbb{Z}_p$-extensions of real quadratic fields, Acta Arith., 69(1995), 277-292.

[7] R.Greenberg, On the Iwasawa invariants of totally real number fields, Amer.J.Math., 98(1976),263-284.

[8] R.Greenberg, Iwasawa theory for elliptic curves, Lecture Notes in Math., 1716, Springer-Verlag, 1999, 53-144.

[9] R.Greenberg and V.Vatsal, On the Iwasawa invariants of elliptic curves, Invent. Math.,

[10] K.Iwasawa, On Γ-extensions of algebraic number fields, Bull.Amer.math.Soc.65(1959), 183-226.

[11] K.Iwasawa, On the μ-invariants of $\mathbb{Z}_\ell$-extensions, Number Theory, Algebraic Geometry and Commutative Algebra(in honor of Y.Akizuki). Kinokuniya:Tokyo, 1973, 1-11.

[12] K.Komatsu, On the Iwasawa λ-invariants of quaternion extensions, Acta Arith., 87(1999), 219-221.

[13] J.Oh, On zeta functions and Iwasawa modules, Trans.Amer.Math.Soc.,350(1998), 3639-3655.

[14] J.Oh, On the λ-invariants of totally real fields, Proc.Japan Acad., 74(1998), 125-126.

[15] J.Oh, On the Iwasawa λ-invariants of imaginary quadratic fields, Proc.Japan Acad., 75(1999),29-31.

[16] J.Oh, ℓ-adic L-functions and rational function measures, Acta Arith., 83(1998), 369-379.

[17] M.Ozaki and H.Taya, A note on Greenberg's conjecture for real abelian number fields, Manuscripta Math.,88(1995), 311-320.

[18] L.Schneps, On the μ-invariant of p-adic L-functions attached to elliptic curves with complex multiplication, J.Number Theory, 25(1987), 20-33.

[19] W.Sinnott, On the μ-invariant of the Γ-transform of a rational function, Invent math., 75(1984), 273-282.

[20] L.Washington, *Introduction to Cyclotomic Fields*, Springer Berlin Heidelberg New York(1982)

[21] L.Washington, The non-p-part of the class number of in a cyclotomic $\mathbb{Z}_p$-extension, Invent Math., 49(1979),87-97.

Department of Applied mathematics, College of Natural Scinences, Sejong University, Seoul,143-747 , Korea

E-mail address: oh@sejong.ac.kr