COMPOSITIO MATHEMATICA

MASATO KURIHARA

Some remarks on conjectures about cyclotomic fields and K-groups of Z

Compositio Mathematica, tome 81, nº 2 (1992), p. 223-236

<http://www.numdam.org/item?id=CM_1992__81_2_223_0>

© Foundation Compositio Mathematica, 1992, tous droits réservés.

L'accès aux archives de la revue « Compositio Mathematica » (http://http://www.compositio.nl/) implique l'accord avec les conditions générales d'utilisation (http://www.numdam.org/conditions). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques
http://www.numdam.org/

Compositio Mathematica **81**: 223–236, 1992.
© 1992 *Kluwer Academic Publishers. Printed in the Netherlands.*

Some remarks on conjectures about cyclotomic fields and K-groups of $\mathbf{Z}$

MASATO KURIHARA

Department of Mathematics, Tokyo Metropolitan University, Fukazawa, Setagaya, Tokyo, 158, Japan

Received 14 September 1990; accepted 23 April 1991

0. Introduction

In this article, we study the relations between some conjectures about the cyclotomic fields, and the K-groups and the etale cohomology groups of $\mathbf{Z}$.

For an odd prime number p, let $\mathbf{Q}(\mu_p)$ be the field of primitive pth roots of unity, and $\Delta = \mathrm{Gal}(\mathbf{Q}(\mu_p)/\mathbf{Q})$ its Galois group. We denote by $\omega \in \Delta^\wedge = \mathrm{Hom}(\Delta, \mathbf{Z}_p^\times)$ the Teichmüller character. We decompose the p-Sylow subgroup A of the ideal class group of $\mathbf{Q}(\mu_p)$ into the ω^k-eigenspaces $A^{[k]}$ for characters $\omega^k \in \Delta^\wedge$

$$A \simeq \bigoplus_{0 \leqslant k < p-1} A^{[k]}.$$

It is conjectured that (i) $A^{[i]}$ for even i is zero (by Kummer–Vandiver) and that (ii) $A^{[j]}$ for odd j is cyclic (by Iwasawa cf. [9], and (ii) is also a consequence of (i)). It can be shown that (i) is equivalent to $H^2_{\mathrm{et}}(\mathbf{Z}[1/p], \mathbf{Z}_p(r)) = 0$ for odd r, and (ii) is to the cyclicity of $H^2_{\mathrm{et}}(\mathbf{Z}[1/p], \mathbf{Z}_p(r))$ for even r, respectively (cf. Corollary 1.5). Let $K_*(\mathbf{Z})$ be Quillen's K-groups of $\mathbf{Z}$. In this article, we show that $K_{2r-2}(\mathbf{Z})$ contains *a direct summand* isomorphic to $H^2(\mathbf{Z}[1/p], \mathbf{Z}_p(r))$ for $r \geqslant 2$ (Proposition 2.1). So, we know that $K_{4n}(\mathbf{Z})\{p\} = 0$ implies (i) and that the cyclicity of $K_{4n+2}(\mathbf{Z})\{p\}$ implies (ii). Here, $K_*(\mathbf{Z})\{p\}$ means the p-Sylow subgroup of the K-group of $\mathbf{Z}$. More precisely, see Section 3. For example, by $K_4(\mathbf{Z}) = 0$ modulo 2 and 3 torsions (Lee and Szczarba's theorem [11]), we have $A^{[p-3]} = 0$, and the cyclicity of $A^{[3]}$ by duality. We shall give in Section 4 some results (on the Jacobian of Fermat curves, on the Galois representation to the pro-p braid group in Ihara [7], and on the first case of Fermat's problem) which are deduced from $A^{[p-3]} = 0$ and the cyclicity of $A^{[3]}$.

As an appendix, in Section 5 we show that the notion of Euler system due to Kolyvagin works well for the study of $H^2(\mathbf{Z}[1/p], \mathbf{Z}_p(r))$ for odd $r \geqslant 3$, by using the cyclotomic elements of Deligne–Soulé [4], [16], [17].

Notation

For an abelian group A and an integer n, the kernel (resp. cokernel) of the multiplication by n is denoted by ${}_nA$ (resp. A/n), and the torsion subgroup of A is denoted by A_{tors}. For a number field F, its integer ring is denoted by O_F. For a ring R and a sheaf M on $(\operatorname{Spec} R)_{\mathrm{et}}$, the etale cohomology group $H^*_{\mathrm{et}}(\operatorname{Spec} R, M)$ is written as $H^*(R, M)$. For an etale sheaf M and an integer r, $M(r)$ means the Tate twist. For a prime number p, $\operatorname{ord}_p: \mathbf{Q}^\times \to \mathbf{Z}$ is the normalized additive valuation at p.

1. Ideal class groups and cohomology groups

Let p be an odd prime number and μ_p the group of pth roots of unity. In this article, we always assume that F is a number field such that there is only one prime of $F(\mu_p)$ over p. A typical and principal example is $F = \mathbf{Q}$.

We are interested in the cohomology groups

$$H^2(O_F[1/p], \mathbf{Z}_p(r)) = \varprojlim H^2(O_F, \mathbf{Z}/p^n(r)) \quad \text{for } r \in \mathbf{Z}$$

because of the relation with ideal class groups, which will be shown in this section.

PROPOSITION 1.1. *Let F be as above. The sequence*

$$H^1(F, \mathbf{Z}/p^n(r)) \to \bigoplus_{v \nmid p} H^0(\kappa(v), \mathbf{Z}/p^n(r-1)) \to H^2(O_F[1/p], \mathbf{Z}/p^n(r)) \to 0$$

which comes from the localization sequence of the etale cohomology groups, is exact for all $n \geqslant 1$ and $r \in \mathbf{Z}$. Here, O_F is the integer ring of F and $\kappa(v)$ is the residue field at v.

Let $\Delta = \operatorname{Gal}(F(\mu_p)/F)$ and ω be a $\mathbf{Z}_p$-valued character of Δ such that $\zeta^{\omega(\sigma)} = \zeta^\sigma$ for all $\sigma \in \Delta$ and all $\zeta \in \mu_p$. Let A_F be the p-Sylow subgroup of the group $H^1(O_F[\mu_p, 1/p], \mathbf{G}_m) \simeq (\oplus_{v \nmid p} \mathbf{Z})/F^\times$. For an integer $k \in \mathbf{Z}$ we denote by $A_F^{[k]}$ the ω^k-eigenspace of A_F. Since $d = [F(\mu_p): F]$ is prime to p, we have

$$A_F \simeq \bigoplus_{0 \leqslant k < d} A_F^{[k]}.$$

LEMMA 1.2. $A_F^{[k]}/p \simeq H^2(O_F[1/p], \mathbf{Z}/p(1-k))$.

Put $R = O_F[\mu_p, 1/p]$. Since there is only one prime over p of $F(\mu_p)$,

$$\operatorname{Br}(R) = H^2(R, \mathbf{G}_m) = \operatorname{Ker}(\operatorname{Br}(F(\mu_p)) \to \bigoplus_{v \nmid p} \operatorname{Br}(F(\mu_p)_v)) = 0.$$

Hence, by Kummer sequence, we have

$$A_F/p \simeq H^2(R, \mathbf{Z}/p(1)). \tag{1}$$

Since $d=\#\Delta$ is prime to p, $H^q(R, \mathbf{Z}/p(r))^{\Delta}=H^q(O_F[1/p], \mathbf{Z}/p(r))$ for all q. After tensoring $\mathbf{Z}/p(-k)$, taking Δ-invariants of both sides of the above isomorphism (1), we obtain Lemma 1.2.

We shall prove Proposition 1.1. The problem is only the surjectivity of the last map

$$\phi_n\colon \bigoplus_{v\nmid p} H^0(\kappa(v), \mathbf{Z}/p^n(r-1)) \to H^2(O_F[1/p], \mathbf{Z}/p^n(r)).$$

Let $M/F(\mu_p)$ be the maximal unramified abelian extension. Since $M/F(\mu_p)$ and $F(\mu_{p^n})/F(\mu_p)$ are linearly disjoint, the natural map $\bigoplus_{\#\kappa(v)\equiv 1(\mathrm{mod}\, p^n)} \mathbf{Z} \to A_F$ is surjective by Cĕbotarev density. Hence, by Lemma 1.2, the composite

$$\bigoplus_{v\nmid p} H^0(\kappa(v), \mathbf{Z}/p^n(r-1)) \to \bigoplus_{v\nmid p} H^0(\kappa(v), \mathbf{Z}/p(r-1)) \xrightarrow{\phi_1} H^2(O_F[1/p], \mathbf{Z}/p(r)) \tag{2}$$

is surjective. By the surjectivity of (2) and induction on n

$$\begin{tikzcd}
\bigoplus_{v\nmid p} H^0(\kappa(v), \mathbf{Z}/p^{n-1}(r-1)) \arrow[r] \arrow[d, "\phi_{n-1}"] & \bigoplus_{v\nmid p} H^0(\kappa(v), \mathbf{Z}/p^n(r-1)) \arrow[r] \arrow[d, "\phi_n"] & \bigoplus_{v\nmid p} H^0(\kappa(v), \mathbf{Z}/p(r-1)) \arrow[d, "\phi_1"] \\
H^2(O_F[1/p], \mathbf{Z}/p^{n-1}(r)) \arrow[r] & H^2(O_F[1/p], \mathbf{Z}/p^n(r)) \arrow[r] & H^2(O_F[1/p], \mathbf{Z}/p(r)),
\end{tikzcd}$$

we get the surjectivity of ϕ_n.

COROLLARY 1.3. *For $r \geqslant 2$, we have isomorphisms*

$$\begin{aligned} H^2(O_F[1/p], \mathbf{Z}_p(r)) &\simeq \mathrm{Ker}(H^2_{\mathrm{cont}}(F, \mathbf{Z}_p(r))_{\mathrm{tors}} \to \varprojlim H^2(F, \mathbf{Z}/p^n(r))) \\ &\simeq (\varprojlim{}^1 H^1(F, \mathbf{Z}/p^n(r)))_{\mathrm{tors}} \end{aligned}$$

where $H^*_{\mathrm{cont}}(F, \mathbf{Z}_p(r))$ is the continuous cochain cohomology.

Proof. By the localization sequences, we have a diagram of exact sequences

$$\begin{tikzcd}
 & 0 \arrow[d] & 0 \arrow[d] & & \\
0 \arrow[r] & H^1(O_F[1/p], \mathbf{Z}_p(r)) \otimes \mathbf{Q}_p/\mathbf{Z}_p \arrow[r] \arrow[d] & H^1(O_F[1/p], \mathbf{Q}_p/\mathbf{Z}_p(r)) \arrow[r] \arrow[d] & H^2(O_F[1/p], \mathbf{Z}_p(r)) \arrow[r] & 0 \\
0 \arrow[r] & H^1(F, \mathbf{Z}_p(r)) \otimes \mathbf{Q}_p/\mathbf{Z}_p \arrow[r] \arrow[d] & H^1(F, \mathbf{Q}_p/\mathbf{Z}_p(r)) \arrow[r] \arrow[d] & H^2_{\mathrm{cont}}(F, \mathbf{Z}_p(r))_{\mathrm{tors}} \arrow[r] & 0 \\
 & 0 & \to \bigoplus_{v\nmid p} H^0(\kappa(v), \mathbf{Q}_p/\mathbf{Z}_p(r-1)) \arrow[r] \arrow[d] & \bigoplus_{v\nmid p} H^1(\kappa(v), \mathbf{Z}_p(r-1)) \arrow[r] & 0 \\
 & & 0 & &
\end{tikzcd}$$

Here we use $H^2(O_F[1/p], \mathbf{Z}_p(r))$ is a torsion group [16]. Hence,

$$0 \to H^2(O_F[1/p], \mathbf{Z}_p(r)) \to H^2_{\mathrm{cont}}(F, \mathbf{Z}_p(r))_{\mathrm{tors}} \to \bigoplus_{v \nmid p} H^1(\kappa(v), \mathbf{Z}_p(r-1)) \to 0$$

is exact. On the other hand, Proposition 1.1 implies an isomorphism

$$H^2(F, \mathbf{Z}/p^n(r)) \simeq \bigoplus_{v \nmid p} H^1(\kappa(v), \mathbf{Z}/p^n(r-1))$$

by the localization sequence. Thus, we have

$$H^2(O_F[1/p], \mathbf{Z}_p(r)) \simeq \mathrm{Ker}(H^2_{\mathrm{cont}}(F, \mathbf{Z}_p(r))_{\mathrm{tors}} \to \varprojlim H^2(F, \mathbf{Z}/p^n(r))).$$

The second isomorphism is due to [19] Proposition (2.2).

REMARK 1.4. If F is totally real, as a consequence of Iwasawa's main conjecture proved by Wiles, we know

$$\mathrm{ord}_p \ \# H^2(O_F[1/p], \mathbf{Z}_p(r)) = \mathrm{ord}_p \zeta_F(1-r) + \mathrm{ord}_p \ \# H^1(O_F[1/p], \mathbf{Z}_p(r))$$

for even integers $r \geqslant 2$ where ζ_F is Dedekind's zeta function ([22] Th. 1.6).

A remark in the case $F = \mathbf{Q}$. Since the unique prime over p of $\mathbf{Q}(\mu_p)$ is principal,

$$H^1(\mathbf{Z}[\mu_p, 1/p], \mathbf{G}_m) = H^1(\mathbf{Z}[\mu_p], \mathbf{G}_m) = \mathrm{Pic}(\mathbf{Z}[\mu_p]).$$

So $A_{\mathbf{Q}}$ in Lemma 1.2 is the p-Sylow subgroup of the ideal class group of $\mathbf{Q}(\mu_p)$. We simply write $A^{[k]}$ for $A_{\mathbf{Q}}^{[k]}$, which is the ω^k-eigenspace of $A_{\mathbf{Q}} = \mathrm{Pic}(\mathbf{Z}[\mu_p]) \otimes \mathbf{Z}_p$. From Lemma 1.2, we easily obtain

COROLLARY 1.5. *For $r \geqslant 2$, $A^{[1-r]}$ is cyclic (resp. zero) if and only if $H^2(\mathbf{Z}[1/p], \mathbf{Z}_p(r))$ is cyclic (resp. zero).*

In fact, since $H^3(\mathbf{Z}[1/p], \mathbf{Z}_p(r)) = 0$, $H^2(\mathbf{Z}[1/p], \mathbf{Z}_p(r))/p = H^2(\mathbf{Z}[1/p], \mathbf{Z}/p(r))$. Using $H^2(\mathbf{Z}[1/p], \mathbf{Z}_p(r))$ is a finite group [16], we obtain this corollary from Lemma 1.2.

2. Relation with K-groups

Let $K_*(O_F)$ be the K-group of the integer ring of F, and for $r \geqslant 2$

$$\mathrm{ch}\colon K_{2r-2}(O_F) \to H^2(O_F[1/p], \mathbf{Z}_p(r))$$

be the Chern character which is defined as the composite of the natural maps

$K_{2r-2}(O_F)\to\varprojlim K_{2r-2}(O_F,\mathbf{Z}/p^n)\to\varprojlim K^{\text{et}}_{2r-2}(O_F[1/p],\mathbf{Z}/p^n)\simeq H^2(O_F[1/p],\mathbf{Z}_p(r))$ [5]. This is known to be surjective by [5] and conjectured by Quillen to be bijective [12] p. 495.

PROPOSITION 2.1. *Let F be a number field satisfying the condition in Section* 1 *and r be an integer $\geqslant 2$. Then,* $\text{ch}: K_{2r-2}(O_F)\to H^2(O_F[1/p],\mathbf{Z}_p(r))$ *is split surjective.*

Consider the localization sequence of the etale K-theory

$$K^{\text{et}}_{2r-1}(F,\mathbf{Z}/p^n)\longrightarrow\bigoplus_{v\nmid p}K^{\text{et}}_{2r-2}(\kappa(v),\mathbf{Z}/p^n)\xrightarrow{\varphi_n}K^{\text{et}}_{2r-2}(O_F[1/p],\mathbf{Z}/p^n).$$

Since

$$K^{\text{et}}_{2r-1}(F,\mathbf{Z}/p^n)\simeq H^1(F,\mathbf{Z}/p^n(r))$$

and

$$K^{\text{et}}_{2r-2}(\kappa(v),\mathbf{Z}/p^n)\simeq H^0(\kappa(v),\mathbf{Z}/p^n(r-1)),$$

by Proposition 1.1 the image of φ_n is $H^2(O_F[1/p],\mathbf{Z}/p^n(r))$ in $K^{\text{et}}_{2r-2}(O_F[1/p],\mathbf{Z}/p^n)$ (cf. [5] Prop. 5.2). Hence, the canonical homomorphisms from K-theory to etale K-theory and the localization sequences give the diagram of exact sequences

$$\begin{tikzcd}
K_{2r-1}(F,\mathbf{Z}/p^n) \arrow[r] \arrow[d, "\alpha_n"] & \bigoplus_{v\nmid p}K_{2r-2}(\kappa(v),\mathbf{Z}/p^n) \arrow[r, "\delta_n"] \arrow[d, "\beta_n"] & K_{2r-2}(O_F[1/p],\mathbf{Z}/p^n) \arrow[d, "\gamma_n"] & \\
H^1(F,\mathbf{Z}/p^n(r)) \arrow[r] & \bigoplus_{v\nmid p}H^0(\kappa(v),\mathbf{Z}/p^n(r-1)) \arrow[r, "\varphi_n"] & H^2(O_F[1/p],\mathbf{Z}/p^n(r)) \arrow[r] & 0.
\end{tikzcd}$$

By [5] section 8, α_n is surjective and β_n is bijective. Hence, γ_n induces an isomorphism between the image of δ_n and $H^2(O_F[1/p],\mathbf{Z}/p^n(r))$. This also shows that γ_n is split surjective. Taking the projective limits

$$\begin{aligned}\varprojlim \text{Image }\delta_n &\subset \varprojlim K_{2r-2}(O_F[1/p],\mathbf{Z}/p^n)=K_{2r-2}(O_F[1/p])\otimes\mathbf{Z}_p\\ &=K_{2r-2}(O_F)\otimes\mathbf{Z}_p\subset K_{2r-2}(O_F),\end{aligned}$$

$\text{ch}=\varprojlim\gamma_n$ induces an isomorphism between the direct summand $\varprojlim$ Image δ_n of $K_{2r-2}(O_F)$ and $H^2(O_F[1/p],\mathbf{Z}_p(r))$.

COROLLARY 2.2. *For $2\leqslant r<p$, the homology group*

$$H_{2r-2}(\text{GL}(O_F),\mathbf{Z})=H_{2r-2}(\text{GL}_{4r-4}(O_F),\mathbf{Z})\qquad(3)$$

contains a direct summand isomorphic to $H^2(O_F[1/p], \mathbf{Z}_p(r))$.

For $2 \leqslant r < p$, the Chern character coincides modulo $\mathbf{Z}_p^\times$ with the Chern class in [15], which is defined as a composite

$$K_{2r-2}(O_F) \otimes \mathbf{Z}_p \xrightarrow{Hu} H_{2r-2}(\mathrm{GL}(O_F), \mathbf{Z}_p) \longrightarrow H^2(O_F[1/p], \mathbf{Z}_p(r))$$

where Hu is the Hurewitz homomorphism. Hence,

$$H_{2r-2}(\mathrm{GL}(O_F), \mathbf{Z}_p) \to H^2(O_F[1/p], \mathbf{Z}_p(r))$$

is also split surjective. The isomorphism (3) is due to the stability by Suslin [18].

3. Conjectures about $K_q(\mathbf{Z})$ and the ideal class groups of cyclotomic fields

In the rest of the paper, we consider the case $F = \mathbf{Q}$.

Let $\zeta(s)$ be Riemann's zeta function. For a positive even integer k, we write

$$\zeta(1-k) = (-1)^{k/2} N_k/D_k,$$

where N_k, D_k are positive integers and $(N_k, D_k) = 1$. If we use the Bernoulli numbers, $(-1)^{k/2+1} B_k/k = N_k/D_k$. It is known that $D_k = \Pi p^{n_p+1}$ where p runs through prime numbers such that k is divisible by $p-1$, and $n_p = \mathrm{ord}_p(k)$. Prime divisors of N_k are irregular primes.

Concerning the structures of the K-groups $K_q(\mathbf{Z})$,

CONJECTURE 3.1. *$K_q(\mathbf{Z})_{\mathrm{tors}}$ is cyclic up to 2-torsion for all $q \geqslant 0$.*

More precisely,

CONJECTURE 3.2. *Up to 2-torsion groups, for $n \geqslant 0$,*

(1) $K_{4n}(\mathbf{Z}) = 0$ $(n \neq 0)$.
(2) $K_{4n+1}(\mathbf{Z}) \simeq \mathbf{Z}$.
(3) $K_{4n+2}(\mathbf{Z}) \simeq \mathbf{Z}/N_k$ *where* $k = 2n + 2$.
(4) $K_{4n+3}(\mathbf{Z}) \simeq \mathbf{Z}/D_k$ *where* $k = 2n + 2$.

REMARK 3.3. I heard from the referee that a more precise conjecture including 2-torsion subgroups, was given independently by S. A. Mitchell. We also remark that (2) and (4) are no other than Quillen's conjecture $K_{2r-1}(\mathbf{Z}) \otimes \mathbf{Z}_p \simeq H^1(\mathbf{Z}[1/p], \mathbf{Z}_p(r))$ for an odd prime p.

Conjecture 3.1 for $q = 4n+2$ and Conjecture 3.2 (3) are almost equivalent. Precisely, PROPOSITION 3.4. *Assume $n \geqslant 0$ and $p|N_{2n+2}$. If the p-Sylow subgroup of $K_{4n+2}(\mathbf{Z})$ is cyclic, it is isomorphic to $\mathbf{Z}_p/N_{2n+2}\mathbf{Z}_p$.*

Proof. Note that by Iwasawa's main conjecture, we have $\mathrm{ord}_p(\# H^2(\mathbf{Z}[1/p], \mathbf{Z}_p(2n+2))) = \mathrm{ord}_p(N_{2n+2})$ (cf. Remark 1.4). Hence, if $K_{4n+2}(\mathbf{Z}) \otimes \mathbf{Z}_p$ is cyclic, by Proposition 2.1 we must have $K_{4n+2}(\mathbf{Z}) \otimes \mathbf{Z}_p \simeq H^2(\mathbf{Z}[1/p], \mathbf{Z}_p(2n+2))) \simeq \mathbf{Z}_p/N_{2n+2}\mathbf{Z}_p$.

As in Section 1, we denote by $A^{[k]}$ the ω^k-eigenspace of the p-Sylow subgroup of the ideal class group of $\mathbf{Q}(\mu_p)$ (ω: Teichmüller character). It is easy to see that $A^{[0]} = A^{[1]} = 0$. Concerning $A^{[k]}$, there are famous conjectures.

CONJECTURE 3.5 (Kummer–Vandiver). *For an even integer i, $A^{[i]} = 0$.*

CONJECTURE 3.6. *For an odd integer j such that $j \not\equiv 1 (\mathrm{mod}\, p-1)$, $A^{[j]}$ is isomorphic to $\mathbf{Z}_p/L(0, \omega^{-j})\mathbf{Z}_p$ where $L(s, \omega^{-j})$ is Dirichlet's L-function.*

If these conjectures are true, the theory of the cyclotomic fields, for example, Iwasawa theory becomes very simple (cf. [9]). It is well known that Conjecture 3.5 for i implies Conjecture 3.6 for j such that $i + j \equiv 1 (\mathrm{mod}\, p-1)$. We shall give a proof of this fact using Tate–Poitou's duality. By Lemma 1.2, $A^{[i]} = 0$ implies $H^2(\mathbf{Z}[1/p], \mathbf{Z}/p(1-i)) = 0$. Hence,

$$H^1_c(\mathbf{Z}[1/p], \mathbf{Z}/p(i)) = \mathrm{Ker}(H^1(\mathbf{Z}[1/p], \mathbf{Z}/p(i)) \to H^1(\mathbf{Q}_p, \mathbf{Z}/p(i))) = 0$$

by Tate–Poitou's duality. Since $H^1(\mathbf{Q}_p, \mathbf{Z}/p(i)) \simeq \mathbf{Z}/p$, we have

$$\dim_{\mathbf{F}_p} H^1(\mathbf{Z}[1/p], \mathbf{Z}/p(i)) \leqslant 1.$$

So, considering the Euler–Poincaré characteristic, we get

$$\dim_{\mathbf{F}_p} H^2(\mathbf{Z}[1/p], \mathbf{Z}/p(i)) \leqslant 1.$$

This shows that $A^{[j]}$ is cyclic where $j = 1 - i$ again by Lemma 1.2. On the other hand, from Iwasawa's main conjecture proved by Mazur and Wiles, we know $\mathrm{ord}_p \# A^{[j]} = \mathrm{ord}_p L(0, \omega^{-j})$. Thus, $A^{[i]} = 0$ implies Conjecture 3.6 for $j = 1 - i$.

PROPOSITION 3.7. *Conjecture* 3.2 (1) *implies Conjectures* 3.5 *and* 3.6. *More precisely, Conjecture* 3.2 (1) *for n implies Conjecture* 3.5 *for $i \equiv -2n (\mathrm{mod}\, p-1)$ and Conjecture* 3.6 *for $j \equiv 1 + 2n (\mathrm{mod}\, p-1)$.*

In fact, if there are no p-torsions in $K_{4n}(\mathbf{Z})$, $H^2(\mathbf{Z}[1/p], \mathbf{Z}_p(2n+1)) = 0$ by Proposition 2.1. Hence, $A^{[-2n]} = 0$ by Corollary 1.5. By the duality explained above, we have the cyclicity of $A^{[1+2n]}$.

COROLLARY 3.8. *For an odd prime p, we have*

$$A^{[p-3]}=0, \quad A^{[3]} \simeq \mathbf{Z}_p/L(0,\omega^{-3})\mathbf{Z}_p, \quad \textit{and} \quad H^2(\mathbf{Z}[1/p],\mathbf{Z}_p(k)) \simeq \mathbf{Z}_p/N_k\mathbf{Z}_p$$

for $k \equiv p-3(\bmod p-1)$ *and* $k > 0$.

In fact, by [11], $K_4(\mathbf{Z})=0$ modulo 2 and 3-torsions. Now, we may assume $p \neq 3$ because 3 is a regular prime. For the last isomorphism, the cyclicity of $A^{[3]}$ implies that of $H^2(\mathbf{Z}[1/p],\mathbf{Z}_p(k))$ for $k \equiv p-3(\bmod p-1)$ and $k > 0$ by Corollary 1.5, and the order of $H^2(\mathbf{Z}[1/p],\mathbf{Z}_p(k))$ is known from Remark 1.4.

By the same method, we obtain

PROPOSITION 3.9. *Conjecture* 3.2 (3) *for n implies Conjecture* 3.6 *for* $j \equiv -1-2n(\bmod p-1)$.

REMARK 3.10. In order to prove Propositions 3.7, 3.8, 3.9, we only need Lemma 1.2 and the surjectivity of $K_{2r-2}(\mathbf{Z}) \to H^2(\mathbf{Z}[1/p],\mathbf{Z}/p(r))$ proved by Soulé [15], and we do not need Proposition 2.1.

REMARK 3.11. If we assume Quillen's conjecture

$$K_{2r-2}(\mathbf{Z}) \otimes \mathbf{Z}_p \simeq H^2(\mathbf{Z}[1/p],\mathbf{Z}_p(r)),$$

the converse is also true, namely Conjectures 3.5 and 3.6 imply Conjectures 3.2 (1) and (3).

REMARK 3.12. Let G_* be the stable homotopy groups of the spheres. Quillen showed that the image in $K_{4n+3}(\mathbf{Z})$ of the J-homomorphism

$$\pi_{4n+3}(O) \to G_{4n+3} \to K_{4n+3}(\mathbf{Z})$$

is a direct summand and cyclic of order D_k up to 2-torsion [13]. One could also notice that cyclic groups of order the numerator of Bernoulli numbers appear in the work of Adams on the J-group. If a subgroup of $K_{4n+2}(\mathbf{Z})$ of order N_{2n+2} was produced using geometric topology, this would probably be a cyclic group. Therefore, Quillen's conjecture would then imply Conjecture 3.2 (3) and Conjecture 3.6.

4. Applications

In this section, we describe several applications of Corollary 3.8.

(1) *Rational points of some abelian varieties.* Let p be an odd prime $\geqslant 5$ and ζ_p a primitive pth root of unity. For an integer a such that $1 \leqslant a \leqslant p-2$, let J_a be

the Jacobian variety of the curve $y^p = x^a(1-x)$. J_a has the complex multiplication by $\mathbf{Z}[\mu_p]$. Let $J_a[\pi^3]$ be the subgroup of π^3-division points of J_a where $\pi = 1-\zeta_p$. Greenberg showed that $J_a[\pi^3]$ is $\mathbf{Q}(\mu_p)$-rational ([6] Th. 1). By $A^{[p-3]}=0$ (Corollary 3.8) and [6] p. 359, we know that $J_a[\pi^3]$ is just $\mathbf{Q}(\mu_p)$-rational points of p-primary torsions.

PROPOSITION 4.1. *Let $J_a(\mathbf{Q}(\mu_p))_{p-\mathrm{tors}}$ be the subgroup of $J_a(\mathbf{Q}(\mu_p))$ whose points have p-primary torsions. Then, we have*

$$J_a(\mathbf{Q}(\mu_p))_{p-\mathrm{tors}} = J_a[\pi^3] \simeq (\mathbf{Z}/p)^{\oplus 3}.$$

This is generalized in Proposition 4.4 below.

(2) *Galois representation arising from* $\pi_1^{\text{pro-}p}(\mathbf{P}^1\backslash\{0, 1, \infty\})$. We shall briefly describe the theory of the representation of $G_{\mathbf{Q}} = \mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$ in [7]. (Concerning this theory, see also [4].) Let p be an odd prime. Put $X = \mathbf{P}^1\backslash\{0, 1, \infty\}$. Then, $G_{\mathbf{Q}}$ acts on $\pi_1(X)$ and on its pro-p completion $\pi_1^{\text{pro-}p}(X) \simeq \mathscr{F}$ by conjugation where $\mathscr{F}$ is the free pro-p group of rank 2. So, we have a representation $G_{\mathbf{Q}} \to \mathrm{Aut}\,\pi_1^{(p)}(X)/\mathrm{Int} = \mathrm{Out}\,\pi_1^{(p)} \simeq \mathrm{Out}\,\mathscr{F}$. Ihara defined the pro-$p$ braid group $\Phi = Br\ d_2^{(p)}$ ([7] p. 46) which is a subgroup of Out $\mathscr{F}$, and proved that the image of the above representation is in it. So we have a homomorphism

$$\varphi\colon G_{\mathbf{Q}} = \mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q}) \to \Phi = Br\ d_2^{(p)}.$$

We can define a natural filtration $(\Phi(m))_{m\geqslant 1}$ on Φ by using the lower central series of $\mathscr{F}$ ([7] p. 59). We know that φ induces a bijective $\mathrm{Gal}(\mathbf{Q}(\mu_{p^\infty})/\mathbf{Q}) \simeq \Phi/\Phi(1)$ and that $\Phi(1) = \Phi(2) = \Phi(3)$. By $A^{[p-3]} = 0$ (Corollary 3.8) and [7] Th. 6, we have

PROPOSITION 4.2. *The restriction of φ to $G_{\mathbf{Q}(\mu_{p^\infty})} = \mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q}(\mu_{p^\infty})) \to \Phi(3)$ induces a surjective $G_{\mathbf{Q}(\mu_{p^\infty})} \to \Phi(3)/\Phi(4) \simeq \mathbf{Z}_p$.*

REMARK 4.3. The above homomorphism $\mathrm{gr}^3\varphi\colon G_{\mathbf{Q}(\mu_{p^\infty})} \to \Phi(3)/\Phi(4)$ is unramified outside p, and $\Phi(3)/\Phi(4)$ is isomorphic to $\mathbf{Z}_p(3)$ as a $G_\infty = \mathrm{Gal}(\mathbf{Q}(\mu_{p^\infty})/\mathbf{Q})$-module. Hence, $\mathrm{gr}^3\varphi$ gives an element of

$$H^1(\mathbf{Z}[1/p, \mu_{p^\infty}], \mathbf{Z}_p(3))^{G_\infty} \simeq H^1(\mathbf{Z}[1/p], \mathbf{Z}_p(3)).$$

We know that $\mathrm{gr}^3\varphi$ in $H^1(\mathbf{Z}[1/p], \mathbf{Z}_p(3))$ coincides with the cyclotomic element of Deligne–Soulé $c(1)$ in Section 5 (4) modulo $\mathbf{Z}_p^\times$ ([8] Th. B, [3] Th. C). Hence, the surjectivity of $\mathrm{gr}^3\varphi$ corresponds to the fact that the cyclotomic element generates $H^1(\mathbf{Z}[1/p], \mathbf{Z}_p(3))$. The latter is also deduced from Proposition 5.1 below and $H^2(\mathbf{Z}[1/p], \mathbf{Z}_p(3)) = 0$.

The results in [6] are generalized in [7]. Let n be a positive integer, and a, b, c

be integers such that $0 < a, b, c \leqslant p^n$, $a+b+c \equiv 0 (\operatorname{mod} p^n)$, and at least one of a, b, c is prime to p. We denote by $X_n^{(a,b,c)}$ the curve $y^{p^n} = x^a(1-x)^b$. We define an abelian variety $A_n^{(a,b,c)}$ as a primitive part of the Jacobian of $X_n^{(a,b,c)}$ ([7] p. 76). Then, by Corollary 3.8 and [7] Th. 6, we have

PROPOSITION 4.4. *There is a* $(\zeta_{p^n}^a - 1)(\zeta_{p^n}^b - 1)(\zeta_{p^n}^c - 1)(\zeta_{p^n} - 1)$th *division point of* $A_n^{(a,b,c)}$ *which is not* $\mathbf{Q}(\mu_{p^\infty})$*-rational where* ζ_{p^n} *is a primitive* p^nth *root of unity.*

For the relation with Jacobi sums, see [7] Th. 6.

(3) *The first case of Fermat's problem.* Let p be an odd prime number. Vandiver showed in [20] that if there is a nontrivial solution to $x^p + y^p = z^p$ by integers such that xyz is prime to p, then p^2 divides the Bernoulli number $B_{(p-4)p+1}$.

Let $L_p(s, \omega^{-2})$ be Kubota–Leopoldt's p-adic L function. Then Kummer's congruence (cf. [21] Th. 5.12) implies

$$\begin{aligned} L(0, \omega^{-3}) &\equiv L_p(0, \omega^{-2}) \equiv L_p(1 - ((p-4)p+1), \omega^{-2}) \\ &\equiv -B_{(p-4)p+1}/((p-4)p+1) \pmod{p^2}. \end{aligned}$$

So if p^2 divides $B_{(p-4)p+1}$, p^2 also divides $L(0, \omega^{-3})$. By Corollary 3.8, we have

PROPOSITION 4.5. *If the first case of Fermat's problem fails, then* $A^{[3]}$ *has an element of order* p^2.

Note that there are many examples of cyclotomic fields such that p^2 divides $\#$ Pic $\mathbf{Z}[\mu_p]$, but there is no known example such that Pic $\mathbf{Z}[\mu_p]$ has an element of order p^2. Recently, Iwasawa and Fujisaki gave a simple proof of Vandiver's result and generalized it (in preparation).

5. Cyclotomic elements as an Euler system

Let p be an odd prime number, and r an odd number $\geqslant 3$. In this section, we show that the cyclotomic elements of Deligne–Soulé in $H^1(\mathbf{Z}[1/p, \mu_L], \mathbf{Z}_p(r))$ [4], [16], [17], give an example of the Euler system by Kolyvagin [10]. In this case, the group corresponding to the Tate–Shafarevich group for an elliptic curve, is the group $H^2(\mathbf{Z}[1/p], \mathbf{Z}_p(r))$. As an application of the exact sequence in Prop. 1.1, using an argument of Kolyvagin [10], we show the finiteness of $H^2(\mathbf{Z}[1/p], \mathbf{Z}_p(r))$ (this was already known by using Borel's calculation of K-groups [15], [17]), and evaluate its order (this was also known by using Iwasawa's main conjecture [2] Section 6).

Let $(\zeta_{p^n}) \in \mathbf{Z}_p(1) = \varprojlim \mu_{p^n}$ be a projective system of a primitive p^nth root of unity. For an integer L prime to p and $\eta \in \mu_L$, we define η_n by the image in

$H^1(\mathbf{Z}[1/p, \eta, \mu_{p^n}], \mathbf{Z}/p^n(r))$ of

$$(1 - \zeta_{p^n}\eta^{1/p^n}) \otimes (\zeta_{p^n})^{\otimes(r-1)} \in (\mathbf{Z}[1/p, \eta, \mu_{p^n}]^\times/p^n) \otimes \mu_{p^n}^{\otimes(r-1)}.$$

Further, we define Deligne–Soulé's cyclotomic element by

$$\begin{aligned} c(\eta) &= \varprojlim_n \operatorname{Cor}_{\mathbf{Z}[1/p,\eta,\mu_{p^n}]/\mathbf{Z}[1/p,\eta]}(\eta_n) \in \varprojlim H^1(\mathbf{Z}[1/p, \eta], \mathbf{Z}/p^n(r)) \\ &= H^1(\mathbf{Z}[1/p, \eta], \mathbf{Z}_p(r)), \end{aligned} \tag{4}$$

where

$$\operatorname{Cor}_{\mathbf{Z}[1/p,\eta,\mu_{p^n}]/\mathbf{Z}[1/p,\eta]}: H^1(\mathbf{Z}[1/p, \eta, \mu_{p^n}], \mathbf{Z}/p^n(r)) \to H^1(\mathbf{Z}[1/p, \eta], \mathbf{Z}/p^n(r))$$

is the corestriction map.

Let C be the subgroup of $H^1(\mathbf{Z}[1/p], \mathbf{Z}_p(r))$ (topologically) generated by $c(1)$. By [1], $c(1)$ comes from the cyclotomic element of Beilinson in the K-group under the Chern class. Since the Chern class is injective modulo torsion [16] and the element of Beilinson is not zero in $K_{2r-1}(\mathbf{Z}) \otimes \mathbf{Q}$, we have $c(1) \neq 0$. This fact can be also proved by using Iwasawa's main conjecture [17]. Notice that $H^1(\mathbf{Z}[1/p], \mathbf{Z}_p(r))$ is a free $\mathbf{Z}_p$-module of rank 1. In fact, by [16] its rank is equal to 1. Further, since r is odd, $H^0(\mathbf{Z}[1/p], \mathbf{Z}/p(r)) = 0$. This implies $H^1(\mathbf{Z}[1/p], \mathbf{Z}_p(r))$ is torsion free. Therefore, $H^1(\mathbf{Z}[1/p], \mathbf{Z}_p(r)) \simeq \mathbf{Z}_p$, and $c(1) \neq 0$ implies that C is a subgroup of finite index.

PROPOSITION 5.1. *For an odd number $r \geqslant 3$, $H^2(\mathbf{Z}[1/p], \mathbf{Z}_p(r))$ is finite, and we have*

$$\# H^2(\mathbf{Z}[1/p], \mathbf{Z}_p(r)) \leqslant \#(H^1(\mathbf{Z}[1/p], \mathbf{Z}_p(r))/C).$$

REMARK 5.2. This was already proved in [2] (6.8) and (6.9). (The above inequality is really an equality.) We give here another proof following the argument of Kolyvagin. (We do not use Iwasawa's main conjecture for the proof.)

By definition, $c(\eta)$ has good properties like a system of cyclotomic units in [10] and [14]. For example, let $\eta \in \mu_L$, l a prime not dividing pL, ζ_l a primitive lth root of unity, and Frob_l the Frobenius substitution in $\operatorname{Gal}(\mathbf{Q}(\eta)/\mathbf{Q})$. Then, $\operatorname{Cor}_{\mathbf{Z}[1/p,\eta,\mu_l]/\mathbf{Z}[1/p,\eta]}(c(\zeta_l\eta)) = (l^{1-r}\operatorname{Frob}_l - 1)c(\eta)$. From now on, we follow the argument in [14].

Put

$$e = \operatorname{ord}_p \#(H^1(\mathbf{Z}[1/p], \mathbf{Z}_p(r))/C).$$

We fix an integer n such that $n > e$. Let P be the set of prime numbers l such that $l \equiv 1 (\bmod p^n)$, and $\mathscr{L}$ the set of positive squarefree integers whose prime divisors are in P. We suppose that 1 is also in $\mathscr{L}$. In the following, we consider only $c(L)$ for $L \in \mathscr{L}$.

We denote by G_L the Galois group of the extension $\mathbf{Q}(\mu_L)/\mathbf{Q}$ for $L \in \mathscr{L}$. For a prime number $l \in \mathscr{L}$, take a generator σ_l of G_l, and put $D_l = \Sigma_{i=1}^{l-2} i\sigma_l^i \in \mathbf{Z}[G_l]$, and $D_L = \Pi_{l|L} D_l \in \mathbf{Z}[G_L]$. Further, take a primitive lth root of unity ζ_l and put $\zeta_L = \Pi_{l|L} \zeta_l$. We can consider $D_L(c(\zeta_L)) \bmod p^n$ as an element of $H^1(\mathbf{Z}[1/pL], \mathbf{Z}/p^n(r))$ as follows. For a cyclotomic field K, we denote by K^+ the maximal real subfield. Let $N: \mathbf{Q}(\mu_{p^nL})^\times \to (\mathbf{Q}(\mu_{p^nL})^+)^\times$ be the norm map. By [14] Lemma 2.1, $D_L N(1 - \zeta_{p^n}\zeta_L^{1/p^n}) \bmod p^n$ in $(\mathbf{Q}(\mu_{p^nL})^+)^\times/p^n$ is in

$$((\mathbf{Q}(\mu_{p^nL})^+)^\times/p^n)^{G_L} = H^1(\mathbf{Q}(\mu_{p^nL})^+, \mathbf{Z}/p^n(1))^{G_L}$$

$$= H^1(\mathbf{Q}(\mu_{p^n})^+, \mathbf{Z}/p^n(1)) = (\mathbf{Q}(\mu_{p^n})^+)^\times/p^n.$$

So, one can write

$$D_L N(1 - \zeta_{p^n}\zeta_L^{1/p^n}) \bmod p^n = \varepsilon(L) \bmod p^n \quad \text{for some } \varepsilon(L) \in (\mathbf{Q}(\mu_{p^n})^+)^\times.$$

We define

$$\kappa(L) = \mathrm{Cor}_{\mathbf{Q}(\mu_{p^n})^+/\mathbf{Q}}(\varepsilon(L) \otimes \zeta_{p^n}^{\otimes(r-1)}) \in H^1(\mathbf{Q}, \mathbf{Z}/p^n(r)).$$

Notice that $\kappa(L)$ is equal to $D_L c(L)$ in H^1 $(\mathbf{Q}(\mu_L), \mathbf{Z}/p^n(r))$.

For any $\mathbf{Z}_p$-module X, we define a function v on X as follows. For $x \in X$, $v(x)$ is the maximal integer n such that $x = p^n y$ for some $y \in X$. For example, for $\mathbf{Z}_p$, v is the usual additive valuation ord_p.

For a prime number $l \neq p$, let

$$\partial_l: H^1(\mathbf{Q}, \mathbf{Z}/p^n(r)) \to H^0(\mathbf{F}_l, \mathbf{Z}/p^n(r-1))$$

be the homomorphism which comes from the localization sequence. The following is a consequence of Prop. 2.4 in [14].

LEMMA 5.3. (i) *If $L \in \mathscr{L}$ and l does not divide Lp, $\partial_l(\kappa(L)) = 0$.*

(ii) *If $Ll \in \mathscr{L}$, then we have*

$$v(\partial_l \kappa(Ll)) = v(\psi_l \kappa(L)),$$

where

$$\psi_l: H^1(\mathbf{Z}[1/pL], \mathbf{Z}/p^n(r)) \to H^1(\mathbf{F}_l, \mathbf{Z}/p^n(r))$$

is the canonical homomorphism. (*Note that* $\kappa(L) \in H^1(\mathbf{Z}[1/pL], \mathbf{Z}/p^n(r))$ *by* (i).)

Using this lemma and Proposition 1.1, we shall show Proposition 5.1 (cf. Th. 4.1 in [14]). Suppose $H^2(\mathbf{Z}[1/p], \mathbf{Z}/p^n(r)) \simeq \oplus_{1 \leqslant i \leqslant a} A_i$ where A_i's are cyclic. For a prime number $l \in P$, we denote by u_l the image in $H^2(\mathbf{Z}[1/p], \mathbf{Z}/p^n(r))$ of $\zeta_{p^n}^{\otimes(r-1)}$ under the homomorphism

$$H^0(\mathbf{F}_l, \mathbf{Z}/p^n(r-1)) \to H^2(\mathbf{Z}[1/p], \mathbf{Z}/p^n(r))$$

which comes from the localization sequence. We can choose inductively prime numbers $l_1, \dots, l_a$ such that (i) u_{l_i} is a generator of A_i, (ii) $l_i \in P$, and that (iii) $v(\psi_{l_i}\kappa(\Pi_{1 \leqslant j \leqslant i-1} l_j)) = v(\kappa(\Pi_{1 \leqslant j \leqslant i-1} l_j))$ by Cĕbotarev density theorem (cf. Th. 3.1 in [14]). Put $L_i = \Pi_{1 \leqslant j \leqslant i} l_j$, $L_0 = 1$, and $e_i = v(\kappa(L_i))$. Since $H^1(\mathbf{Z}[1/p], \mathbf{Z}_p(r))$ is a free $\mathbf{Z}_p$-module of rank 1, we have $e_0 = v(\kappa(1)) = v(c(1)) = e$.

Consider the exact sequence in Proposition 1.1

$$H^1(\mathbf{Q}, \mathbf{Z}/p^n(r)) \xrightarrow{\oplus \partial_v} \bigoplus_{v \nmid p} H^0(\kappa(v), \mathbf{Z}/p^n(r-1)) \to H^2(\mathbf{Z}[1/p], \mathbf{Z}/p^n(r)) \to 0.$$

By Lemma 5.3 and the property (iii),

$$v(\partial_{l_i}\kappa(L_i)) = v(\psi_{l_i}\kappa(L_{i-1})) = v(\kappa(L_{i-1})) = e_{i-1}.$$

Since $e_i = v(\kappa(L_i)) \leqslant v(\partial_{l_i}\kappa(L_i))$, we have $e_{i-1} \geqslant e_i$. By the definition of v, there is an element $w(L_i) \in H^1(\mathbf{Z}[1/pL_i], \mathbf{Z}/p^n(r))$ such that $\kappa(L_i) = p^{e_i} w(L_i)$. We have

$$v(\partial_{l_i} w(L_i)) = e_{i-1} - e_i$$

and $v(\partial_l w(L_i)) = 0$ for a prime l not dividing pL_i. Hence, by the property (i), we have

$$p^{e_{i-1} - e_i} u_{l_i} = 0 \quad \text{in } H^2(\mathbf{Z}[1/p], \mathbf{Z}/p^n(r)) \Big/ \bigoplus_{j=1}^{i-1} A_j.$$

This implies $e = e_0 \geqslant \Sigma_{i=1}^{a} (e_{i-1} - e_i) \geqslant \mathrm{ord}_p \, \# H^2(\mathbf{Z}[1/p], \mathbf{Z}/p^n(r))$. Hence, we have $p^e \geqslant \# H^2(\mathbf{Z}[1/p], \mathbf{Z}_p(r))$.

Acknowledgements

I would like to thank Prof. K. Iwasawa, who encouraged me to write this article. I discussed almost everything in this article with Prof. K. Kato. I would like to thank him very much for the discussions. I also express my hearty thanks to Prof. C. Soulé for his interest and some useful advice.