45. A Remark on Ribet's Theorem

By Hajime NAKAZATO
Department of Mathematics, Tokyo Institute of Technology

(Communicated by Kunihiko KODAIRA, M. J. A., April 12, 1980)

Introduction. Let p be an odd prime, ζ_p be a primitive p-th root of unity and A be the p-Sylow subgroup of the ideal class group of $\boldsymbol{Q}(\zeta_p)$. In [5], Ribet obtained a remarkable theorem on the structure of A as a Galois module by means of modular forms. We obtain a generalization of this Ribet's Theorem.

After this work had been finished, Prof. M. Koike kindly informed the auther that he had obtained a result on the existence of modular forms satisfying a certain congruence (Koike [8]). By using his decisive result, he obtained a desirable generalization of our theorem.

Notations. For a prime p, let $\bar{\boldsymbol{Q}}_p$ (resp. $\bar{\boldsymbol{Q}}$) be an algebraic closure of $\boldsymbol{Q}_p$ (resp. $\boldsymbol{Q}$) and fix them. We fix embeddings $\bar{\boldsymbol{Q}}\to\boldsymbol{C}$ and $\bar{\boldsymbol{Q}}\to\bar{\boldsymbol{Q}}_p$, through which we regard elements of $\bar{\boldsymbol{Q}}$ as elements of $\boldsymbol{C}$ or $\bar{\boldsymbol{Q}}_p$. Let $\mathfrak{p}$ be the prime of $\bar{\boldsymbol{Q}}$, lying above p, corresponding to the fixed embedding $\bar{\boldsymbol{Q}}\to\bar{\boldsymbol{Q}}_p$. For a finite abelian group G, let $\hat{G}=\mathrm{Hom}\,(G, \bar{\boldsymbol{Q}}^\times)$. For a positive integer n, let ζ_n be a primitive n-th root of unity in $\bar{\boldsymbol{Q}}$.

§ 1. Put $m=5, 7$ or 11. Let p be an odd prime satisfying $(p, m\varphi(m))=1$, where φ is the Euler's φ-function. We use the following notations: $k=\boldsymbol{Q}\,(\cos(2\pi/m))$, $H=\mathrm{Gal}\,(k/\boldsymbol{Q})$, $K=k(\zeta_p)$, $G=\mathrm{Gal}\,(K/\boldsymbol{Q})$. Let ω be the Dirichlet character modulo p satisfying $\omega(a)\equiv a \bmod \mathfrak{p}$ for all integers a, $(a, p)=1$. For $\phi\in\hat{G}$, we identify ϕ with the primitive Dirichlet character attached to ϕ by class field theory. Then

$$\hat{G}=\{\psi\omega^i \mid \psi\in\hat{H},\ i \bmod (p-1)\}.$$

We say that $\phi\in\hat{G}$ is imaginary if ϕ (complex conjugation)$=-1$. Let $\hat{G}^-$ be the set of imaginary characters of G. For a positive integer i and for $\phi\in\hat{G}$, let $B_i(\phi)$ be the i-th generalized Bernoulli number associated with ϕ. For $\phi\in\hat{G}$, let Φ be the $\boldsymbol{Q}_p$-irreducible character of a representation of G which has ϕ as a $\bar{\boldsymbol{Q}}_p$-irreducible component. Then the orthogonal idempotent $e(\Phi)$ attached to Φ lies in the group ring $\boldsymbol{Z}_p[G]$ since $(p, [K:\boldsymbol{Q}])=1$. Let A be the p-Sylow subgroup of the ideal class group of K. We regard A as an additive group on which $\boldsymbol{Z}_p[G]$ acts naturally.

Our main result is the following

Theorem 1. *Let $\phi\in\hat{G}^-$. Then $B_1(\phi^{-1})\equiv 0 \bmod \mathfrak{p}$ if and only if $e(\Phi)A\neq 0$. In other words, let $\psi\in\hat{H}$ and let i be an even integer with $2\leq i\leq p-1$. Then $B_i(\psi^{-1})\equiv 0 \bmod \mathfrak{p}$ if and only if $e(\Psi\omega^{1-i})A\neq 0$, where*

$\Psi\omega^{1-i}$ is the $\boldsymbol{Q}_p$-irreducible character of G which has $\psi\omega^{1-i}$ as a $\bar{\boldsymbol{Q}}_p$-irreducible component.

Remark 1. The first statement and the second one are equivalent since $i^{-1}B_i(\psi^{-1})\equiv B_1(\psi^{-1}\omega^{i-1}) \bmod \mathfrak{p}$ (cf. 2.11 of [1]).

Remark 2. Note that $e(\Phi)A$ depends only on Φ if we consider Φ as the corresponding character of $\mathrm{Gal}(\bar{\boldsymbol{Q}}/\boldsymbol{Q})$. Hence Ribet's Theorem is equivalent to the second statement in the case of $\psi=$the trivial character. To prove Theorem 1 we may assume that ψ is a primitive Dirichlet character modulo m.

Remark 3. The fact that $e(\Phi)A\neq 0$ implies $B_1(\phi^{-1})\equiv 0 \bmod \mathfrak{p}$ is a result of the Stickelberger relations (cf. [3]).

§ 2. By Remark 2 in § 1, we may assume that ψ is an even primitive Dirichlet character whose conductor is m $(=5, 7$ or $11)$.

Lemma 1. *Let h_{pm}^- be the imaginary factor (i.e. the first factor) of the class number of $\boldsymbol{Q}(\zeta_{pm})$. If p is a prime such that $p\geqq 5$ and $p\neq m$. Then $h_{pm}^-<(4pm)(pm/24)^{\varphi(pm)/4}$.*

Proof. By the class number formula, we have

$$(h_{pm}^-)^2=(4pm)^2\prod_{\phi}|-2^{-1}B_1(\phi)|^2=(4pm)^2(2pm)^{-\varphi(pm)/2}\prod_{\phi}\left|\sum_{a=1}^{pm-1}\phi(a)a\right|^2.$$

Here ϕ runs over all odd primitive Dirichlet characters whose conductors divide pm. By the arithmetical-geometical mean inequality, we have

$$\left(\prod_{\phi}\left|\sum_{a}\phi(a)a\right|^2\right)^{2/\varphi(nm)}\leqq(2/\varphi(pm))\sum_{\phi}\left|\sum_{a}\phi(a)a\right|^2.$$

By a calculation (cf. [4]), we obtain

$$\begin{aligned}(2/\varphi(pm))\sum_{\phi}\left|\sum_{a}\phi(a)a\right|^2&=(2/\varphi(pm))\sum_{a,b=1}^{pm-1}\sum_{\phi}\phi(a)\overline{\phi(b)}ab\\&<6^{-1}pm(pm-1)(pm-2)\\&\quad-pm(pm-4p-4m)\{p(m-1)^2+m(p-1)^2\}(p-1)^{-1}(m-1)^{-1}\\&<6^{-1}(pm)^3.\end{aligned}$$

Combining these estimations, we have Lemma 1.

We note that the norm of $B_2(\psi)$ from $\boldsymbol{Q}$ (values of ψ) to $\boldsymbol{Q}$ is $2^2\cdot 5^{-1}$ (resp. $2^4\cdot 7^{-1}$, $2^8\cdot 5\cdot 11^{-1}$) if $m=5$ (resp. 7, 11). Hence we may assume that $4\leqq i\leqq p-1$. Put $\varepsilon=\psi^{-1}\omega^{i-2}$. Then ε is primitive and its conductor is pm.

As in the proof of Theorem (3.3) of [5], we have:

Lemma 2. *There exists a modular form of weight 2 and type ε on $\Gamma_0(pm)$ whose Fourier-expansion coefficients are $\mathfrak{p}$-integers in $\bar{\boldsymbol{Q}}$ and whose constant term is 1.*

Put

$$G_{2,\varepsilon}(z)=-\frac{1}{4}B_2(\varepsilon)+\sum_{n=1}^{\infty}\left(\sum_{d|n,d>0}\varepsilon(d)d\right)\exp(2\pi\sqrt{-1}nz).$$

This is an Eisenstein series of weight 2 and type ε on $\Gamma_0(pm)$. Note that $2^{-1}B_2(\varepsilon)\equiv i^{-1}B_i(\psi^{-1})\equiv B_1(\psi^{-1}\omega^{i-1}) \bmod \mathfrak{p}$.

As in the proof of Proposition (3.5) of [5], we obtain the following

Theorem 2. *Suppose that $B_i(\psi^{-1})\equiv 0 \bmod \mathfrak{p}$. Then there exists a cusp form f of weight 2 and type ε on $\Gamma_0(pm)$ which satisfies the following conditions:*

i) *f is a normalized common eigen-form for all Hecke operators.*

ii) *$f\equiv G_{2,\varepsilon} \bmod \mathfrak{p}$ in Fourier-expansions.*

§3. In this section, under the same assumption as in §2, we regard ϕ (resp. $\tilde{\phi}$) as the character of Gal $(\bar{\boldsymbol{Q}}/\boldsymbol{Q})$ via the natural projection (resp. the reduction of ϕ i.e. the map $x\mapsto\phi(x) \bmod \mathfrak{p}$).

Theorem 3. *Suppose that there exists a cusp form f satisfying the conditions in Theorem 2. Then there exists a finite field $\boldsymbol{F}\supset\boldsymbol{F}_p$ and a continuous representation*

$$\tilde{\rho}: \mathrm{Gal}\,(\bar{\boldsymbol{Q}}/\boldsymbol{Q})\to \mathrm{GL}\,(2,\boldsymbol{F})$$

which has the following properties:

i) *$\tilde{\rho}|_{\mathrm{Gal}\,(\bar{\boldsymbol{Q}}/K)}$ is unramified outside the set of primes of K lying above p.*

ii) *$\tilde{\rho}$ is reducible over $\boldsymbol{F}$ in such a way that $\tilde{\rho}$ is isomorphic to a representation of the form*

$$\begin{pmatrix} 1 & * \\ 0 & \tilde{\phi}^{-1}\end{pmatrix}.$$

iii) *$\tilde{\rho}$ is not diagonalizable.*

iv) *Let D be a decomposition group for p in* Gal $(\bar{\boldsymbol{Q}}/\boldsymbol{Q})$. *Then the order of $\tilde{\rho}(D)$ is prime to p.*

This theorem is proved by the same argument as in [5]. We note the following points. (This theorem is known to specialists.)

1) Let X be an abelian variety attached to f (cf. [7, Theorem 7.14]). Then X has everywhere good reduction over the maximal real subfield K^+ of K since ε is primitive and pm is square free (cf. [2, Exemples 3.7, (iii)]).

2) Using the Tate module of X, we have a continuous representation of Gal $(\bar{\boldsymbol{Q}}/\boldsymbol{Q})$ over a certain local field. This representation is irreducible (cf. [6, Theorem (2.3)]).

3) Let E be the completion of K^+ at $\mathfrak{p}\cap K^+$. Then its absolute ramification index is $(p-1)/2$. Hence we can apply Proposition (4.3) and Theorem (4.4) of [5].

Using Theorem 3, we obtain the following

Theorem 4. *Suppose that there exists a cusp form f satisfying the conditions in Theorem 2. Then $e(\Phi)A\neq 0$.*

Now we obtain Theorem 1 by using Remark 3 in §1, Theorems 2 and 4.

§4. We have an application of Theorem 1. For $\phi\in\hat{G}^-$, let L_ϕ be the field generated by the values of ϕ over $\boldsymbol{Q}_p$, $\mathfrak{O}_\phi$ be its integer ring and $\mathfrak{p}_\phi$ be its maximal ideal. For $\phi\in\hat{G}^-$, put $n(\phi)=\mathrm{ord}_{\mathfrak{p}_\phi} B_1(\phi^{-1})$ if $\phi\neq\omega$

and $n(\omega)=0$.

Proposition. *Under the same assumption as Theorem* 1, *if* $n(\phi)\leqq 1$ *for each* $\phi\in\hat{G}^-$, *then* $e(\Phi)A$ *is isomorphic to* $\mathfrak{O}_\phi/\mathfrak{p}_\phi^{n(\phi)}$ *for each* $\phi\in\hat{G}^-$.

This proposition is proved by using Theorem 1, the class number formula and the Stickelberger relations (cf. [3]).

Acknowledgements. The author would like to thank Profs. M. Koike and K. A. Ribet for their comments on Theorem 2.

References

[1] J. Coates and S. Lichtenbaum: On l-adic zeta functions. Ann. of Math., **98**, 498–550 (1973).
[2] P. Deligne and M. Rapoport: Les schémas de modules de courbes ellipitiques. Lect. Notes in Math., vol. 349, pp. 143–316, Berlin-Heidelberg-New York, Springer (1973).
[3] G. Gras: Classes d'idéaux des corps abéliens et nombres de Bernoulli généralisés. Ann. Inst. Fourier, Grenoble, **27**, 1–66 (1977).
[4] T. Metsänkylä: Class numbers and μ-invariants of cyclotomic fields. Proc. Amer. Math. Soc., **43**, 299–300 (1974).
[5] K. A. Ribet: A modular construction of unramified p-extensions of $\boldsymbol{Q}(\mu_p)$. Invent. math., **34**, 151–162 (1976).
[6] ——: Galois representations attached to eigenforms with Nebentypus. Lect. Notes in Math., vol. 601, pp. 17–52, Berlin-Heidelberg-New York, Springer (1977).
[7] G. Shimura: Introduction to the arithmetic theory of automorphic functions. Publ. Math. Soc. Japan, **11**, Iwanami Shoten-Princeton University Press, Tokyo-Princeton (1971).
[8] M. Koike: A Note on Modular Forms mod p. Proc. Japan Acad., **55**A(8), 313–315 (1979).