K. KATO
KODAI MATH. J.
22 (1999), 313–372

EULER SYSTEMS, IWASAWA THEORY, AND SELMER GROUPS

KAZUYA KATO*)

Introduction

Kolyvagin discovered the method of Euler system, and used it to analyze ideal class groups of certain cyclotomic fields and Selmer groups of elliptic curves. Rubin used the method of Euler system to obtain a new proof of Iwasawa main conjecture and a proof of the main conjecture for imaginary quadratic fields ([Ko_1], [Ko_2], [Ru_1], [Ru_2]). It is vaguely believed that once a nice Euler system is discovered, we can analyze certain étale cohomology groups and "Selmer groups" which are generalizations of ideal class groups and of Selmer groups of elliptic curves. This paper is an attempt to prove the truth of this belief. In this paper, we show that once a nice Euler system of a p-adic representation of $\mathrm{Gal}(\bar{\boldsymbol{Q}}/\boldsymbol{Q})$ is given (see Proposition 1.1 for the meaning of "an Euler system for a p-adic representation of $\mathrm{Gal}(\bar{\boldsymbol{Q}}/\boldsymbol{Q})$"), then we can prove finiteness theorems for the second étale cohomology $H^2_{\text{ét}}$ (Theorem 13.3) and for the Selmer group (Theorem 13.2) of the Galois representation, and can prove a part of an analogue of Iwasawa main conjecture (Theorem 0.8) of the Galois representation.

During I was preparing this paper, I leaned that similar results were obtained also by B. Perrin-Riou and by K. Rubin, independently ([Pe], [Ru_4]). The results of this paper will be used in [Ka_2] to develop the Iwasawa theory of elliptic cusp forms and Iwasawa theory of elliptic curves without complex multiplication. Results of this paper on $H^2_{\text{ét}}$ and Selmer groups are obtained under the assumption that we are given a nice Euler system, and how to find an Euler system is a difficult problem. In [Ka_2], we actually find nice Euler systems for two dimensional Galois representations associated to elliptic cusp forms. These Euler systems come from Beilinson's elements in K_2 of modular curves ([Be]).

I thank Prof. V. A. Kolyvagin for encouragement. I appreciate the hospitality of Institute for Advanced Study at which some part of this paper was written.

§0. Main result

In this §0, we fix the meaning of "an Euler system for p-adic representation of $\mathrm{Gal}(\bar{\boldsymbol{Q}}/\boldsymbol{Q})$" (cf. 0.1) in our sense, and state the main result Theorem 0.8 of this

*) Partially supported by Sloan Foundation
Received June 17, 1998; revised April 22, 1999.

paper. The well known Euler system of cyclotomic units is reviewed in Examples 0.2, 0.5.1, 0.6.1, Remark 0.8.1, and the reader will see how our Euler systems, if discovered, generalize this example.

0.1. Let p be a prime number, we use the following notation

F a finite extension of $\boldsymbol{Q}_p$,
O_F the integer ring of F,
$\bar{\boldsymbol{Q}}$ an algebraic closure of $\boldsymbol{Q}$,
T a free O_F-module of finite rank endowed with a continuous O_F-linear action of $\mathrm{Gal}(\bar{\boldsymbol{Q}}/\boldsymbol{Q})$.

Let $N \geq 1$ be a multiple of p, and assume that the action of $\mathrm{Gal}(\bar{\boldsymbol{Q}}/\boldsymbol{Q})$ on T is unramified at any prime number which does not divide N. Let $N' \geq 1$ be an integer which is prime to N.

By an *Euler system* for (F, T, N, N') (or simply, an Euler system for T), we mean a system of elements

$$z_m \in H^1\left(\boldsymbol{Z}\left[\zeta_m, \frac{1}{N}\right], T\right)$$

(ζ_m denotes a primitive m-th root of 1 in $\bar{\boldsymbol{Q}}$) defined for any integer $m \geq 1$ such that $N|m$ and $(m, N') = 1$, satisfying the conditions (0.1.1) below. Here for a finite extension K of $\boldsymbol{Q}$ with integer ring O_K,

$$H^q\left(O_K\left[\frac{1}{N}\right], T\right) \underset{\text{def}}{=} \varprojlim_n H^q\left(O_K\left[\frac{1}{N}\right], T/p^nT\right) \quad (q \in \boldsymbol{Z})$$

denotes the étale cohomology. (It is known that each $H^q(O_K[1/N], T/p^nT)$ is a finite group and $H^q(O_K[1/N], T)$ is a finitely generated O_F-module.)

For a prime number l which does not divide N, let

$$P_l(t) = \det_{O_F}(1 - \varphi_l t; T \to T) \in O_F[t]$$

where φ_l denotes the action of the arithmetic Frobenius substitution of l on T (which is determined up to conjugacy but $P_l(t)$ is well defined). (So, $P_l(t)^{-1}$ is the congruence zeta function of restriction to $\mathrm{Spec}(F_l)_{\text{ét}}$ of the dual O_F-sheaf $T^* = \mathrm{Hom}_{O_F}(T, O_F)$ of the O_F-sheaf T on $\mathrm{Spec}(\boldsymbol{Z}[1/N])_{\text{ét}}$. On the other hand, for such l and for an integer $m \geq 1$ which is not divisible by l, let $\sigma_{l,m}$ be the arithmetic Frobenius substitution in $\mathrm{Gal}(\boldsymbol{Q}(\zeta_m)/\boldsymbol{Q})$.

(0.1.1) *For any integer* $m \geq 1$ such that $N|m$ and $(m, N') = 1$, and for *a prime number* l which does not divide N', *the norm map*

$$H^1\left(\boldsymbol{Z}\left[\zeta_{ml}, \frac{1}{N}\right], T\right) \to H^1\left(\boldsymbol{Z}\left[\zeta_m, \frac{1}{N}\right], T\right)$$

sends

$$z_{ml} \text{ to } z_m \quad (\text{resp. to } P_l(l^{-1}\sigma_{l,m}^{-1}) \cdot z_m)$$

if l *divides* m (resp. l *does not divide* m).

Here $P_l(l^{-1}\sigma_{l,m}^{-1})$ is regarded as an element of the group ring $O_F[\mathrm{Gal}(\boldsymbol{Q}(\zeta_m)/\boldsymbol{Q})]$ acting naturally on $H^1(\boldsymbol{Z}[\zeta_m, 1/N], T)$.

Example 0.2 (Classical example). Let $F = \boldsymbol{Q}_p, T = \boldsymbol{Z}_p(1), N = p$, and $N' = 1$. We have

$$H^1\left(O_K\left[\frac{1}{p}\right], \boldsymbol{Z}_p(1)\right) \cong \left(O_K\left[\frac{1}{p}\right]\right)^{\times} \otimes_{\boldsymbol{Z}} \boldsymbol{Z}_p \tag{0.2.1}$$

if K is a finite extension of $\boldsymbol{Q}$, where $(\ )^{\times}$ is the multiplicative group of invertible elements. (This isomorphism comes from the connecting maps of the Kummer exact sequence

$$0 \to \boldsymbol{Z}/p^n\boldsymbol{Z}(1) \to \boldsymbol{G}_m \xrightarrow{p^n} \boldsymbol{G}_m \to 0 \quad (n \geq 0)$$

for etale topology.) Fix a primitive m-th root ζ_m of 1 in $\bar{Q}$ for each $m \geq 1$ satisfying $(\zeta_{mn})^n = \zeta_m$ for any $m, n \geq 1$. For a multiple m of p, let

$$z_m \in H^1\left(\boldsymbol{Z}\left[\zeta_m, \frac{1}{p}\right], \boldsymbol{Z}_p(1)\right)$$

be the image of $1 - \zeta_m \in (\boldsymbol{Z}[\zeta_m, 1/p])^{\times}$ under the isomorphism (0.2.1) for $K = \boldsymbol{Q}(\zeta_m)$. Then $(z_m)_m$ is an Euler system for $(\boldsymbol{Q}_p, \boldsymbol{Z}_p(1), p, 1)$ in the sense of 0.1. Indeed, (0.1.1) follows from

$$P_l(l^{-1}\sigma_{l,m}^{-1}) = 1 - \sigma_{l,m}^{-1} \quad (\text{since } P_l(t) = 1 - lt),$$

and from the fact that the norm map

$$\boldsymbol{Z}\left[\zeta_{ml}, \frac{1}{N}\right]^{\times} \to \boldsymbol{Z}\left[\zeta_m, \frac{1}{N}\right]^{\times}$$

sends $1 - \zeta_{ml}$ to $1 - \zeta_m$ if l divides m, and to

$$(1 - \zeta_m)(1 - \sigma_{l,m}^{-1}(\zeta_m))^{-1}$$

if l does not divide m.

Example 0.3. In the forthcoming paper [Ka_2], we will study an Euler system in the case T comes from an elliptic cusp form of weight ≥ 2 which is an eigen form for all Hecke operators.

0.4. Fix a divisor $d \geq 1$ of N. Let $\boldsymbol{Q}(\zeta_{dp^\infty}) = \bigcup_n \boldsymbol{Q}(\zeta_{dp^n})$ and let

$$\Lambda = O_F[[\mathrm{Gal}(\boldsymbol{Q}(\zeta_{dp^\infty})/\boldsymbol{Q})]]$$

where for a profinite group G and a ring R, $R[[G]]$ denotes $\varprojlim_H R[G/H]$ where H ranges over all open subgroups of G. Then if Δ denotes the finite subgroup

of $\mathrm{Gal}(\boldsymbol{Q}(\zeta_{dp^\infty})/\boldsymbol{Q})$ consisting of all elements of finite orders, Λ is isomorphic to the formal power series ring $O_F[\Delta][[t]]$ (t is an indeterminate). From this we have (cf. 10.4):

(0.4.1) Let $\mathfrak{p}$ be a prime ideal of Λ of height one which does not contain p. Then $\Lambda_{\mathfrak{p}}$ is a discrete valuation ring.

(0.4.2) If the order of Δ is prime to p (this happens for example, if $d = 1$ and $p \neq 2$), Λ is regular and $\Lambda_{\mathfrak{p}}$ is a discrete valuation ring for any prime ideal of Λ of height one.

0.5. Let

$$\boldsymbol{H}^q = \varprojlim_n H^q\left(\boldsymbol{Z}\left[\zeta_{dp^n}, \frac{1}{N}\right], T\right)$$

where the inverse limit is taken with respect to the norm maps. It is known that $\boldsymbol{H}^q = 0$ if $q \neq 1, 2$, and $\boldsymbol{H}^1$ and $\boldsymbol{H}^2$ are finitely generated Λ-modules. The Λ-module $\boldsymbol{H}^2$ is especially important and are the main subject of our study. It is closely related to ideal class groups of cyclotomic fields in the case of Example 0.2 (see Example 0.5.1 below) and to Selmer groups and Tate-Shafarevich groups of elliptic curves over $\boldsymbol{Q}$ in some cases of Example 0.3 ([Ka_3]). Let

$$\boldsymbol{H}_0^2 = \mathrm{Ker}\left(\boldsymbol{H}^2 \to \bigoplus_{l|N} \varprojlim_n H^2(\boldsymbol{Q}_l \otimes_{\boldsymbol{Q}} \boldsymbol{Q}(\zeta_{dp^n}), T)\right).$$

Example 0.5.1. Let $F = \boldsymbol{Q}_p$, $T = \boldsymbol{Z}_p(1)$, $N = p$ as in Remark 1.2, and let $d = 1$. Then

$$H^2\left(\boldsymbol{Z}\left[\zeta_{p^n}, \frac{1}{p}\right], \boldsymbol{Z}_p(1)\right) \cong \mathrm{Cl}(\boldsymbol{Q}(\zeta_{p^n})\{p\}$$

where $\mathrm{Cl}(\boldsymbol{Q}(\zeta_{p^n}))$ denotes the ideal class group of $\boldsymbol{Q}(\zeta_{p^n})$ and $\{p\}$ means the p-primary part. (The Kummer exact sequence in Example 0.2 gives

$$\mathrm{Cl}(\boldsymbol{Q}(\zeta_{p^n})) \cong H^1\left(\boldsymbol{Z}\left[\zeta_{p^n}, \frac{1}{p}\right], \boldsymbol{G}_m\right) \to H^2\left(\boldsymbol{Z}\left[\zeta_{p^n}, \frac{1}{p}\right], \boldsymbol{Z}/p^n\boldsymbol{Z}(1)\right)$$

and induces the above isomorphism.) In this case, we have

$$\boldsymbol{H}_0^2 = \boldsymbol{H}^2 = \varprojlim_n (\mathrm{Cl}(\boldsymbol{Q}(\zeta_{p^n}))\{p\})$$

where the limit is taken with respect to norm maps.

Remark 0.5.2. For a prime number l, the group $\varprojlim_n H^2(\boldsymbol{Q}_l \otimes \boldsymbol{Q}(\zeta_{dp^n}), T)$ is well understood. In fact, by local Tate duality ([S_2, Chapter II §5]),

$$\varprojlim_n H^2(\boldsymbol{Q}_l \otimes \boldsymbol{Q}(\zeta_{dp^n}), T) \cong \mathrm{Hom}(H^0(\boldsymbol{Q}_l \otimes \boldsymbol{Q}(\zeta_{dp^\infty}), T^*(1) \otimes \boldsymbol{Q}/\boldsymbol{Z}), \boldsymbol{Q}/\boldsymbol{Z})$$

where $T^* = \mathrm{Hom}_{O_F}(T, O_F)$ with the dual action of $\mathrm{Gal}(\bar{\boldsymbol{Q}}/\boldsymbol{Q})$.

$\boldsymbol{Q}_l \otimes \boldsymbol{Q}(\zeta_{dp^\infty})$ is a finite product of fields, and hence $H^0(\boldsymbol{Q}_l \otimes \boldsymbol{Q}(\zeta_{dp^\infty}), T^*(1) \otimes \boldsymbol{Q}/\boldsymbol{Z})$ is a subgroup of finite product of copies of $T^*(1) \otimes \boldsymbol{Q}/\boldsymbol{Z}$. By duality, this shows that $\varprojlim_n H^2(\boldsymbol{Q}_l \otimes \boldsymbol{Q}(\zeta_{dp^n}), T)$ is a finitely generated O_F-module, and is a torsion Λ-module (that is, it is killed by a non-zero-divisor of Λ).

0.6. We consider the following conditions on (F, T, N, N').

In the following, let m_F be the maximal ideal of O_F, and let $\boldsymbol{Q}^{\mathrm{ab}}$ be the maximal abelian extension of $\boldsymbol{Q}$ in $\bar{\boldsymbol{Q}}$.

(i) *$V = F \otimes_{O_F} T$ is irreducible as a representation of* $\mathrm{Gal}(\bar{\boldsymbol{Q}}/\boldsymbol{Q})$ *over F.*

($\mathrm{i_{str}}$) *$O_F/m_F \otimes_{O_F} T$ is irreducible as a representation of* $\mathrm{Gal}(\bar{\boldsymbol{Q}}/\boldsymbol{Q})$ *over O_F/m_F.*

(ii) *There exists an element σ of* $\mathrm{Gal}(\bar{\boldsymbol{Q}}/\boldsymbol{Q}^{\mathrm{ab}})$ *such that* $\dim_F(\mathrm{Ker}(1-\sigma; V \to V)) = 1$.

($\mathrm{ii_{str}}$) *There exists an element σ of* $\mathrm{Gal}(\bar{\boldsymbol{Q}}/\boldsymbol{Q}^{\mathrm{ab}})$ *such that* $\mathrm{Coker}(1-\sigma : T \to T)$ *is a free O_F-module of rank one.*

(We see easily that ($\mathrm{i_{str}}$) is stronger than (i) (that is, ($\mathrm{i_{str}}$) implies (i)) and that ($\mathrm{ii_{str}}$) is stronger than (ii)).

(iii) *There exists an integer w such that for any prime number l which does not divide NN', the roots of $P_l(t)$ are algebraic numbers whose all conjugates have absolute value $l^{w/2}$ in $\boldsymbol{C}$.* (In other words, V is "pure".)

To state the condition ($\mathrm{iv_\mathfrak{p}}$), we need some preliminary.

For a prime ideal $\mathfrak{p}$ of Λ such that $\Lambda_\mathfrak{p}$ is a discrete valuation ring, let $\mathrm{sgn}(\mathfrak{p}) \in \{1, -1\}$ be the image of the complex conjugation in $\mathrm{Gal}(\boldsymbol{Q}(\zeta_{dp^\infty})/\boldsymbol{Q})$ under $\mathrm{Gal}(\boldsymbol{Q}(\zeta_{dp^\infty})/\boldsymbol{Q}) \subset \Lambda \to \Lambda_\mathfrak{p}$.

Fix an embedding $\bar{\boldsymbol{Q}} \to \boldsymbol{C}$, and let $\iota \in \mathrm{Gal}(\bar{\boldsymbol{Q}}/\boldsymbol{Q})$ be the complex conjugation. Let

$$n(V, \mathfrak{p}) = \dim_F(\{x \in V; \iota(x) = -\mathrm{sgn}(\mathfrak{p})x\}).$$

Then $n(V, \mathfrak{p})$ is independent of the choice of $\bar{\boldsymbol{Q}} \to \boldsymbol{C}$, and

$$\mathrm{rank}_{\Lambda_\mathfrak{p}}(\boldsymbol{H}^1_\mathfrak{p}) - \mathrm{rank}_{\Lambda_\mathfrak{p}}(\boldsymbol{H}^2_p) = n(V, \mathfrak{p}).$$

This follows from Tate ([Ta, Theorem 2.2]). Now the condition ($\mathrm{iv_\mathfrak{p}}$) is as follows.

($\mathrm{iv_\mathfrak{p}}$) For a prime ideal $\mathfrak{p}$ of Λ such that $\Lambda_\mathfrak{p}$ is a discrete valuation ring,

$$n(V, \mathfrak{p}) = 1.$$

Example 0.6.1. Let $F = \boldsymbol{Q}_p, T = \boldsymbol{Z}_p(1), N = p, N' = 1$, and let $d = 1$. Then the conditions ($\mathrm{i_{str}}$), ($\mathrm{ii_{str}}$), (iii) are satisfied. (In ($\mathrm{ii_{str}}$), take $\sigma = 1$. In (iii), $w = -2$.) ($\mathrm{iv_\mathfrak{p}}$) is satisfied if $\mathrm{sgn}(\mathfrak{p}) = 1$.

Example 0.6.2. Let E be an elliptic curve over $\boldsymbol{Q}$, and consider the case $F = \boldsymbol{Q}_p, T$ is the p-adic Tate module $\varprojlim_n \mathrm{Ker}(p^n : E(\bar{\boldsymbol{Q}}) \to E(\bar{\boldsymbol{Q}}))$, and N is the conductor of $E, N' = 1$. Then the conditions (i), (iii) are satisfied (the integer w

in the condition (iii) is -1), and the condition $(\mathrm{iv}_{\mathfrak{p}})$ is satisfied for any prime ideal $\mathfrak{p}$ of Λ such that $\Lambda_{\mathfrak{p}}$ is a discrete valuation ring. If $E \otimes \bar{\boldsymbol{Q}}$ does not have a complex multiplication, the condition (ii) is satisfied, for the image of $\mathrm{Gal}(\bar{\boldsymbol{Q}}/\boldsymbol{Q}^{\mathrm{ab}})$ in $\mathrm{Aut}_{\boldsymbol{Z}_p}(T) \cong GL_2(\boldsymbol{Z}_p)$ contains an open subgroup of $SL_2(\boldsymbol{Z}_p)$ (Serre [S4, Chapter IV]) and hence contains an element of the form $\sigma = \left(\begin{smallmatrix} 1 & c \\ 0 & 1 \end{smallmatrix}\right)$ with $c \neq 0$ which satisfies $\dim_F(\mathrm{Ker}(1-\sigma : V \to V)) = 1$.

Remark 0.6.3. The condition (iii) is satisfied if there exist a proper smooth scheme X over $\boldsymbol{Z}[1/N]$ and $q \in \boldsymbol{Z}$ such that V is a subquotient of the representation $F \otimes_{\boldsymbol{Q}_p} H^q(X \otimes \bar{\boldsymbol{Q}}, \boldsymbol{Q}_p)$ of $\mathrm{Gal}(\bar{\boldsymbol{Q}}/\boldsymbol{Q})$ over F. The integer w in (iii) in this case is q. This is by Deligne [De].

0.7. Let

$$\xi \in \boldsymbol{H}^1$$

be the image of $(z_{Np^n})_{n\geq 0} \in \varprojlim_n H^1(\boldsymbol{Z}[\zeta_{Np^n}, 1/N], T)$ under the norm map. (Note $(z_{Np^n})_{n\geq 0}$ belongs to the above inverse limit by virtue of (0.1.1).) Define the ideal $J(\xi)$ of Λ by

$$J(\xi) = \{h(\xi); h \text{ is a } \Lambda\text{-homomorphism } \boldsymbol{H}^1 \to \Lambda\}.$$

Now the main result of this paper is the following.

THEOREM 0.8. *Let (F, T, N, N') be as in* 0.1 *and let $(z_m)_m$ be an Euler system for (F, T, N, N'). Let d and Λ be as in* 0.4, *and let $\mathfrak{p}$ be a prime ideal of Λ such that $\Lambda_{\mathfrak{p}}$ is a discrete valuation ring. Assume $\mathfrak{p}$ does not contain p (resp. $\mathfrak{p}$ contains p). Assume that the image $\xi_{\mathfrak{p}} \in \boldsymbol{H}^1_{\mathfrak{p}} = \Lambda_{\mathfrak{p}} \otimes_{\Lambda} \boldsymbol{H}^1$ of the element $\xi \in \boldsymbol{H}^1$ (cf.* 0.7) *is not a $\Lambda_{\mathfrak{p}}$-torsion element, and that the conditions* (i), (ii), (iii) (*resp.* $(\mathrm{i}_{\mathrm{str}})$, $(\mathrm{ii}_{\mathrm{str}})$, (iii)) *are satisfied. Then $\boldsymbol{H}^2_{\mathfrak{p}}$ is a torsion $\Lambda_{\mathfrak{p}}$-module and*

$$\mathrm{length}_{\Lambda_{\mathfrak{p}}}(\boldsymbol{H}^2_{0,\mathfrak{p}}) \leq \mathrm{length}_{\Lambda_{\mathfrak{p}}}(\Lambda_{\mathfrak{p}}/J(\xi)_{\mathfrak{p}}).$$

If furthermore the condition $(\mathrm{iv}_{\mathfrak{p}})$ *is satisfied, $\boldsymbol{H}^1_{\mathfrak{p}}/\Lambda_{\mathfrak{p}}\xi_{\mathfrak{p}}$ is a torsion $\Lambda_{\mathfrak{p}}$-module and*

$$\mathrm{length}_{\Lambda_{\mathfrak{p}}}(\boldsymbol{H}^2_{0,\mathfrak{p}}) \leq \mathrm{length}_{\Lambda_{\mathfrak{p}}}(\boldsymbol{H}^1_{\mathfrak{p}}/\Lambda_{\mathfrak{p}}\xi_{\mathfrak{p}})).$$

Remark 0.8.1. Let $F = \boldsymbol{Q}_p$, $T = \boldsymbol{Z}_p(1), N = p, N' = 1$, and let $d = 1$. Assume $p \neq 2$. Let $\mathfrak{p}$ be a prime ideal of Λ of height one such that $\mathrm{sgn}(\mathfrak{p}) = 1$. Then the image $\xi_{\mathfrak{p}}$ of $(1-\zeta_{p^n})_{n\geq 1}$ (cf. 0.2) in $\boldsymbol{H}^1_{\mathfrak{p}}$ is not a $\Lambda_{\mathfrak{p}}$-torsion element. Theorem 0.8 says

$$(*) \qquad \mathrm{length}_{\Lambda_{\mathfrak{p}}}(\boldsymbol{H}^2_{\mathfrak{p}}) \leq \mathrm{length}_{\Lambda_{\mathfrak{p}}}(\boldsymbol{H}^1_{\mathfrak{p}}/\Lambda_{\mathfrak{p}}\xi_{\mathfrak{p}}).$$

Iwasawa main conjecture, which says

$$\mathrm{length}_{\Lambda_{\mathfrak{p}}}(\boldsymbol{H}^2_{\mathfrak{p}}) = \mathrm{length}_{\Lambda_{\mathfrak{p}}}(\boldsymbol{H}^1_{\mathfrak{p}}/\Lambda_{\mathfrak{p}}\xi_{\mathfrak{p}}),$$

follows from (*) by the analytic class number formula (see [Ru_1]). Iwasawa main conjecture was proved by Mazur-Wiles ([MW]) and a new proof of it by using the method of Euler system was found by Rubin ([Ru_1]). In fact Rubin proves (*) in [Ru_1], and our proof of Theorem 0.8 is a natural generalization of the proof of (*) by Rubin given in [Ru_1].

Remark 0.8.2. Let (F, T, N) be as in 0.1, let d, Λ be as in 0.4, and let $\mathfrak{p}$ be a prime ideal of Λ such that $\Lambda_{\mathfrak{p}}$ is a discrete valuation ring. Then the conjecture in [Ka_1, Chapter I, 3.2.2] on "p-adic zeta elements" predicts that, if $\boldsymbol{H}^1_{\mathfrak{p}}$ is torsion free as a $\Lambda_{\mathfrak{p}}$-module (e.g. if $H^0(\boldsymbol{Q}(\zeta_{dp^\infty}), V) = 0$) and if the condition $(\mathrm{iv})_{\mathfrak{p}}$ is satisfied, there is an Euler system $(z_m)_m$ for $(F, T, N, 1)$ such that

$$\mathrm{length}_{\Lambda_{\mathfrak{p}}}(\boldsymbol{H}^2_{\mathfrak{p}}) = \mathrm{length}_{\Lambda_{\mathfrak{p}}}(\boldsymbol{H}^1_{\mathfrak{p}}/\Lambda_{\mathfrak{p}}\xi_{\mathfrak{p}}).$$

If V comes from a motif M, this Euler system should be related to special values of complex zeta functions of $M \otimes \chi$ for Dirichlet characters χ.

0.9. We sketch the main idea of the proof of Theorem 0.8 and the plan of this paper.

For an integer $m \geq 1$ which divides dp^i for some i, and for $n \geq 1$, consider the localization sequence of étale cohomology

$$\begin{aligned} H^1(\boldsymbol{Q}(\zeta_m), T/p^nT) &\xrightarrow{\partial} \bigoplus_l H^0(\boldsymbol{F}_l \otimes \boldsymbol{Z}[\zeta_m], T/p^nT(-1)) \\ &\xrightarrow{\iota} H^2\left(\boldsymbol{Z}\left[\zeta_m, \frac{1}{N}\right], T/p^nT\right) \end{aligned} \tag{0.9.1}$$

where l ranges over all prime numbers which do not divide N. The image of the map ι "nearly" coincides with the kernel $H^2(\boldsymbol{Z}[\zeta_m, 1/N], T/p^nT)_0$ of

$$H^2\left(\boldsymbol{Z}\left[\zeta_m, \frac{1}{N}\right], T/p^nT\right) \to \bigoplus_{l|N} H^2(\boldsymbol{Q}_l \otimes \boldsymbol{Q}(\zeta_m), T/p^nT)$$

where l ranges over all prime divisors of N. That is, $H^2(\boldsymbol{Z}[\zeta_m, 1/N], T/p^nT)_0$ is nearly the cokernel of ∂. To have the inequalities in Theorem 0.8, we have to show that $H^2(\boldsymbol{Z}[\zeta_m, 1/N], T/p^nT)_0$ is small enough, that is, the image of ∂ is big enough. To show this, we define in §2 certain elements κ_r in $H^1(\boldsymbol{Q}(\zeta_m), T/p^nT)$ (following the definition of the "derivatives" of the Euler system by Kolyvagin) and we compute the images of κ_r under ∂ (Theorem 4.5). From this computation, we can conclude that the image of ∂ is big enough. This is a rough idea of the proof of Theorem 0.8.

The following point is technically important. In the direct sum $\bigoplus_l$ in (0.9.1), we consider exclusively the l-components for "good prime numbers" l in the sense of §5. In fact, the l-components for good prime numbers l have simple structures (they are almost isomorphic to the group ring $(O_F/p^nO_F)[\mathrm{Gal}(\boldsymbol{Q}(\zeta_m)/\boldsymbol{Q})]$) and can be analyzed well (Proposition 5.5, here the condition (ii) in 0.6 plays an

essential role). It is sufficient to consider the l-components only for good prime numbers l, because the images of l-components for good prime numbers l under ι nearly generates $H^2(\boldsymbol{Z}[\zeta_m, 1/N], T/p^nT)_0$ (cf. 11.11). To show the last fact, we need results on Galois cohomology proved in §6 and §7.

§§8–12 are final steps of the proof of Theorem 0.8. In §8 (resp. §9), we show that $\boldsymbol{Q} \otimes H^2(\boldsymbol{Z}[1/N], V) = 0$ (resp. the localization of $\boldsymbol{H}^2$ at some prime ideal of Λ of height zero is zero) under a certain assumption on (F, T, N, N') and the Euler system $(z_m)_m$. After a module theoretic preliminary in §10, we complete the proof of Theorem 0.8 in §11 and §12.

In §13, we prove a finiteness theorem for Selmer groups (Theorem 13.2) and a finiteness theorem for H^2 (Theorem 13.3) as applications of Theorem 0.8.

§1. A local property of Euler system

The aim of §1 is to prove

PROPOSITION 1.1. *Let (F, T, N, N') be as in* 0.1, *and let $(z_m)_m$ be an Euler system for (F, T, N, N'). Then for an integer m such that $N|m$ and $(m, N') = 1$, of N and for a prime number l which does not divide mN', the image of z_{ml} in $H^1(\boldsymbol{Q}_l(\zeta_{ml}), T)$ coincides with the image of*

$$\{(l-1)^{-1}(P_l(l^{-1}\sigma_{l,m}^{-1}) - P_l(\sigma_{l,m}^{-1}))\} \cdot z_m \in H^1\left(\boldsymbol{Z}\left[\zeta_m, \frac{1}{N}\right], T\right).$$

Note that $P_l(l^{-1}\sigma_{l,m}^{-1}) \equiv P_l(\sigma_{l,m}^{-1}) \bmod (l-1)$, and hence

$$(l-1)^{-1}(P_l(l^{-1}\sigma_{l,m}^{-1}) - P_l(\sigma_{l,m}^{-1})) \in O_F[\mathrm{Gal}(\boldsymbol{Q}(\zeta_m)/\boldsymbol{Q})]$$

is defined.

This Proposition 1.1 will play an important role in §4 (Proposition 1.1 is not used in §2, §3).

Remark 1.2. In the case of the Euler system of cyclotomic units in Example 0.2,

$$(l-1)^{-1}(P_l(l^{-1}\sigma_{l,m}^{-1}) - P_l(\sigma_{l,m}^{-1})) = \sigma_{l,m}^{-1},$$

and the statement of Proposition 1.1 is the fact that $1 - \zeta_{ml}$ and $1 - \sigma_{l,m}^{-1}(\zeta_m)$ has the same image in

$$H^1(\boldsymbol{Z}_l[\zeta_{ml}], \boldsymbol{Z}_p(1)) \cong H^1(\boldsymbol{F}_l(\zeta_m), \boldsymbol{Z}_p(1)) \cong \boldsymbol{F}_l(\zeta_m)^\times\{p\}$$

where $\{p\}$ denotes the p-primary component of $\boldsymbol{F}_l(\zeta_m)^\times$. This property of the system of cyclotomic units is called the "congruence property", and the property (0.1.1) of the system of cyclotomic units is called the norm property. It is proved in [Ru3] that the congruence property of any Euler system of units is deduced from its norm property, by a different method.

In the rest of §1, we prove Proposition 1.2.

1.3. The map $H^1(\boldsymbol{Z}[\zeta_{ml}, 1/N], T) \to H^1(\boldsymbol{Q}_l(\zeta_{ml}), T)$ factors through

$$H^1\left(\boldsymbol{Z}_l \otimes \boldsymbol{Z}\left[\zeta_{ml}, \frac{1}{N}\right], T\right),$$

and

$$H^1\left(\boldsymbol{Z}_l \otimes \boldsymbol{Z}\left[\zeta_{ml}, \frac{1}{N}\right], T\right) \xrightarrow{\cong} H^1(\boldsymbol{F}_l \otimes \boldsymbol{Z}[\zeta_{ml}], T) \xleftarrow{\cong} H^1(\boldsymbol{F}_l \otimes \boldsymbol{Z}[\zeta_m], T).$$

We consider the inverse limit $\varprojlim_n H^1(\boldsymbol{F}_l \otimes \boldsymbol{Z}[\zeta_{mp^n}], T)$ with respect to norm maps, and prove that the image of $(z_{mlp^n})_{n\geq 0}$ in this inverse limit coincides with the image of

$$(\{(l-1)^{-1}(P_l(l^{-1}\sigma_{l,mp^n}^{-1}) - P_l(\sigma_{l,mp^n}^{-1}))\} \cdot z_{mp^n})_{n\geq 0}.$$

LEMMA 1.4. *$\varprojlim_n H^1(\boldsymbol{F}_l \otimes \boldsymbol{Z}[\zeta_{mp^n}, 1/N], T)$ is a torsion free O_F-module.*

Proof. By the duality of Galois cohomology of a finite field,

$$\varprojlim_n H^1(\boldsymbol{F}_l \otimes \boldsymbol{Z}[\zeta_{mp^n}], T) \cong \mathrm{Hom}_{O_F}(H^0(\boldsymbol{F}_l \otimes \boldsymbol{Z}[\zeta_{mp^\infty}], T^* \otimes_{O_F} F/O_F), F/O_F).$$

It is sufficient to show that $H^0(\boldsymbol{F}_l \otimes \boldsymbol{Z}[\zeta_{mp^\infty}], T^* \otimes_{O_F} F/O_F)$ is p-divisible. Since the degree of any finite extension of $\boldsymbol{F}_l(\zeta_{mp^\infty})$ is prime to p, we have $H^1(\boldsymbol{F}_l \otimes \boldsymbol{Z}[\zeta_{mp^\infty}], T^*/pT^*) = 0$. By the long exact sequence of $H^\cdot(\boldsymbol{F}_l \otimes \boldsymbol{Z}[\zeta_{mp^\infty}], \ )$ associated to the exact sequence

$$0 \to T^*/pT^* \to T^* \otimes_{O_F} F/O_F \xrightarrow{p} T^* \otimes_{O_F} F/O_F \to 0,$$

this implies that $H^0(\boldsymbol{F}_l \otimes \boldsymbol{Z}[\zeta_{mp^\infty}], T^* \otimes_{O_F} F/O_F)$ is p-divisible.

1.5. By Lemma 1.4, it is sufficient to prove that the image of $(l-1) \cdot z_{mlp^n}$ in $H^1(\boldsymbol{F}_l \otimes \boldsymbol{Z}[\zeta_{mp^n}], T)$ coincides with the image of $(P_l(l^{-1}\sigma_{l,mp^n}^{-1}) - P_l(\sigma_{l,mp^n}^{-1})) \cdot z_{mp^n}$ for any n. By replacing mp^n by m, we are reduced to

LEMMA 1.6. (1) *The image of $(l-1) \cdot z_{ml}$ in $H^1(\boldsymbol{F}_l \otimes \boldsymbol{Z}[\zeta_m], T)$ coincides with the image of $P_l(l^{-1}\sigma_{l,m}^{-1}) \cdot z_m$.*

(2) *The image of $P_l(\sigma_{l,m}^{-1}) \cdot z_m$ in $H^1(\boldsymbol{F}_l \otimes \boldsymbol{Z}[\zeta_m], T)$ is zero.*

Proof. (1) follows from (0.1.1) by the commutative diagram

$$\begin{array}{ccc} H^1\left(\boldsymbol{Z}\left[\zeta_{ml}, \frac{1}{N}\right], T\right) & \longrightarrow & H^1(\boldsymbol{F}_l \otimes \boldsymbol{Z}[\zeta_m], T) \\ \Big\downarrow \text{norm} & & \Big\downarrow l-1 \\ H^1\left(\boldsymbol{Z}\left[\zeta_m, \frac{1}{N}\right], T\right) & \longrightarrow & H^1(\boldsymbol{F}_l \otimes \boldsymbol{Z}[\zeta_m], T). \end{array}$$

To prove (2), let

$$\Phi_m = \Lambda_m \otimes_{O_F} T \quad \text{where } \Lambda_m = O_F[\mathrm{Gal}(\boldsymbol{Q}(\zeta_m)/\boldsymbol{Q})]$$

on which $\mathrm{Gal}(\bar{\boldsymbol{Q}}/\boldsymbol{Q})$ acts as follows. For $\sigma \in \mathrm{Gal}(\bar{\boldsymbol{Q}}/\boldsymbol{Q})$, the action of σ on Φ_m is $(\bar{\sigma})^{-1} \otimes \sigma$, where $\bar{\sigma}$ denotes the image of σ in $\mathrm{Gal}(\boldsymbol{Q}(\zeta_m)/\boldsymbol{Q}) \subset \Lambda_m$. Then

$$H^1(\boldsymbol{F}_l \otimes \boldsymbol{Z}[\zeta_m], T) \cong H^1(\boldsymbol{F}_l, \Phi_m) \cong \Phi_m/(1-\varphi_l)\Phi_m$$

as Λ_m-modules (for explanations of these isomorphisms, see 3.4 and 4.2), and

$$P_l(\sigma_{l,m}^{-1}) = \det_{\Lambda_m}(1-\varphi_l : \Phi_m \to \Phi_m).$$

This shows that $P_l(\sigma_{l,m}^{-1})$ kills $H^1(\boldsymbol{F}_l \otimes \boldsymbol{Z}[\zeta_m], T)$.

§2. Derivatives of an Euler systems

2.1. Let (F, T, N, N') be as in 0.1, and let $(z_m)_m$ be an Euler system for (F, T, N, N'). Fix an integer m such that $N|m$ and $(m, N') = 1$, and integers n, n' such that $n' \geq n \geq 1$. Assume

(2.1.1) there exists an integer $c \geq 0$ such that p^c kills $H^0(\boldsymbol{Q}(\zeta_m), T \otimes (\boldsymbol{Q}/\boldsymbol{Z}))$ and $n' \geq n + 2c$.

The aim of §2 is to define important elements

$$\kappa_r \in H^1\left(\boldsymbol{Z}\left[\zeta_m, \frac{1}{Nr}\right], T/p^n T\right)$$

for integers $r \geq 1$ satisfying the following conditions (2.1.2) and (2.1.3). Our definition of κ_r here follows the definition of the derivative of an Euler system in [Ko$_1$], [Ko$_2$].

(2.1.2) r is square free, and is prime to m.

(2.1.3) $P_l(l^{-1}\sigma_{l,m}^{-1}) \in p^{n'} O_F[\mathrm{Gal}(\boldsymbol{Q}(\zeta_m)/\boldsymbol{Q})]$ and $l - 1 \in p^{n'}\boldsymbol{Z}$ for any prime divisor l of r.

(In fact κ_r is defined canonically only after we fix generators of some cyclic Galois groups over $\boldsymbol{Q}$. See Remark 2.9.)

2.2. Assume r satisfies the conditions (2.1.2) and (2.1.3).

For a prime divisor l of r, let $L^{(l)}/\boldsymbol{Q}(\zeta_m)$ be the unique subextension of $\boldsymbol{Q}(\zeta_{ml})/\boldsymbol{Q}(\zeta_m)$ of degree $p^{n'}$. For a divisor s of r, let $L^{(s)}$ be the composite of $L^{(l)}$ where l ranges over all prime divisors of s, and let $R^{(s)}$ be the integral closure of $\boldsymbol{Z}[1/Nr]$ in $L^{(s)}$.

In this 2.2, we define an element $\omega_r \in H^1(R^{(r)}, T/p^{n'}T)$. As a preliminary for the definition of ω_r, we define

$$v_s \in H^1(R^{(s)}, T), \quad v_{r,s} \in H^1(R^{(r)}, T)$$

as follows. Let v_s be the image of z_{ms} under the norm map

$$H^1\left(\boldsymbol{Z}\left[\zeta_{ms}, \frac{1}{Nr}\right], T\right) \xrightarrow{\text{norm}} H^1(R^{(s)}, T).$$

Let $v_{r,s}$ be the image of

$$\mu(s) \cdot \left\{ \prod_{l|(r/s)} p^{-n'} P_l(l^{-1} \cdot (\sigma_{l,m}^{-1} \times 1)) \right\} \cdot v_s,$$

under the canonical map $H^1(R^{(s)}, T) \to H^1(R^{(r)}, T)$ associated to the inclusion map $R^{(s)} \xrightarrow{\subset} R^{(r)}$. Here, $\mu(s)$ denotes Möbius function (that is, $\mu(s) = (-1)^k$ where k is the number of prime divisors of s), $\prod_{l|(r/s)}$ means the product over all prime divisors l of r/s, and $\sigma_{l,m}^{-1} \times 1$ means the element of $\mathrm{Gal}(\boldsymbol{Q}(\zeta_{ms})/\boldsymbol{Q})$ (acting on $H^1(R^{(s)}, T)$) whose restriction to $\boldsymbol{Q}(\zeta_m)$ coincides with $\sigma_{l,m}^{-1}$ and whose restriction to $\boldsymbol{Q}(\zeta_s)$ is the identity map. Let

$$\omega_r = \sum_s v_{r,s}$$

where $\sum_s$ means the sum over all divisors s of r.

2.3. For a divisor s of r, let $G^{(s)} = \mathrm{Gal}(L^{(s)}/Q(\zeta_m))$. Then for a prime divisor l of r, $G^{(l)}$ is a cyclic groups of order $p^{n'}$, and $G^{(r)} \xrightarrow{\cong} \prod_{l|r} G^{(l)}$. Fix a generator α_l of $G^{(l)}$ for each l, and regard α_l as an element of $G^{(r)}$ via this isomorphism.

For a $G^{(r)}$-module M killed by $p^{n'}$, and for a divisor s of r, let

$$D^{(s)} : M \to M$$

be the composite $\prod_{l|s} D^{(l)}$ where l ranges over all prime divisors of s and $D^{(l)}$ is a homomorphism $M \to M$ defined as follows ($D^{(l)}$ commutes with each other);

$$D^{(l)}(x) = \sum_{i=0}^{p^{n'}-1} i \cdot (\alpha_l)^i(x).$$

LEMMA 2.4. *The map*

$$D^{(r)} : H^1(R^{(r)}, T/p^{n'}T) \to H^1(R^{(r)}, T/p^{n'}T)$$

sends ω_r into the $G^{(r)}$-fixed part of $H^1(R^{(r)}, T/p^{n'}T)$.

For the proof of Lemma 2.4, we use

LEMMA 2.5. *For a prime divisor l of r, the norm map*

$$N^{(l)} : H^1(R^{(r)}, T) \to H^1(R^{(r/l)}, T).$$

sends ω_r (*cf.* 2.2) *to*

$$(P_l(l^{-1} \cdot (\sigma_{l,m}^{-1} \times 1)) - P_l(l^{-1}\sigma_{l,mr/l}^{-1})) \cdot \omega_{r/l}.$$

Proof. Let s be a divisor of r/l. Then by simple computation we have

$$N^{(l)}(v_{r,s}) = P_l(l^{-1} \cdot (\sigma_{l,m}^{-1} \times 1)) \cdot v_{r/l,s}.$$

By using (0.1.1), we have also

$$N^{(l)}(v_{r,sl}) = -P_l(l^{-1}\sigma_{l,mr/l}^{-1}) \cdot v_{r/l,s}.$$

By taking the sum of these equations for all s, we obtain Lemma 2.5.

2.6. We prove Lemma 2.4 by induction on the number of prime divisors of r.

It is sufficient to prove $(1 - \alpha_l)(D^{(r)}(\omega_r)) = 0$ for each prime divisor l of r. We have

$$(1 - \alpha_l) \circ D^{(l)} = \sum_{\tau \in G^{(l)}} \tau.$$

Hence

$$(1 - \alpha_l) \circ D^{(r)} = D^{(r/l)}(N^{(l)}(\omega_r)).$$

By Lemma 2.5, $N^{(l)}(\omega_r)$ is generated by elements of the form $(1 - \tau)(\omega_{r/l})$ with $\tau \in G^{(r/l)}$. Hence we are reduced to proving

$$(1 - \tau) \circ D^{(r/l)}(\omega_{r/l}) = 0$$

but this follows by induction.

LEMMA 2.7. *Let* c *be as in* 2.1. *Then for any* $a \geq 0$ *and* $a' \geq a + c$, *the canonical map*

$$H^0(R^{(r)}, T/p^{a'}\ T) \to H^0(R^{(r)}, T/p^a T)$$

is the zero map.

Proof. We have a commutative diagram

$$\begin{array}{ccc} H^0(R^{(r)}, T/p^{a'}T) & \xrightarrow{\subset} & H^0(\boldsymbol{Q}(\zeta_{mr}), T \otimes (\boldsymbol{Q}/\boldsymbol{Z})) \\ \downarrow & & \downarrow{\scriptstyle p^{a'-a}} \\ H^0(R^{(r)}, T/p^a T) & \xrightarrow{\subset} & H^0(\boldsymbol{Q}(\zeta_{mr}), T \otimes (\boldsymbol{Q}/\boldsymbol{Z})) \end{array}$$

with injective horizontal arrows. Since $a' - a \geq c$, it is sufficient to prove that p^c kills $H^0(\boldsymbol{Q}(\zeta_{mr}), T \otimes (\boldsymbol{Q}/\boldsymbol{Z}))$. For this it is enough to show that the inclusion

$$H^0(\boldsymbol{Q}(\zeta_m), T \otimes (\boldsymbol{Q}/\boldsymbol{Z})) \subset H^0(\boldsymbol{Q}(\zeta_{mr}), T \otimes (\boldsymbol{Q}/\boldsymbol{Z}))$$

is in fact an equality. This follows from the fact that $\mathrm{Gal}(\bar{\boldsymbol{Q}}/\boldsymbol{Q}(\zeta_m))$ is generated by $\mathrm{Gal}(\bar{\boldsymbol{Q}}/\boldsymbol{Q}(\zeta_{mr}))$ and the inertia subgroups at prime divisors of r which act trivially on T.

2.8. Now we define κ_r. Consider the exact sequences

$$0 \to H^1(G^{(r)}, H^0(R^{(r)}, T/p^aT)) \to H^1\left(\boldsymbol{Z}\left[\zeta_m, \frac{1}{Nr}\right], T/p^aT\right)$$
$$\to H^0(G^{(r)}, H^1(R^{(r)}, T/p^aT)) \to H^2(G^{(r)}, H^0(R^{(r)}, T/p^aT))$$

for $a \geq 1$.

By Lemma 2.4, $D^{(r)}(\omega_r)$ belongs to $H^0(G^{(r)}, H^1(R^{(r)}, T/p^{n'}T))$. By Lemma 2.7 and by the above exact sequences for $a = n + c$ and $a = n'$, we see that the image of $D^{(r)}(\omega_r)$ in $H^0(G^{(r)}, H^1(R^{(r)}, T/p^{n+c}T))$ is the image of an element x of $H^1(\boldsymbol{Z}[\zeta_m, 1/Nr], T/p^{n+c}T)$. By Lemma 2.7 and by the above exact sequences for $a = n$ and for $a = n + c$, the image of x in $H^1(\boldsymbol{Z}[\zeta_m, 1/Nr], T/p^nT)$ is independent of the choice of x. We define $\kappa_r \in H^1(\boldsymbol{Z}[\zeta_m, 1/Nr], T/p^nT)$ to be the image of x.

Remark 2.9. The element

$$\left(\bigotimes_{l|N} \alpha_l\right) \otimes \kappa_r \in H^1\left(\boldsymbol{Z}\left[\zeta_m, \frac{1}{Nr}\right], \left(\bigotimes_{l|r} G^{(l)}\right) \otimes T/p^nT\right). \tag{2.9.1}$$

is independent of the choices of the generators α_l of $G^{(l)}$.

§3. Local study

In this section, we review some basic facts about Galois cohomology of a local field, and prove Proposition 3.6 which will play a key role in the proof of a local property Theorem 4.5 of derivatives of an Euler system.

3.1. In this section, let K be a complete discrete valuation field with residue field k. Let $\bar{K}$ be a separable closure of K, and let K_{ur} be the maximal unramified extension of K in $\bar{K}$. Then the residue field $\bar{k}$ of K_{ur} is a separable closure of k, and

$$\mathrm{Gal}(K_{\mathrm{ur}}/K) \xrightarrow{\cong} \mathrm{Gal}(\bar{k}/k).$$

To make arguments about inverse limits of Galois cohomology simple, we assume that K has the following property: If T is a discrete finite abelian group endowed with a continuous action of $\mathrm{Gal}(\bar{K}/K)$, and if the order of T is invertible in k, $H^q(K, T)$ is a finite group for any q. For example, K has this property if k is a finite field (and this case is sufficient for this paper). For a prime number p which is invertible in k and for a finitely generated $\boldsymbol{Z}_p$-module T endowed with a continuous action of $\mathrm{Gal}(\bar{K}/K)$, let

$$H^q(K, T) = \varprojlim_n H^q(K, T/p^nT).$$

3.2. We review some general fact on Galois cohomology of K.

Let p be a prime number which is invertible in k, and let T be a finitely generated $\boldsymbol{Z}_p$-module endowed with a continuous action of $\mathrm{Gal}(K_{\mathrm{ur}}/K)$. Then we have an exact sequence

$$0 \to H^q(k, T) \to H^q(K, T) \xrightarrow{\partial} H^{q-1}(k, T(-1)) \to 0 \tag{3.2.1}$$

where (-1) means the Tate twist by -1. The second arrow in (3.2.1) is the inflation map for the surjection $\mathrm{Gal}(\bar{K}/K) \to \mathrm{Gal}(K_{\mathrm{ur}}/K) \cong \mathrm{Gal}(\bar{k}/k)$, and ∂ is defined as follows. Consider the isomorphisms

$$H^1(K_{\mathrm{ur}}, \boldsymbol{Z}/n(1)) \xleftarrow{\cong} K_{\mathrm{ur}}^{\times}/(K_{\mathrm{ur}}^{\times})^n \xrightarrow{\cong} \boldsymbol{Z}/n \tag{3.2.2}$$

where the first arrow is by Kummer theory and the second arrow is the valuation of K_{ur}. By tensoring (3.2.2) with $T(-1)$, we obtain

$$H^1(K_{\mathrm{ur}}, T) \cong T(-1). \tag{3.2.3}$$

The map ∂ is defined to be the composite

$$H^1(K, T) \to H^0(\mathrm{Gal}(K_{\mathrm{ur}}/K), H^1(K_{\mathrm{ur}}, T)) = H^0(k, H^1(K_{\mathrm{ur}}, T))$$
$$\underset{(3.2.3)}{\cong} H^0(k, T(-1)).$$

3.3. Let L be a totally ramified Galois extension of K and assume that $n = [L : K]$ is invetible in k. Then K contains a primitive n-th root of 1, L is a cyclic extension of K, $L = K(\pi^{1/n})$ for some prime element π of K, and we have an isomorphism

$$\mathrm{Gal}(L/K) \xrightarrow{\cong} \boldsymbol{Z}/n(1); \quad \sigma \mapsto \sigma(\alpha)\alpha^{-1} \quad \text{where } \alpha = \pi^{1/n}.$$

(Cf. [Se_1, Chapter IV §2, Corollary 1].)

3.4. We give general comments on Galois representations.

Let A be a field and let A' be a subring of A which is normal Noetherian and whose field of fractions is A. Let $\bar{A}$ be a separable closure of A, B a finite Galois extension of A in $\bar{A}$ with Galois group G, and let B' be the integral closure of A' in B. Assume B' is unramified over A'. Let p be a prime number and let T be a finitely generated $\boldsymbol{Z}_p$-module endowed with a continuous action of $\mathrm{Gal}(\bar{A}/A)$ which is unramified at any prime ideal of A'. Let

$$R = \boldsymbol{Z}_p[G], \quad M = R \otimes_{\boldsymbol{Z}_p} T,$$

and endow M with the following R-linear action of $\mathrm{Gal}(\bar{A}/A)$: For $\sigma \in \mathrm{Gal}(\bar{A}/A)$, the action of σ on M is $(\bar{\sigma})^{-1} \otimes \sigma$ where $\bar{\sigma}$ denotes the canonical image of σ in $G \subset R$. If we identify T (resp. M) with the corresponding $\boldsymbol{Z}_p$ (resp. R)-sheaf on $\mathrm{Spec}(A')_{\text{ét}}$,

$$M = f_* f^* T \tag{3.4.1}$$

as an R-sheaf, where f is the canonical morphism $\mathrm{Spec}(B') \to \mathrm{Spec}(A')$. So we have

$$H^q(A', M) = H^q(B', T) \quad \text{for any } q \geq 0 \tag{3.4.2}$$

as an R-module, where $H^q(\ , M) = \varprojlim_n H^q(\ , M/p^n M)$, $H^q(\ , T) = \varprojlim_n H^q(\ , T/p^n T)$.

The norm map $H^q(B', T) \to H^q(A', T)$ is identified with $H^q(A', M) \to H^q(A', T)$ induced by $M \to T$; $\sigma \otimes x \mapsto x$ $(\sigma \in G)$, and the canonical morphism $H^q(A', T) \to H^q(B', T)$ is identified with $H^q(A', T) \to H^q(A', M)$ induced by $\iota : T \to M$; $x \mapsto (\sum_{\sigma \in G} \sigma) \otimes x$.

3.5. Let the situation be as in 3.4. Let I_G be the kernel of the homomorphism $\boldsymbol{Z}[G] \to \boldsymbol{Z}$; $\sigma \mapsto 1$ $(\sigma \in G)$ and let $G^{\mathrm{ab}} = G/[G, G]$. We define a homomorphism

$$D : I_G M \to G^{\mathrm{ab}} \otimes T \tag{3.5.1}$$

to be the composite map

$$I_G M \to I_G M / I_G^2 M \xleftarrow{\cong} I_G / I_G^2 \otimes_{\boldsymbol{Z}} M / I_G M \xrightarrow{\cong} I_G / I_G^2 \otimes T \cong G^{\mathrm{ab}} \otimes T$$

where the last isomorphism comes from

$$G^{\mathrm{ab}} \xrightarrow{\cong} I_G / I_G^2; \quad \sigma \mapsto 1 - \sigma.$$

If G is a cyclic group of order n and α is a generator of G, we regard D as a homomorphism $I_G M \to T/nT$ (G^{ab} in (3.5.1) is identified with $\boldsymbol{Z}/n\boldsymbol{Z}$ by $\alpha \mapsto 1$). In this case, the diagram

$$\begin{array}{ccc} I_G M & \xrightarrow{\subset} & M \\ {\scriptstyle D}\downarrow & & \downarrow{\scriptstyle \sum_{\iota=0}^{n-1} i\alpha^\iota} \\ T/nT & \xrightarrow{\iota} & M/nM \end{array}$$

is commutative (thus D is related to the homomorphism $D^{(l)}$ in §2), and hence we have a commutative diagram

$$\begin{array}{ccc} H^q(A', I_G M) & \longrightarrow & H^q(A', M) = H^q(B', T) \\ {\scriptstyle D}\downarrow & & \downarrow{\scriptstyle \sum_{\iota=0}^{n-1} i\alpha^\iota} \\ H^q(A', T) & \longrightarrow & H^q(B', T/nT) \end{array}$$

for any i.

PROPOSITION 3.6. *In* 3.4, *consider the case* $A = A' = K$, $B = B' = L$ *where* L *is a totally ramified cyclic extension of* K *of degree* p^n *for a prime number* p *which*

is invertible in k and for some $n \geq 0$. Assume that T is p-torsion free, and the action of $\mathrm{Gal}(\bar{K}/K)$ *on T factors through* $\mathrm{Gal}(K_{\mathrm{ur}}/K)$. *Then the map*

$$H^1(K, I_G M) \to H^1(K, M) \underset{(3.4.2)}{=} H^1(L, T) \tag{3.6.1}$$

coincides with the minus of the composite

$$H^1(K, I_G M) \xrightarrow{D} H^1(K, G \otimes T) \underset{3.3}{\cong} H^1(K, T/p^n T(1)) \tag{3.6.2}$$

$$\xrightarrow{\partial} H^0(k, T/p^n T) = H^0(K, T/p^n T) \xrightarrow{\delta} H^1(K, T) \to H^1(L, T)$$

where δ denotes the connecting map of the exact sequence

$$0 \to T \xrightarrow{p^n} T \to T/p^n \to 0.$$

The rest of §3 is devoted to the proof of Proposition 3.6.

LEMMA 3.7. *Let $f : H^0(K, T/p^n T) \to H^1(K, I_G M)$ be the following homomorphism. For $a \in T$ such that $a \bmod p^n \in H^0(K, T/p^n T)$, let $f(a \bmod p^n)$ be the class of the 1-cocycle*

$$g_a : \mathrm{Gal}(\bar{K}/K) \to I_G M; \quad \sigma \mapsto (1 - (\bar{\sigma})^{-1}) \otimes \sigma(a) - \left(\sum_{\alpha \in G} (1 - \alpha)\right) \otimes p^{-n}(\sigma(a) - a).$$

(g_a is a 1-cocycle because

$$g_a(\sigma) = (1 - \sigma)\left\{\sum_{\alpha \in G} (1 - \alpha) \otimes p^{-n} a\right\} \quad \text{in } Q \otimes I_G M.)$$

Then:

(1) *The diagram*

$$\begin{array}{ccccccc} H^0(K, T) & \longrightarrow & H^0(K, T/p^n T) & \longrightarrow & H^1(K, T) & \xrightarrow{p^n} & H^1(K, T) \\ \| & & \downarrow f & & \downarrow & & \| \\ H^0(K, T) & \longrightarrow & H^1(K, I_G M) & \longrightarrow & H^1(K, M) & \xrightarrow{p^n} & H^1(K, T) \end{array}$$

is commutative, where the upper horizontal sequence is the exact sequence obtained from the exact sequence $0 \to T \xrightarrow{p^n} T \to T/p^n \to 0$ and the lower horizontal sequence is the exact sequence obtained from the exact sequence $0 \to I_G M \to M \to T \to 0$.

(2) *f is surjective.*

Proof. (1) is checked directly. To prove (2), by the commutativity of the diagram in (1), it is sufficient to prove that

$$\mathrm{Ker}(H^1(K, T) \xrightarrow{p^n} H^1(K, T)) \to \mathrm{Ker}(H^1(K, M) \to H^1(K, T)) \tag{3.7.1}$$

is surjective. Note that $H^1(L,T) = H^1(K,M) \to H^1(K,T)$ is the norm map. The surjectivity of (3.7.1) follows from the commutative diagram of exact sequences

$$\begin{array}{ccccccccc} 0 & \longrightarrow & H^1(k,T) & \longrightarrow & H^1(L,T) & \longrightarrow & H^0(k,T(-1)) & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle p^n} & & \downarrow{\scriptstyle \text{norm}} & & \downarrow{\scriptstyle \text{id.}} & & \\ 0 & \longrightarrow & H^1(k,T) & \longrightarrow & H^1(K,T) & \longrightarrow & H^0(k,T(-1)) & \longrightarrow & 0. \end{array}$$

Now by Lemma 3.7 (2), for the proof of Proposition 3.6, it is sufficient to show that the compositions (3.6.1) $\circ f$ and (3.6.2) $\circ f$ are equal.

LEMMA 3.8. *The composite*

$$H^0(K,T/p^nT) \xrightarrow{f} H^1(K,I_GM) \xrightarrow{D} H^1(K,G\otimes T) \xrightarrow{\partial} H^0(k,T/p^nT)$$
$$= H^0(K,T/p^nT)$$

coincides with the multiplication by -1.

Proof. Let a be an element of T such that $a \bmod p^n \in H^0(K,T/p^nT)$. Then $D \circ f$ $(a \bmod p^n)$ is the class of the 1-cocycle

$$\mathrm{Gal}(\bar{K}/K) \to G\otimes T; \quad \sigma \mapsto -\bar{\sigma}\otimes a - \sum_{\alpha\in G}\{\alpha\otimes p^{-n}(\sigma(a)-a)\}.$$

Since $\sigma(a)-a=0$ if σ belongs to $\mathrm{Gal}(\bar{K}/K_{\mathrm{ur}})$, we see that ∂ kills the class of the 1-cocycle $\sigma \mapsto \sum_{\alpha\in G}\{\alpha\otimes p^{-n}(\sigma(a)-a)\}$. It remains to show that $H^1(K,G) \cong H^1(K,\boldsymbol{Z}/p^n(1)) \xrightarrow{\partial} H^0(K,\boldsymbol{Z}/p^n\boldsymbol{Z})$ sends the class of the 1-cocycle $\sigma \mapsto \bar{\sigma}$ to 1. But this follows from the definitions of the isomorphism $G \cong \boldsymbol{Z}/p^n(1)$ and ∂.

3.9. Now we complete the proof of Proposition 3.6. Consider the commutative diagram

$$\begin{array}{ccc} H^0(K,T/p^nT) & \longrightarrow & H^1(K,T) \\ \downarrow{\scriptstyle f} & & \downarrow \\ H^1(K,I_GM) & \longrightarrow & H^1(K,M) = H^1(L,T) \end{array}$$

(Lemma 3.7 (1)). The composite $H^0(K,T/p^nT) \xrightarrow{f} H^1(K,I_GM \to H^1(L,T)$ in this diagram coincides with (3.6.1) $\circ f$. On the other hand, by Lemma 3.8, the composite $H^0(K,T/p^nT) \to H^1(K,T) \to H^1(L,T)$ in this diagram coincides with $-$(3.6.2) $\circ f$. This shows that

$$(3.6.1)\circ f = -(3.6.2)\circ f.$$

§4. Local property of derivatives of an Euler system

We prove a formula Theorem 4.5 concerning a local property of derivatives of an Euler system.

4.1. We first give a preliminary on "cofactor homomorphism".

Let R be a commutative ring, let M be a free R-module of finite rank r, and let $f : M \to M$ be an R-homomorphism. Then the cofactor homomorphism $c_f : M \to M$ is defined to be the unique R-homomorphism which makes the following diagram commutative.

$$\begin{array}{ccc} M & \xrightarrow{\cong} & \mathrm{Hom}_R\left(\bigwedge_R^{r-1} M, \bigwedge_R^{r} M\right) \\ {\scriptstyle c_f}\downarrow & & \downarrow{\scriptstyle h \mapsto h \circ \left(\bigwedge^{r-1} f\right)} \\ M & \xrightarrow{\cong} & \mathrm{Hom}_R\left(\bigwedge_R^{r-1} M, \bigwedge_R^{r} M\right) \end{array}$$

Here the horizontal arrows are $x \mapsto (y \mapsto x \wedge y)$.

If f is expressed by a matrix A, c_f is expresed as the matrix of cofactors of A.

We have

$$f \circ c_f = c_f \circ f = \text{multiplication by } \det(f).$$

4.2. Let l be a prime number, and let $\varphi_l \in \mathrm{Gal}(\bar{\boldsymbol{F}}_l/\boldsymbol{F}_l)$ be the arithmetic Frobenius $\bar{\boldsymbol{F}}_l \to \bar{\boldsymbol{F}}_l$; $x \mapsto x^l$. Let R be a pro-finite commutative ring, and let M a free R-module of finite rank endowed with an R-linear continuous action of $\mathrm{Gal}(\bar{\boldsymbol{F}}_l/\boldsymbol{F}_l)$. Assume

$$\det_R(1 - \varphi_l : M \to M) = 0.$$

We define an *important homomorphism*

$$\psi_l : H^1(\boldsymbol{F}_l, M) \to H^0(\boldsymbol{F}_l, M)$$

as follows.

Recall that $H^q(\boldsymbol{F}_l, M) = 0$ for $q \neq 0, 1$ and there are canonical isomorphisms

$$H^0(\boldsymbol{F}_l, M) \cong \mathrm{Ker}(1 - \varphi_l : M \to M),$$

$$H^1(\boldsymbol{F}_l, M) \cong \mathrm{Coker}(1 - \varphi_l : M \to M).$$

(In the latter isomorphism, an element of $H^1(\boldsymbol{F}_l, M)$ represented by a continuous 1-cocycle $c : \mathrm{Gal}(\bar{\boldsymbol{F}}_l/\boldsymbol{F}_l) \to M$ corresponds to the element $c(\varphi_l) \bmod (1 - \varphi_l)M$. Cf. [Se$_1$, Chapter XIII §1].

Let $f = 1 - \varphi_l : M \to M$, and consider the cofactor homomorphism c_f. Since $f \circ c_f$ and $c_f \circ f$ induce the zero map $\det_R(f : M \to M)$ on M,

$$c_f : M \to M$$

induces

$$\mathrm{Coker}(f : M \to M) \to \mathrm{Ker}(f : M \to M),$$

that is,

$$H^1(\boldsymbol{F}_l, M) \to H^0(\boldsymbol{F}_l, M)$$

which we denote by ψ_l.

4.3. Now let (F, T, N, N') be as in 0.1. In 4.3 and 4.4, we fix some notations.

For $m \geq 1$, let

$$\Lambda_m = O_F[\mathrm{Gal}(\boldsymbol{Q}(\zeta_m)/\boldsymbol{Q})], \quad \Lambda_{m,n} = \Lambda_m/p^n\Lambda_m \quad \text{for } n \geq 0.$$

Define a Λ_m-module Φ_m endowed with a Λ_m-linear continuous action of $\mathrm{Gal}(\bar{\boldsymbol{Q}}/\boldsymbol{Q})$ as follows. As a Λ_m-module, let

$$\Phi_m = \Lambda_m \otimes_{O_F} T.$$

Define the action of $\sigma \in \mathrm{Gal}(\bar{\boldsymbol{Q}}/\boldsymbol{Q})$ on Φ_m to be $(\bar{\sigma})^{-1} \otimes \sigma$ where $\bar{\sigma}$ denotes the canonical image of σ in $\mathrm{Gal}(\boldsymbol{Q}(\zeta_m)/\boldsymbol{Q}) \subset \Lambda_m$. (Cf. 3.4.) Then, if l is a prime number which does not divide Nm, we have

$$\begin{aligned} P_l(\sigma_{l,m}^{-1}) &= \det_{\Lambda_m}(1 - \varphi_l : \Phi_m \to \Phi_m), \\ P_l(l^{-1}\sigma_{l,m}^{-1}) &= \det_{\Lambda_m}(1 - l^{-1}\varphi_l : \Phi_m \to \Phi_m). \end{aligned} \tag{4.3.1}$$

Let

$$\Phi_{m,n} = \Phi_m/p^n\Phi_m \quad \text{for } n \geq 0.$$

If

$$\det_{\Lambda_{m,n}}(1 - \varphi_l : \Phi_{m,n} \to \Phi_{m,n}) = 0$$

$$(\text{i.e. if } P_l(\sigma_{l,m}^{-1}) \equiv 0 \bmod p^n),$$

$$\psi_l : H^1(\boldsymbol{F}_l \otimes \boldsymbol{Z}[\zeta_m], T/p^nT) \to H^0(\boldsymbol{F}_l \otimes \boldsymbol{Z}[\zeta_m], T/p^nT)$$

is defined by identifying $H^q(\boldsymbol{F}_l \otimes \boldsymbol{Z}[\zeta_m], T/p^nT)$ with $H^q(\boldsymbol{F}_l, \Phi_{m,n})$ $(q = 0, 1)$ (cf. 3.4) and by taking $\Lambda_{m,n}$ and $\Phi_{m,n}$ as R and M in 4.2, respectively.

4.4. Let (F, T, N, N') be as in 0.1 and let $(z_m)_m$ be an Euler system for (F, T, N, N').

Let m, n, n', r be as in 2.1 assuming (2.1.1)–(2.1.3) are satisfied. Let l be a prime divisor of r.

By fixing generators of $G^{(l')}$ (cf. 2.3) for any prime divisor l' of r/l, we denote the element (2.9.1) of $H^1(\boldsymbol{Z}[\zeta_m, 1/Nr], G^{(l)} \otimes T/p^nT)$ by κ_r. We have also an element $\kappa_{r/l} \in H^1(\boldsymbol{Z}[\zeta_m, 1/(Nr/l)], T/p^nT)$.

Let

$$\partial_l : H^1\left(\boldsymbol{Z}\left[\zeta_m, \frac{1}{Nr}\right], G^{(l)} \otimes T/p^nT\right) \to H^0(\boldsymbol{F}_l \otimes \boldsymbol{Z}[\zeta_m], T/p^nT)$$

be the composite map

$$H^1\left(\boldsymbol{Z}\left[\zeta_m, \frac{1}{Nr}\right], G^{(l)} \otimes T/p^nT\right) \to H^1(\boldsymbol{Q}_l \otimes \boldsymbol{Q}(\zeta_m), G^{(l)} \otimes T/p^nT)$$

$$\underset{3.3}{\cong} H^1(\boldsymbol{Q}_l \otimes \boldsymbol{Q}(\zeta_m), T/p^nT(1)) \xrightarrow{\partial} H^0(\boldsymbol{F}_l \otimes \boldsymbol{Z}[\zeta_m], T/p^nT).$$

(See 3.2 for the homomorphism ∂.)

Note that

$$\det_{\Lambda_{m,n}}(1 - \varphi_l : \Phi_{m,n} \to \Phi_{m,n}) = 0$$

because

$$\det_{\Lambda_{m,n}}(1 - l^{-1}\varphi_l : \Phi_{m,n} \to \Phi_{m,n}) = 0 \quad \text{and} \quad l \equiv 1 \bmod p^n$$

by (2.1.3) and (4.3.1). Hence

$$\psi_l : H^1(\boldsymbol{F}_l \otimes \boldsymbol{Z}[\zeta_m], T/p^nT) \to H^0(\boldsymbol{F}_l \otimes \boldsymbol{Z}[\zeta_m], T/p^nT)$$

is defined.

THEOREM 4.5. *Let m, n, n', r, l be as in* 4.4. *Assume*

$$H^0(\boldsymbol{F}_l(\zeta_{r/l}), T) = 0,$$

and assume that

$$l \equiv 1 \bmod r/l.$$

Then the image of $\kappa_{r/l}$ under

$$H^1\left(\boldsymbol{Z}\left[\zeta_m, \frac{1}{Nr/l}\right], T/p^nT\right) \to H^1(\boldsymbol{F}_l \otimes \boldsymbol{Z}[\zeta_m], T/p^nT)$$

$$\xrightarrow{\psi_l} H^0(\boldsymbol{F}_l \otimes \boldsymbol{Z}[\zeta_m], T/p^nT)$$

coincides with $\partial_l(\kappa_r)$.

To prove Theorem 4.5, we use the following Lemmas 4.6–4.8.

LEMMA 4.6. *Let R be a pro-finite commutative ring and let M be a free R-module of finite rank endowed with an R-linear continuous action of* $\mathrm{Gal}(\bar{\boldsymbol{F}}_l/\boldsymbol{F}_l)$.

Let $n \geq 1$ *and assume*

$$\det_R(1 - \varphi_l : M \to M) \equiv 0 \bmod p^n.$$

Assume R *is* p*-torsion free. Let* $\delta : H^0(\boldsymbol{F}_l, M/p^nM) \to H^1(\boldsymbol{F}_l, M)$ *be the connecting map of the exact sequence* $0 \to M \xrightarrow{p^n} M \to M/p^nM \to 0$. *Then the composite map*

$$H^1(\boldsymbol{F}_l, M) \to H^1(\boldsymbol{F}_l, M/p^nM) \xrightarrow{\psi_l} H^0(\boldsymbol{F}_l, M/p^nM) \xrightarrow{\delta} H^1(\boldsymbol{F}_l, M)$$

coincides with the map induced by

$$-p^{-n} \det_R(1 - \varphi_l : M \to M) : M \to M.$$

Proof. Let $u \in M$, and consider the class $\bar{u}$ of u in $H^1(\boldsymbol{F}_l, M) = M/\mathrm{Im}(1 - \varphi_l : M \to M)$. Then $\psi_l(u) \in H^0(\boldsymbol{F}_l, M/p^nM) \subset M/p^nM$ is $c_f u \bmod p^nM$ where c_f is the cofactor homomorphism of $f = 1 - \varphi_l$. Hence $\delta \circ \psi_l(u)$ is represented by the 1-cocycle $\mathrm{Gal}(\bar{\boldsymbol{F}}_l/\boldsymbol{F}_l) \to M$ which sends φ_l to $p^{-n}(\varphi_l - 1)c_f u = -p^{-n} \det_R(1 - \varphi_l) \cdot u$.

LEMMA 4.7. *Let the notation be as in* 2.2. *Then the image of* ω_r *in* $H^1(\boldsymbol{Q}_l \otimes L^{(r)}, T/p^{n'}T)$ *coincides with the image of*

$$\{p^{-n'} P_l(\sigma_{l,mr/l}^{-1})\} \cdot \omega_{r/l}.$$

Here, $P_l(\sigma_{l,mr/l}^{-1}) \equiv 1 \bmod p^{n'}$ because $P_l(\sigma_{l,m}^{-1}) \equiv 1 \bmod p^{n'}$ and $\sigma_{l,r/l} = \mathrm{id}$. (The last equation follows from the fact $l \equiv 1 \bmod r/l$.)

Proof of Lemma 4.7. Let s be a divisor of r/l. By Proposition 1.1, the image of z_{msl} in $H^1(\boldsymbol{Q}_l \otimes \boldsymbol{Q}(\zeta_{msl}), T)$ coincides with the image of

$$\{(l-1)^{-1}(P_l(l^{-1}\sigma_{l,mr/l}^{-1}) - P_l(\sigma_{l,mr/l}^{-1})\} \cdot z_{ms}. \tag{4.7.1}$$

From this we see that the image of v_{sl} in $H^1(\boldsymbol{Q}_l \otimes L^{(sl)}, T)$ coincides with the image of

$$\{p^{-n'}(P_l(l^{-1}\sigma_{l,mr/l}^{-1}) - P_l(\sigma_{l,mr/l}^{-1})\} \cdot v_s \in H^1(R^{(s)}, T).$$

This shows

CLAIM 4.7.2. *The image of* $v_{r,sl}$ *in* $H^1(\boldsymbol{Q}_l \otimes L^{(r)}, T)$ *is equal to the image of*

$$-\{p^{-n'}(P_l(l^{-1}\sigma_{l,mr/l}^{-1}) - P_l(\sigma_{l,mr/l}^{-1})\} \cdot v_{r/l,s} \in H^1(R^{(r/l)}, T).$$

On the other hand, by definition,

CLAIM 4.7.3. $v_{r,s}$ *coincides with the image of*

$$\{p^{-n'} P_l(l^{-1} \cdot (\sigma_{l,m}^{-1} \times 1))\} \cdot v_{r/l,s} = \{p^{-n'} P_l(l^{-1}\sigma_{l,mr/l}^{-1})\} \cdot v_{r/l,s}.$$

When we take the sum of Claims 4.7.2 and 4.7.3 in $H^1(\boldsymbol{Q}_l \otimes L^{(r)}, T)$, we obtain

CLAIM 4.7.4. *The image of* $v_{r,sl} + v_{r,s}$ *in* $H^1(\boldsymbol{Q}_l \otimes L^{(r)}, T)$ *coincides with the image of* $\{p^{-n'} P_l(\sigma_{l,mr/l}^{-1})\} \cdot v_{r/l,s}$.

We obtain Lemma 4.7 by taking the sum of Claim 4.7.4 for all s.

LEMMA 4.8. ω_r *belongs to*

$$\mathrm{Ker}(\mathrm{norm} : H^1(R^{(r)}, T) \to H^1(R^{(r/l)}, T)).$$

This follows from Lemma 2.5 and $\sigma_{l,r/l} = \mathrm{id}$.

4.9. Now we prove Theorem 4.5.

Let $G = G^{(l)}$, and consider the $\mathrm{Gal}(\bar{\boldsymbol{Q}}/L^{(r/l)})$-module

$$M = \boldsymbol{Z}[G] \otimes_{\boldsymbol{Z}} T$$

on which $\sigma \in \mathrm{Gal}(\bar{\boldsymbol{Q}}/L^{(r/l)})$ acts by $(\bar{\sigma})^{-1} \otimes \sigma$, where $\bar{\sigma}$ is the canonical image of σ in G. Consider the commutative diagram

$$\begin{array}{ccccc}
H^1(R^{(r/l)}, I_G M) & \xrightarrow{D} & H^1(R^{(r/l)}, G \otimes T) & \xrightarrow{D^{(r/l)}} & H^1(R^{(r/l)}, G \otimes T) \\
 & & \downarrow{\scriptstyle \partial_l} & & \downarrow{\scriptstyle \partial_l} \\
 & & H^0(\boldsymbol{F}_l \otimes R^{(r/l)}, T/p^{n'}) & \xrightarrow{D^{(r/l)}} & H^0(\boldsymbol{F}_l \otimes R^{(r/l)}, T/p^{n'}) \\
 & & \uparrow{\scriptstyle \psi_l} & & \uparrow{\scriptstyle \psi_l} \\
 & & H^1(\boldsymbol{F}_l \otimes R^{(r/l)}, T/p^{n'}) & \xrightarrow{D^{(r/l)}} & H^1(\boldsymbol{F}_l \otimes R^{(r/l)}, T/p^{n'}).
\end{array}$$

Here D is the map defined in 3.5 (we are considering the case $A = L^{(r/l)}$, $A' = R^{(r/l)}$, $B = L^{(r)}$, $B' = R^{(r)}$).

The composite of the two upper horizontal arrows sends

$$\omega_r \in H^1(R^{(r/l)}, I_G M) = \mathrm{Ker}(\mathrm{norm} : H^1(R^{(r)}, T) \to H^1(R^{(r/l)}, T))$$

(cf. Lemma 4.8) to $D^{(r)}(\omega_r)$. To prove Theorem 4.5, it is sufficient to show that $\partial_l(D^{(r)}(\omega_r)) \in H^0(\boldsymbol{F}_l \otimes R^{(r/l)}, T/p^{n'})$ coincides with the image of $-D^{(r/l)}(\omega_{r/l})$ under ψ_l. Hence by the above diagram, it is sufficient to prove that

$$\alpha \underset{\mathrm{def}}{=} \partial_l(D(\omega_r)) \in H^0(\boldsymbol{F}_l \otimes R^{(r/l)}, T/p^{n'}T)$$

coincides with the image β of $\omega_{r/l}$ under ψ_l.

The connecting map

$$\delta : H^0(\boldsymbol{F}_l \otimes R^{(r/l)}, T/p^{n'}T) \to H^1(\boldsymbol{F}_l \otimes R^{(r/l)}, T)$$

of the exact sequence $0 \to T \xrightarrow{p^{n'}} T \to T/p^{n'}T \to 0$ is injective since $H^0(\boldsymbol{F}_l \otimes R^{(r/l)}, T) = 0$. By Proposition 3.6 (which we apply by taking n' as n in Proposition 3.6), δ sends α to the image of $-\omega_r$ under the canonical map

$$H^1(R^{(r)}, T) \to H^1(\boldsymbol{F}_l \otimes R^{(r)}, T) \xleftarrow{\cong} H^1(\boldsymbol{F}_l \otimes R^{(r/l)}, T).$$

On the other hand, by Lemma 4.6 (which we apply by taking n' as n in Lemma 4.6), δ sends β to

$$-\{p^{-n'}P_l(\sigma_{l,mr/l}^{-1})\}\cdot\omega_{r/l}\in H^1(R^{(r/l)},T).$$

Hence by Lemma 4.7, δ sends α and β to the same element of $H^1(\boldsymbol{F}_l\otimes R^{(r/l)},T)$. Since δ is injective, we have $\alpha=\beta$.

§5. The condition (ii)

We consider effects of the condition (ii) in 0.6.

Let (F,T,N,N') be as in 0.1 and fix a divisor $d\geq 1$ of N. Let $V=F\otimes_{O_F}T$.

In §5, we assume that the condition (ii) in 0.6 is satisfied. That is, we assume that there exists an element σ of $\mathrm{Gal}(\bar{\boldsymbol{Q}}/\boldsymbol{Q}^{\mathrm{ab}})$ such that $\dim_F(\mathrm{Ker}(1-\sigma: V\to V))=1$. We fix such σ.

The aim of this section is to prove Proposition 5.5 which says that for a prime number l which is "good for (σ,m,n)" in the sense of 5.2, the map

$$\psi_l: H^1(\boldsymbol{F}_l\otimes\boldsymbol{Z}[\zeta_m],T/p^nT)\to H^0(\boldsymbol{F}_l\otimes\boldsymbol{Z}[\zeta_m],T/p^nT)$$

(cf. 4.4) is defined and is nearly an isomorphism, and the $\Lambda_{m,n}$-modules $H^q(\boldsymbol{F}_l\otimes\boldsymbol{Z}[\zeta_m],T/p^nT)$ for $q=0,1$ are nearly isomorphic to $\Lambda_{m,n}$.

5.1. We define some fields Ω,Ω', etc.

Let Ω be the extension of $\boldsymbol{Q}^{\mathrm{ab}}$ corresponding to the kernel of $\mathrm{Gal}(\bar{\boldsymbol{Q}}/\boldsymbol{Q}^{\mathrm{ab}})\to\mathrm{Aut}_{O_F}(T)$. Let Ω' be the fixed subfield of Ω by σ.

For $m,n\geq 1$, let $\Omega_{m,n}$ be the extension of $\boldsymbol{Q}(\zeta_m)$ corresponding to the kernel of $\mathrm{Gal}(\bar{\boldsymbol{Q}}/\boldsymbol{Q}(\zeta_m))\to\mathrm{Aut}_{O_F}(T/p^nT)$, and let $\Omega'_{m,n}$ be the fixed subfield of $\Omega_{m,n}$ by σ.

5.2. By a "good maximal ideal for (σ,m,n)", we mean a maximal ideal v of $O_{\Omega'_{m,n}}[1/(mN')]$ ($O_{\Omega'_{m,n}}$ denotes the integer ring of $\Omega'_{m,n}$) satisfying the following conditions (5.2.1) and (5.2.2).

(5.2.1) The Frobenius substitution of v in $\mathrm{Gal}(\Omega_{m,n}(\zeta_{p^n})/\Omega'_{m,n})$ coincides with the image of σ.

(5.2.2) v is of degree one over $\boldsymbol{Q}$. (That is, the local field of v is isomorphic to $\boldsymbol{Q}_l$ for some prime number l.)

By Chebotarev's density theorem, there are infinitely many good maximal ideals for (σ,m,n).

By a "good prime number for (σ,m,n)", we mean a prime number which lies under a good maximal ideal for (σ,m,n).

A good prime number l for (σ,m,n) satisfies $l\equiv 1 \bmod p^n$ because the Frobenius of l in $\mathrm{Gal}(\boldsymbol{Q}(\zeta_{p^n})/\boldsymbol{Q})$ coincides with the image of σ which is the identity element.

LEMMA 5.3. *If l is a good prime number for (σ, m, n),*

$$\det_{\Lambda_{m,n}}(1 - \varphi_l : \Phi_{m,n} \to \Phi_{m,n}) = 0$$

where $\Lambda_{m,n}$ and $\Phi_{m,n}$ are as in 4.3.

By Lemma 5.3 and 4.2, for a good prime number l for (σ, m, n),

$$\psi_l : H^1(\boldsymbol{F}_l \otimes \boldsymbol{Z}[\zeta_m], T/p^nT) \to H^0(\boldsymbol{F}_l \otimes \boldsymbol{Z}[\zeta_m], T/p^nT)$$

is defined.

Lemma 5.3 and (4.3.1) show that if (m, n, n') has the property (2.1.1) and if $r \geq 1$ is a square free integer whose all prime divisors are good prime numbers for (σ, m, n'), then the conditions (2.1.2) and (2.1.3) are satisfied and hence $\kappa_r \in H^1(\boldsymbol{Z}[\zeta_m, 1/Nr], T/p^n)$ is defined.

Proof of Lemma 5.3. Since l splits completely in $\boldsymbol{Q}(\zeta_m)/\boldsymbol{Q}$ by (5.2.2), we have the first equation in

$$\begin{aligned}
&\det_{\Lambda_{m,n}}(1 - \varphi_l : \Phi_{m,n} \to \Phi_{m,n}) \\
&\quad = \det_{O_F/p^n O_F}(1 - \varphi_l : T/p^nT \to T/p^nT) \\
&\quad = \det_{O_F/p^n O_F}(1 - \sigma : T/p^nT \to T/p^nT) \\
&\quad = \det_{O_F}(1 - \sigma : T \to T) \bmod p^n.
\end{aligned}$$

But

$$\det_{O_F}(1 - \sigma : T \to T) = \det_F(1 - \sigma : V \to V) = 0$$

since $1 - \sigma : V \to V$ has a non-trivial kernel.

5.4. Take O_F-homomorphisms

$$\mu : T \to O_F, \quad \nu : O_F \to T$$

such that $\mu \circ (1 - \sigma) = 0$, μ is surjective, and ν induces an isomorphism from O_F to $\mathrm{Ker}(1 - \sigma : T \to T)$.

For a good maximal ideal v for (σ, m, n) lying over a prime number l, we have $\Lambda_{m,n}$-homomorphisms

$$\mu_v : H^1(\boldsymbol{F}_l \otimes \boldsymbol{Z}[\zeta_m], T/p^nT) \to \Lambda_{m,n}$$

$$\nu_v : \Lambda_{m,n} \to H^0(\boldsymbol{F}_l \otimes \boldsymbol{Z}[\zeta_m], T/p^nT)$$

defined as follows. Let u be the maximal ideal of $\boldsymbol{Z}[\zeta_m, 1/N]$ lying under v. Since l splits completely in $\boldsymbol{Q}(\zeta_m)/\boldsymbol{Q}$ and the residue field $\boldsymbol{F}_v$ of v coincides with $\boldsymbol{F}_l$, we have canonical $\Lambda_{m,n}$-isomorphisms

$$\begin{aligned}
(*) \qquad H^q(\boldsymbol{F}_l \otimes \boldsymbol{Z}[\zeta_m], T/p^nT) &\xleftarrow{\cong} \Lambda_{m,n} \otimes H^q(\boldsymbol{F}_u, T/p^nT) \\
&\xrightarrow{\cong} \Lambda_{m,n} \otimes H^q(\boldsymbol{F}_v, T/p^nT)
\end{aligned}$$

for any q. The map μ induces $H^1(\boldsymbol{F}_v, T/p^nT) \to O_F/p^nO_F$ and the map v induces $O_F/p^nO_F \to H^0(\boldsymbol{F}_v, T/p^nT)$. These maps and the composite isomorphism in $(*)$ give the $\Lambda_{m,n}$-homomorphisms μ_v and ν_v. As is easily seen, the map μ_v is surjective and the map ν_v is injective.

PROPOSITION 5.5. (1) *There exists a non-zero integer t having the following property. For any $m, n \geq 1$, and for any good maximal ideal v for (σ, m, n) lying over a prime number l, t kills the kernels and the cokernels of the maps*

$$\psi_l : H^1(\boldsymbol{F}_l \otimes \boldsymbol{Z}[\zeta_m], T/p^nT) \to H^0(\boldsymbol{F}_l \otimes \boldsymbol{Z}[\zeta_m], T/p^nT)$$

$$\mu_v : H^1(\boldsymbol{F}_l \otimes \boldsymbol{Z}[\zeta_m], T/p^nT) \to \Lambda_{m,n}$$

$$\nu_v : \Lambda_{m,n} \to H^0(\boldsymbol{F}_l \otimes \boldsymbol{Z}[\zeta_m], T/p^nT).$$

(2) *Assume that the condition* $(\mathrm{ii}_{\mathrm{str}})$ *in* 0.6 *is satisfied, and assume that μ is choosen so that μ induces $T/(1-\sigma)T \xrightarrow{\cong} O_F$. Then for v and l as in* (1), *ψ_l, μ_v, and ν_v are bijective.*

PROPOSITION 5.6. *Let v be a good maximal ideal for (σ, m, n) lying over a prime number l. Let $t_1, t_2 \in \Lambda_{m,n}$, $a \in H^1(\boldsymbol{F}_l \otimes \boldsymbol{Z}[\zeta_m], T/p^nT)$, and r a multiple of l. Assume that t_1 kills the cokernel of $\psi_l : H^1(\boldsymbol{F}_l \otimes \boldsymbol{Z}[\zeta_m], T/p^nT) \to H^0(\boldsymbol{F}_l \otimes \boldsymbol{Z}[\zeta_m], T/p^nT)$, and t_2 kills the kernel of $\mu_v : H^1(\boldsymbol{F}_l \otimes \boldsymbol{Z}[\zeta_m], T/p^nT) \to \Lambda_{m,n}$. Assume also that if we identify $H^0(\boldsymbol{F}_l \otimes \boldsymbol{Z}[\zeta_m], T/p^nT)$ with $H^0(\boldsymbol{F}_l \otimes \boldsymbol{Z}[\zeta_m], T/p^nT(-1))$ by using a $\boldsymbol{Z}/p^n\boldsymbol{Z}$-basis of $H^0(\boldsymbol{F}_l, \boldsymbol{Z}/p^n\boldsymbol{Z}(1))$, then $\psi_l(a)$ belongs to $\partial_l(H^1(\boldsymbol{Z}[\zeta_m, 1/Nr], T/p^nT)$. Then $t_1t_2\mu_v(a)$ kills the cokernel of $\partial_l : H^1(\boldsymbol{Z}[\zeta_m, 1/Nr], T/p^nT) \to H^0(\boldsymbol{F}_l \otimes \boldsymbol{Z}[\zeta_m], T/p^nT(-1))$.*

(Note that if l is a good prime number for (σ, m, n), then $\boldsymbol{F}_l$ has a primitive p^n-th root of 1.)

We prove Proposition 5.5 in Lemmas 5.7, 5.8 and section 5.9 below, and prove Proposition 5.6 in 5.10 below.

LEMMA 5.7. *Let $\psi : T \to T$ be the cofactor homomorphism of $1 - \sigma : T \to T$. Then*

$$\psi = a \cdot \nu \circ \mu$$

for some element a of O_F such that

$$\text{(5.7.1)} \qquad \mathrm{length}_{O_F}(O_F/(a)) = \mathrm{length}_{O_F}(\mathrm{Ker}(T/(1-\sigma)T \xrightarrow{\mu} O_F)).$$

Proof. $\mathrm{Ker}(1 - \sigma : T \to T)$ is an O_F-direct summand of T, for the quotient $T/\mathrm{Ker}(1 - \sigma : T \to T)$ is embedded in T via $1 - \sigma$ and hence torsion free. Hence there exists an O_F-basis $(e_i)_{1 \leq i \leq r}$ of T such that $e_1 = \nu(1)$. On the other hand, there exists an O_F-basis $(e_i')_{1 \leq i \leq r}$ of T such that $\mu(e_1') = 1$ and such that $(e_i')_{2 \leq i \leq r}$ is an O_F-basis of $\mathrm{Ker}(\mu)$. From the definition of the cofactor homomorphism,

we have

$$\psi(e_i') = 0 \quad \text{for } 2 \leq i \leq r, \tag{5.7.2}$$

$$\psi(e_1') = ae_1 \quad \text{where } a \text{ is the element of } O_F \text{ satisfying} \tag{5.7.3}$$
$$e_1' \wedge (1-\sigma)e_2 \wedge \cdots \wedge (1-\sigma)e_r = a \cdot e_1 \wedge \cdots \wedge e_r.$$

Let b be the element of O_F such that

$$(1-\sigma)e_2 \wedge \cdots \wedge (1-\sigma)e_r = b \cdot e_2' \wedge \cdots \wedge e_r'. \tag{5.7.4}$$

Then

$$\text{length}_{O_F}(O_F/(b)) = \text{length}_{O_F}(\text{Ker}(T/(1-\sigma)T \xrightarrow{\mu} O_F)).$$

By taking $e_1' \wedge$ of (5.7.4), we have by (5.7.3)

$$a \cdot e_1 \wedge \cdots \wedge e_r = b \cdot e_1' \wedge \cdots \wedge e_r'.$$

Hence $a = b \cdot (\text{unit of } O_F)$.

LEMMA 5.8. *Let $\psi : T \to T$ be as in* 5.2. *Let a be an element of O_F satisfying the equation* (5.7.1), *and let c be an element of O_F which kills* $\text{Ker}(T/(1-\sigma)T \xrightarrow{\mu} O_F)$. *Then for any $n \geq 1$, we have*:

(1) *The map*

$$\text{Coker}(1-\sigma : T/p^n \to T/p^n) \xrightarrow{\mu} O_F/p^n$$

is surjective, and its kernel is killed by c.

(2) *The kernel and the cokernel of*

$$\psi : \text{Coker}(1-\sigma : T/p^n \to T/p^n) \to \text{Ker}(1-\sigma : T/p^n \to T/p^n)$$

are killed by ac.

(3) *The map*

$$O_F/p^n \xrightarrow{\nu} \text{Ker}(1-\sigma : T/p^n \to T/p^n)$$

is injective, and its cokernel is killed by c.

Proof. (1) and (3) are shown easily, and (2) is deduced from Lemma 5.7.

5.9. Now we can prove Proposition 5.5. By Lemma 5.8, the kernel and the cokernel of ψ_l are killed by ac, and the kernels of μ_v and ν_v and the cokernels of μ_v and ν_v are killed by c. Under the assumption of (ii), we can take $a = c = 1$.

5.10. We prove Proposition 5.6. Let $x \in H^0(\boldsymbol{F}_l \otimes \boldsymbol{Z}[\zeta_m], T/p^nT)$. Then $t_1 x = \psi_l(y)$ for some $y \in H^1(\boldsymbol{F}_l \otimes \boldsymbol{Z}[\zeta_m], T/p^nT)$. Since

$$\mu_v(\mu_v(a)y) = \mu_v(a)\mu_v(y) = \mu_v(\mu_v(y)a), \text{ we have}$$
$$t_2\mu_v(a)y = t_2\mu_v(y)a.$$

By applying ψ_l to the last equation, we obtain

$$t_1 t_2 \mu_v(a)x = t_2 \mu_v(y)\psi_l(a) \in \partial_l\left(H^1\left(\boldsymbol{Z}\left[\zeta_m, \frac{1}{Nr}\right], T/p^nT\right)\right).$$

§6. Preliminary on Galois cohomology I

The aim of §6 is to prove Proposition 6.1 concerning Galois cohomology of a Galois representation of $\mathrm{Gal}(\bar{\boldsymbol{Q}}/\boldsymbol{Q})$.

PROPOSITION 6.1. *Let (F, T, N) be as in* 0.1, *and let $V = \boldsymbol{Q} \otimes T$. Assume either one of the following* (i) (ii) *is satisfied.*

(i) *V is semi-simple and $H^0(\boldsymbol{Q}^{\mathrm{ab}}, V) = 0$.*

(ii) *$H^0(\boldsymbol{Q}^{\mathrm{ab}}, V) = V$.*

Fix a subfield Ξ of $\bar{\boldsymbol{Q}}$ such that $\mathrm{Gal}(\bar{\boldsymbol{Q}}/\Xi)$ is an open subgroup of $\mathrm{Ker}(\mathrm{Gal}(\bar{\boldsymbol{Q}}/\boldsymbol{Q}^{\mathrm{ab}}) \to \mathrm{Aut}(T))$ (the arrow is the action on T) and such that Ξ is Galois over $\boldsymbol{Q}$. Let

$$\tilde{\Lambda} = O_F[[\mathrm{Gal}(\boldsymbol{Q}^{\mathrm{ab}}/\boldsymbol{Q})]],$$

and let $\mathfrak{a} \subset \tilde{\Lambda}$ be the annihilator of the $\tilde{\Lambda}$-module $H^0(\boldsymbol{Q}^{\mathrm{ab}}, T)$ (so $\mathfrak{a}$ is $\tilde{\Lambda}$ in the case (i)). *Then there exists a finite number of open ideals $\mathfrak{b}_1, \ldots, \mathfrak{b}_r$ of $\tilde{\Lambda}$ such that the product ideal $\mathfrak{a}\mathfrak{b}_1 \cdots \mathfrak{b}_r$ annihilates the kernel of*

$$H^1(K, T/p^nT) \to H^1(\Xi, T/p^nT)$$

for any subfield K of $\boldsymbol{Q}^{\mathrm{ab}}$ and for any $n \geq 1$.

Here $H^1(K, T/p^nT)$ is regarded as a $\tilde{\Lambda}$-module in the natural way. The kernel in problem is a $\tilde{\Lambda}$-submodule of $H^1(K, T/p^nT)$.

We prove Proposition 6.1.

The image of $\mathrm{Gal}(\bar{\boldsymbol{Q}}/\boldsymbol{Q})$ in $\mathrm{Aut}(T)$ is a Lie group over $\boldsymbol{Q}_p$ ([Bo, Chapter III]). Let $\mathfrak{g}$ be the Lie algebra of this Lie group (loc. cit. §3), and let $\mathfrak{h} = [\mathfrak{g}, \mathfrak{g}]$.

For a sufficiently large finite Galois extension L of $\boldsymbol{Q}$ in $\bar{\boldsymbol{Q}}$, the Lie algebra of the image of $\mathrm{Gal}(\bar{\boldsymbol{Q}}/L^{\mathrm{ab}})$ in $\mathrm{Aut}(T)$ coincides with $\mathfrak{h}$. In the case (i), fix any such L. In the case (ii) ($\mathfrak{h} = 0$ in this case), take $L = \boldsymbol{Q}$. We prove the following two lemmas.

LEMMA 6.2. *$H^q(\mathrm{Gal}(\Xi L^{\mathrm{ab}}/L^{\mathrm{ab}}), T)$ is a finite group for any $q \geq 1$.*

LEMMA 6.3. *Let $\tilde{\Lambda}' = O_F[[\mathrm{Gal}(L^{\mathrm{ab}}/L)]]$, and let $\mathfrak{a}' \subset \tilde{\Lambda}'$ be the annihilator of the $\tilde{\Lambda}'$-module $H^0(L^{\mathrm{ab}}, T)$. Then in the case* (i), *the ideal $\mathfrak{a}'\tilde{\Lambda}$ of $\tilde{\Lambda}$ generated by the image of $\mathfrak{a}'$ is open.*

We prove Proposition 6.1 assuming Lemmas 6.2 and 6.3.

By Lemma 6.2, for each $q \geq 1$, there exists an open ideal $\mathfrak{c}'_q$ of $\tilde{\Lambda}'$ which annihilates $H^q(\mathrm{Gal}(\Xi L^{\mathrm{ab}}/L^{\mathrm{ab}}), T)$. Since $\tilde{\Lambda}' \to \tilde{\Lambda}$ is a finite morphism, the ideal

$\mathfrak{c}_q'\tilde{\Lambda}$ of $\tilde{\Lambda}$ generated by the image of $\mathfrak{c}_q'$ is an open ideal of $\tilde{\Lambda}$. On the other hand, since $\mathrm{Gal}(\boldsymbol{Q}^{\mathrm{ab}}L/\boldsymbol{Q}^{\mathrm{ab}})$ is a finite group, for each $q \geq 1$, there exists an open ideal $\mathfrak{c}_q$ of $\tilde{\Lambda}$ which annihilates $H^q(\mathrm{Gal}(\boldsymbol{Q}^{\mathrm{ab}}L/\boldsymbol{Q}^{\mathrm{ab}}), T)$. Let $\mathfrak{a}'$ be as in Lemma 6.3. Note $\mathfrak{a} = \mathfrak{a}'$ in the case (ii). We show that the ideal $(\mathfrak{a}'\tilde{\Lambda})(\mathfrak{c}_1'\tilde{\Lambda})^2(\mathfrak{c}_2'\tilde{\Lambda})\mathfrak{c}_1^2\mathfrak{c}_2$ annihilates the kernel of the map $H^1(K, T/p^nT) \to H^1(\Xi L^{\mathrm{ab}}, T/p^nT)$ for any subfield K of $\boldsymbol{Q}^{\mathrm{ab}}$ and for any $n \geq 1$. This implies Proposition 6.1 (by virtue of Lemma 6.3 in the case (i)). This map factors as

$$H^1(K, T/p^nT) \xrightarrow{(a)} H^1(KL, T/p^nT) \xrightarrow{(b)} H^1(\Xi L^{\mathrm{ab}}, T/p^nT).$$

We show that $\mathfrak{c}_1^2\mathfrak{c}_2$ kills the kernel of (a), and $\mathfrak{a}'(\mathfrak{c}_1')^2\mathfrak{c}_2'$ kills the kernel of (b).

We consider the kernel of (a). In the case (ii), (a) is the identity map and there is nothing to prove. So consider the case (i). The kernel of (a) is contained in the kernel of $H^1(K, T/p^nT) \to H^1(\boldsymbol{Q}^{\mathrm{ab}}L, T/p^nT)$ which is isomorphic to $H^1(\mathrm{Gal}(\boldsymbol{Q}^{\mathrm{ab}}L/K), T/p^nT)$. There is an exact sequence

$$0 \to H^1(\mathrm{Gal}(\boldsymbol{Q}^{\mathrm{ab}}/K), H^0(\boldsymbol{Q}^{\mathrm{ab}}, T/p^nT)) \to H^1(\mathrm{Gal}(\boldsymbol{Q}^{\mathrm{ab}}L/K), T/p^nT)$$
$$\to H^1(\mathrm{Gal}(\boldsymbol{Q}^{\mathrm{ab}}L/\boldsymbol{Q}^{\mathrm{ab}}), T/p^nT).$$

By the exact sequence

$$H^0(\boldsymbol{Q}^{\mathrm{ab}}, T) \longrightarrow H^0(\boldsymbol{Q}^{\mathrm{ab}}, T/p^nT) \longrightarrow H^1(\mathrm{Gal}(\boldsymbol{Q}^{\mathrm{ab}}L/\boldsymbol{Q}^{\mathrm{ab}}), T)$$
$$\xrightarrow{p^n} H^1(\mathrm{Gal}(\boldsymbol{Q}^{\mathrm{ab}}L/\boldsymbol{Q}^{\mathrm{ab}}), T) \longrightarrow H^1(\mathrm{Gal}(\boldsymbol{Q}^{\mathrm{ab}}L/\boldsymbol{Q}^{\mathrm{ab}}), T/p^nT)$$
$$\longrightarrow H^2(\mathrm{Gal}(\boldsymbol{Q}^{\mathrm{ab}}L/\boldsymbol{Q}^{\mathrm{ab}}), T)$$

and by the assumption $H^0(\boldsymbol{Q}^{\mathrm{ab}}, T) = 0$, $\mathfrak{c}_1$ kills $H^0(\boldsymbol{Q}^{\mathrm{ab}}, T/p^nT)$ and $\mathfrak{c}_1\mathfrak{c}_2$ kills $H^1(\mathrm{Gal}(\boldsymbol{Q}^{\mathrm{ab}}L/\boldsymbol{Q}^{\mathrm{ab}}), T/p^nT)$. Hence $\mathfrak{c}_1^2\mathfrak{c}_2$ kills $H^1(\mathrm{Gal}(L\boldsymbol{Q}^{\mathrm{ab}}/K), T/p^nT)$.

Next we consider the kernel of (b). It is isomorphic to $H^1(\mathrm{Gal}(\Xi L^{\mathrm{ab}}/KL), T/p^nT)$. There is an exact sequence

$$0 \to H^1(\mathrm{Gal}(L^{\mathrm{ab}}/KL), H^0(L^{\mathrm{ab}}, T/p^nT)) \to H^1(\mathrm{Gal}(\Xi L^{\mathrm{ab}}/KL), T/p^nT)$$
$$\to H^1(\mathrm{Gal}(\Xi L^{\mathrm{ab}}/L^{\mathrm{ab}}), T/p^nT).$$

We have an exact sequence

$$H^0(L^{\mathrm{ab}}, T) \longrightarrow H^0(L^{\mathrm{ab}}, T/p^nT)$$
$$\longrightarrow H^1(\mathrm{Gal}(\Xi L^{\mathrm{ab}}/L^{\mathrm{ab}}), T) \xrightarrow{p^n} H^1(\mathrm{Gal}(\Xi L^{\mathrm{ab}}/L^{\mathrm{ab}}), T)$$
$$\longrightarrow H^1(\mathrm{Gal}(\Xi L^{\mathrm{ab}}/L^{\mathrm{ab}}), T/p^nT) \longrightarrow H^2(\mathrm{Gal}(\Xi L^{\mathrm{ab}}/L^{\mathrm{ab}}), T)$$

where $H^q(\mathrm{Gal}(\Xi L^{\mathrm{ab}}/L^{\mathrm{ab}}), T)$ denotes $\varprojlim_i H^q(\mathrm{Gal}(\Xi L^{\mathrm{ab}}/L^{\mathrm{ab}}), T/p^iT)$. (Since $\mathrm{Gal}(\Xi L^{\mathrm{ab}}/L^{\mathrm{ab}}) \to \mathrm{Aut}(T)$ has finite kernel, $\mathrm{Gal}(\Xi L^{\mathrm{ab}}/L^{\mathrm{ab}})$ is a Lie group over $\boldsymbol{Q}_p$. Hence $H^q(\mathrm{Gal}(\Xi L^{\mathrm{ab}}/L^{\mathrm{ab}}), T/p^iT)$ are finite groups for all q and i by [La]. The above sequence is exact because the inverse limits for filtered inverse systems of finite sets preserve exactness.) Hence $\mathfrak{a}'\mathfrak{c}_1'$ kills $H^0(L^{\mathrm{ab}}, T/p^nT)$ and $\mathfrak{c}_1'\mathfrak{c}_2'$ kills

$H^1(\mathrm{Gal}(\Xi L^{\mathrm{ab}}/L^{\mathrm{ab}}), T/p^nT)$. Hence $\mathfrak{a}'(\mathfrak{c}_1')^2\mathfrak{c}_2'$ kills

$$H^1(\mathrm{Gal}(\Xi L^{\mathrm{ab}}/KL), T/p^nT).$$

It remains to prove Lemmas 6.2 and 6.3.

6.4. We prove Lemma 6.2. Let $q \geq 1$. Since $H^q(\mathrm{Gal}(\Xi L^{\mathrm{ab}}/L^{\mathrm{ab}}), T)$ is a finitely generated O_F-module, it is sufficient to prove that $H^q(\mathrm{Gal}(\Xi L^{\mathrm{ab}}/L^{\mathrm{ab}}), V) = \boldsymbol{Q} \otimes H^q(\mathrm{Gal}(\Xi L^{\mathrm{ab}}/L^{\mathrm{ab}}), T)$ is zero. Since the Lie algebra of $\mathrm{Gal}(\Xi L^{\mathrm{ab}}/L^{\mathrm{ab}})$ coincides with $\mathfrak{h}$, $H^q(\mathrm{Gal}(\Xi L^{\mathrm{ab}}/L^{\mathrm{ab}}), V)$ is embedded in $H^q(\mathfrak{h}, V)$ by [La, Chapter 5, Theorem 2.4.10]. As we will see below, $\mathfrak{h}$ is a semi-simple Lie algebra, and this implies $H^q(\mathfrak{h}, V) = 0$ ([CE]).

The semi-simplicity of $\mathfrak{h}$ can be proved as follows. In the case (ii), we have $\mathfrak{h} = 0$ and hence is semi-simple. Consider the case (i). V is regarded as a $\mathfrak{g}$-module and is a semi-simple representation of $\mathfrak{g}$. (The last fact follows from

$$\{\mathfrak{g}\text{-submodules of } V\}$$
$$= \{\boldsymbol{Q}_p\text{-submodules of } V \text{ which are stable under the action of some open subgroup of } \mathrm{Gal}(\bar{\boldsymbol{Q}}/\boldsymbol{Q})\}$$

([La]) and from the fact that V is semi-simple as a representation of any open subgroup of $\mathrm{Gal}(\bar{\boldsymbol{Q}}/\boldsymbol{Q})$ over $\boldsymbol{Q}_p$.) Since $\mathfrak{g}$ has a semi-simple faithful representation, $\mathfrak{h} = [\mathfrak{g}, \mathfrak{g}]$ is a semi-simple Lie algebra ([Bo, Chapter I, §6 Proposition 5]).

6.5. We prove Lemma 6.3. Assume we are in the case (i). Let I be the kernel of $\tilde{\Lambda}' \to \tilde{\Lambda}$. It is enough to show that $\tilde{\Lambda}'/(\mathfrak{a}' + I)$ is a finite group. The ring $\tilde{\Lambda}'/\mathfrak{a}'$ is finitely generated as an O_F-module since it is embedded in $\mathrm{End}_{O_F}(H^0(L^{\mathrm{ab}}, T))$. Since V is semi-simple, $\boldsymbol{Q} \otimes \tilde{\Lambda}'/\mathfrak{a}$ is a product of fields. Since the $\boldsymbol{Q} \otimes \tilde{\Lambda}'/\mathfrak{a}'$-module $\boldsymbol{Q} \otimes \tilde{\Lambda}'/(\mathfrak{a}' + I)$ has no non-trivial homomorphism into the faithful $\boldsymbol{Q} \otimes \tilde{\Lambda}'/\mathfrak{a}'$-module V as is seen by

$$0 = H^0(\boldsymbol{Q}^{\mathrm{ab}}, V) = \mathrm{Hom}_{\tilde{\Lambda}'}(\tilde{\Lambda}'/I, V)$$
$$= \mathrm{Hom}_{\boldsymbol{Q} \otimes \tilde{\Lambda}'/\mathfrak{a}'}(\boldsymbol{Q} \otimes \tilde{\Lambda}'/(\mathfrak{a}' + I), V),$$

we have $\boldsymbol{Q} \otimes \Lambda'/(\mathfrak{a}' + I) = 0$. This proves the finiteness of $\tilde{\Lambda}'/(\mathfrak{a}' + I)$.

Remark 6.6. I learned the method to use the cohomology theory of Lie algebras as above for the study of Galois cohomology, from Serre [Se_3], and also from Jannsen [Ja] in which (§4, Theorem 3) Serre's results in [Se_3] are applied to obtain results on Galois cohomology.

§7. Preliminary on Galois cohomology II

In this §7, we review the duality theory (cf. 7.1) for étale cohomology in number theory and the localizing exact sequence (cf. 7.2), and relate them in Proposition 7.7 to Proposition 6.2.

Let (F, T, N, N') be as in 0.1.

7.1. We review a duality theory of Tate, Poitou, Artin, Verdier, Mazur ([AV], [Ma], [Se$_2$, Chapter II, §6]).

Let K be a finite extension of $\boldsymbol{Q}$, $M \geq 1$ a multiple of N, and let $P = P(K, M)$ be the set of all places of K which are either archimedean or finite places dividing M. Then there exists an exact sequence

$$\begin{aligned}
0 &\to H^0\left(O_K\left[\frac{1}{M}\right], T/p^n\right) \to \bigoplus_{v \in P} \hat{H}^0(K_v, T/p^n) \\
&\to \mathrm{Hom}_{O_F}\left(H^2\left(O_K\left[\frac{1}{M}\right], T^*(1)/p^n\right), O_F/p^n\right) \\
&\to H^1\left(O_K\left[\frac{1}{M}\right], T/p^n\right) \to \bigoplus_{v \in P} H^1(K_v, T/p^n) \\
&\to \mathrm{Hom}_{O_F}\left(H^1\left(O_K\left[\frac{1}{M}\right], T^*(1)/p^n\right), O_F/p^n\right) \\
&\to H^2\left(O_K\left[\frac{1}{M}\right], T/p^n\right) \to \bigoplus_{v \in P} H^2(K_v, T/p^n) \\
&\to \mathrm{Hom}_{O_F}\left(H^0\left(O_K\left[\frac{1}{M}\right], T^*(1)/p^n\right), O_F/p^n\right) \to 0.
\end{aligned}$$

Here T^* denotes $\mathrm{Hom}_{O_F}(T, O_F)$ which is endowed with the dual action of $\mathrm{Gal}(\bar{\boldsymbol{Q}}/\boldsymbol{Q})$, K_v denotes the completion of K at v, $\hat{H}^0(K_v, \ ) = H^0(K_v, \ )$ if v is a finite place, $\hat{H}^0(K_v, \ ) = 0$ if v is a complex place, and $\hat{H}^0(K_v, \ )$ is the cokernel of the norm: $H^0(\bar{K}_v, \ ) \to H^0(K_v, \ )$ if v is a real place.

7.2. For a finite extension K of $\boldsymbol{Q}$ and for a multiple M of N, the exact sequence of étale cohomology for $\mathrm{Spec}(K) \to \mathrm{Spec}(O_K[1/M])$ (the localizing exact sequence) has the form

$$\begin{aligned}
&\cdots \longrightarrow H^1\left(O_K\left[\frac{1}{M}\right], T/p^n\right) \longrightarrow H^1(K, T/p^n) \xrightarrow{(\partial_v)_v} \bigoplus_v H^0(\boldsymbol{F}_v, T(-1)/p^n) \\
&\xrightarrow{(\iota_v)_v} H^2\left(O_K\left[\frac{1}{M}\right], T/p^n\right) \longrightarrow \cdots.
\end{aligned}$$

where v ranges over all finite places of K which do not divide M, and $\boldsymbol{F}_v$ denotes the residue field of v for each v. The map ∂_v is defined by 3.2.

Concerning the relation of the localizing exact sequence with the duality in 7.1, the map ι_v coincides with the composite

$$\begin{aligned}
H^0(\boldsymbol{F}_v, T(-1)/p^n) &\xrightarrow{\cong} \mathrm{Hom}_{O_F}(H^1(\boldsymbol{F}_v, T^*(1)/p^n), O_F/p^n) \\
&\longrightarrow \mathrm{Hom}_{O_F}\left(H^1\left(O_K\left[\frac{1}{M}\right], T^*(1)/p^n\right), O_F/p^n\right) \\
&\longrightarrow H^2\left(O_K\left[\frac{1}{M}\right], T/p^n\right)
\end{aligned}$$

where the first arrow is induced by the cup product to $H^1(\boldsymbol{F}_v, O_F/p^n) \cong O_F/p^n$, the second arrow is induced by $H^1(O_K[1/M], T/p^n) \to H^1(\boldsymbol{F}_v, T/p^n)$, and the third arrow is the map in 7.1.

7.3. Let $n \geq 1$, M a multiple of N, K a finite extension of $\boldsymbol{Q}$ in $\bar{\boldsymbol{Q}}$, L an extension of K in $\bar{\boldsymbol{Q}}$, and let $\gamma \in H^0(L, T^*/p^n)$ (resp. $\gamma \in H^0(L, T/p^n)$). We define homomorphisms

$$\alpha_{n,M}(L/K, T, \gamma) : \mathrm{Gal}(L^{\mathrm{ab}}/L) \to \mathrm{Hom}_{O_F}\left(H^1\left(O_K\left[\frac{1}{M}\right], T/p^n\right), O_F/p^n\right)$$

$$\left(\text{resp. } \beta_{n,M}(L/K, T, \gamma) : \mathrm{Gal}(L^{\mathrm{ab}}/L) \to \mathrm{Ker}\left(H^2\left(O_K\left[\frac{1}{M}\right], T(1)/p^n\right) \to \bigoplus_{v \in P(K,M)} H^2(K_v, T/p^n)\right)\right)$$

as the map induced by the composite map

$$H^1\left(O_K\left[\frac{1}{M}\right], T/p^n\right) \to H^1(L, T/p^n) \xrightarrow{\gamma} H^1(L, O_F/p^n) \cong \mathrm{Hom}_{\mathrm{cont}}(\mathrm{Gal}(L^{\mathrm{ab}}/L), O_F/p^n).$$

(resp. as the composite of $\alpha_{n,M}(L/K, T^*(1), \gamma)$ with the map

$$\mathrm{Hom}_{O_F}\left(H^1\left(O_K\left[\frac{1}{M}\right], T^*(1)/p^n\right), O_F\right) \to H^2\left(O_K\left[\frac{1}{M}\right], T(1)/p^n\right) \quad \text{(cf. 7.1)}.$$

By the definitions, the map $\alpha_{n,M}(L/K, T, \gamma)$ (resp. $\beta_{n,M}(L/K, T, \gamma)$) factors through the canonical surjection

$$\mathrm{Gal}(L^{\mathrm{ab}}/L) \to \Pi_M(L) \underset{\mathrm{def}}{=} \mathrm{Hom}\left(H^1\left(O_L\left[\frac{1}{M}\right], \boldsymbol{Q}/\boldsymbol{Z}\right), \boldsymbol{Q}/\boldsymbol{Z}\right) = \mathrm{Gal}(\tilde{L}/L)$$

where $\tilde{L}$ is the maximal abelian extension of L which is unramified outside prime divisors of M.

7.4. We give a preliminary argument. For a finite group G, a ring R, and an $R[G]$-module X, there exists a canonical isomorphism

$$\mathrm{Hom}_R(X, R) \cong \mathrm{Hom}_{R[G]}(X, R[G])$$

which sends $h \in \mathrm{Hom}_R(X, R)$ to $x \mapsto \sum_{\alpha \in G} h(\alpha^{-1}x)\alpha$.

7.5. Assume that the conditions (i), (ii) in 0.6 are satisfied.

Let σ be an element of $\mathrm{Gal}(\bar{\boldsymbol{Q}}/\boldsymbol{Q}^{\mathrm{ab}})$ such that $\dim_F(\mathrm{Ker}(1 - \sigma : V \to V)) = 1$. Take O_F-homomorphisms $\mu : T \to O_F$ and $\nu : O_F \to T$ satisfying the con-

ditions in 5.4. Fix a $\boldsymbol{Z}_p$-basis η of $\boldsymbol{Z}_p(1)$. Let the notations $\Omega, \Omega', \Omega_{m,n}$, $\Omega'_{m,n} (m, n \geq 1)$ be as in 5.1. Let $\Lambda_{m,n} = (O_F/p^n)[\mathrm{Gal}(\boldsymbol{Q}(\zeta_m)/\boldsymbol{Q})]$ as before.

The following maps will be important in later sections:

(7.5.1) $\alpha_{n,M}(\Omega'_{m,n}/\boldsymbol{Q}(\zeta_m), T, \mu)$:

$$\Pi_M(\Omega'_{m,n}) \to \mathrm{Hom}_{\Lambda_{m,n}}\left(H^1\left(\boldsymbol{Z}\left[\zeta_m, \frac{1}{M}\right], T/p^n\right), \Lambda_{m,n}\right)$$

(7.5.2) $\beta_{n,M}(\Omega'_{m,n}/\boldsymbol{Q}(\zeta_m), T, v\eta^{-1})$:

$$\Pi_M(\Omega'_{m,n}) \to \mathrm{Ker}\left(H^2\left(\boldsymbol{Z}\left[\zeta_m, \frac{1}{M}\right], T/p^n\right) \to \bigoplus_{v \in P} H^2(\boldsymbol{Q}(\zeta_m)_v, T/p^n)\right)$$

(M is a multiple of N, $P = P(\boldsymbol{Q}(\zeta_m), M)$). Here we identify the target group $\mathrm{Hom}_{\Lambda_{m,n}}(H^1(\boldsymbol{Z}[\zeta_m, 1/M], T/p^n), \Lambda_{m,n})$ of (7.5.1) with the target group $\mathrm{Hom}_{O_F}(H^1(\boldsymbol{Z}[\zeta_m, 1/M], T/p^n), O_F/p^n)$ in 7.3 via the isomorphism in 7.4.

We give statements 7.6 and 7.7 concerning the maps (7.5.1) and (7.5.2). In Proposition 7.7, let $\langle \mu \rangle$ (resp. $\langle v \rangle$) be the $O_F[\mathrm{Gal}(\bar{\boldsymbol{Q}}/\boldsymbol{Q})]$-submodule of T^* (resp. T) generated by μ (resp. by the image of v). By the condition (i), there exists a non-zero integer which kills $T^*/\langle \mu \rangle$ and $T/\langle v \rangle$.

LEMMA 7.6. *Let v be a good maximal ideal for (σ, m, n) which does not divide M, and let l be the prime number lying under v. Then:*

(1) *The map* (7.5.1) *sends the Frobenius of v in $\Pi_M(\Omega'_{m,n})$ to the composite homomorphism*

$$H^1\left(\boldsymbol{Z}\left[\zeta_m, \frac{1}{M}\right], T/p^n\right) \to H^1(\boldsymbol{F}_l \otimes \boldsymbol{Z}[\zeta_m], T/p^n) \xrightarrow{\mu_v} \Lambda_{m,n}.$$

(2) *The map* (7.5.2) *sends the Frobenius of v in $\Pi_M(\Omega'_{m,n})$ to the image of $1 \in \Lambda_{m,n}$ under*

$$\Lambda_{m,n} \xrightarrow{v_v \eta^{-1}} H^0(\boldsymbol{F}_l \otimes \boldsymbol{Z}[\zeta_m], T/p^n(-1)) \xrightarrow{\partial_l} H^2\left(\boldsymbol{Z}\left[\zeta_m, \frac{1}{M}\right], T/p^n\right)$$

where ∂_l is the sum of ∂_u for prime divisors u of l in $\boldsymbol{Q}(\zeta_m)$.

Lemma 7.6 (1) is easily shown, and Lemma 7.6 (2) follows from the description of ∂_v in 7.2.

PROPOSITION 7.7. *Let the assumptions and the notations be as in* 7.5. *Let c be a non-zero integer which kills $T^*/\langle \mu \rangle$ and $T/\langle v \rangle$. Fix a finite extension Ξ of Ω such that Ξ is Galois over $\boldsymbol{Q}$, and consider the $\Lambda_{m,n}$-homomorphisms*

(7.7.1) $$\Lambda_{m,n} \otimes \mathrm{Gal}(\Xi^{\mathrm{ab}}/\Xi) \to \mathrm{Hom}_{\Lambda_{m,n}}\left(H^1\left(\boldsymbol{Z}\left[\zeta_m, \frac{1}{M}\right], T/p^n\right), \Lambda_{m,n}\right)$$

$$(7.7.2)\qquad \Lambda_{m,n}\otimes \mathrm{Gal}(\Xi^{\mathrm{ab}}/\Xi) \to \mathrm{Ker}\left(H^2\left(\boldsymbol{Z}\left[\zeta_m,\frac{1}{M}\right],T/p^n\right)\to \bigoplus_{v\in P} H^2(\boldsymbol{Q}(\zeta_m)_v,T/p^n)\right)$$

$$(P=P(\boldsymbol{Q}(\zeta_m),M)$$

induced by (7.5.1) *and* (7.5.2), *respectively. Let* $\tilde{\Lambda}=O_F[[\mathrm{Gal}(\boldsymbol{Q}^{\mathrm{ab}}/\boldsymbol{Q})]]$, *and let* $\mathfrak{a}\subset\tilde{\Lambda}$ *be the annihilator of the* $\tilde{\Lambda}$*-module* $H^0(\boldsymbol{Q}^{\mathrm{ab}},T)$ (*resp.* $H^0(\boldsymbol{Q}^{\mathrm{ab}},T^*(1))$). *Then there exists a finite number of open ideals* $\mathfrak{b}_1,\dots,\mathfrak{b}_r$ *of* $\tilde{\Lambda}$ *such that the product ideal* $\mathfrak{c}\mathfrak{a}\mathfrak{b}_1\cdots\mathfrak{b}_r$ *kills the cokernels of* (7.7.1) (*resp.* (7.7.2)) *for any* $m,n\geq 1$ *and for any multiple* M *of* N.

Remark 7.8. In Proposition 7.7, since we assumed that V is simple (the condition (i) in 0.6), $H^0(\boldsymbol{Q}^{\mathrm{ab}},T)$ is either zero or T itself. If $H^0(\boldsymbol{Q}^{\mathrm{ab}},T)=0$, then $\mathfrak{a}=\tilde{\Lambda}$.

7.9. We prove Proposition 7.7. We consider the statement for (7.7.1). We apply Proposition 6.1. Let $\mathfrak{b}_1,\dots,\mathfrak{b}_r$ be open ideals of $\tilde{\Lambda}$ having the property stated in Proposition 6.1. We prove below that $\mathfrak{c}\mathfrak{a}\mathfrak{b}_1\cdots\mathfrak{b}_r$ kills the cokernel of (7.7.1).

For the statement for (7.7.2), if we take $\mathfrak{b}_1,\dots,\mathfrak{b}_r$ for $T^*(1)$, the same argument shows that $\mathfrak{c}\mathfrak{a}\mathfrak{b}_1\cdots\mathfrak{b}_r$ kills the cokernel of the $\Lambda_{m,n}$-homomorphism

$$\Lambda_{m,n}\otimes\mathrm{Gal}(\Xi^{\mathrm{ab}}/\Xi)\to \mathrm{Hom}_{\Lambda_{m,n}}\left(H^1\left(\boldsymbol{Z}\left[\zeta_m,\frac{1}{M}\right],T^*(1)/p^n\right),\Lambda_{m,n}\right)$$

induced by $\alpha_{n,M}(\Omega'_{m,n}/\boldsymbol{Q}(\zeta_m),T^*(1),v\eta^{-1})$, and this implies that $\mathfrak{c}\mathfrak{a}\mathfrak{b}_1\cdots\mathfrak{b}_r$ kills the cokernel of (7.7.2).

Now consider the homomorphism (7.7.1). By Proposition 6.1 and the injectivity of $H^1(\boldsymbol{Z}[\zeta_m,1/M],T/p^n)\to H^1(\boldsymbol{Q}(\zeta_m),T/p^n)$ and by duality, $\mathfrak{a}\mathfrak{b}_1\cdots\mathfrak{b}_r$ kills the cokernel of

$$(7.9.1)\quad \Lambda_{m,n}\otimes T^*\otimes\mathrm{Gal}(\Xi^{\mathrm{ab}}/\Xi)\to \mathrm{Hom}_{\Lambda_{m,n}}\left(H^1\left(\boldsymbol{Z}\left[\zeta_m,\frac{1}{M}\right],T/p^n\right),\Lambda_{m,n}\right).$$

For $\tau\in\mathrm{Gal}(\bar{\boldsymbol{Q}}/\boldsymbol{Q})$, let $\bar{\tau}$ be the canonical image of τ in $\mathrm{Gal}(\boldsymbol{Q}(\zeta_m)/\boldsymbol{Q})\subset\Lambda_{m,n}$. Then we see easily that for any $x\in\Lambda_{m,n}$, $y\in T^*$, $z\in\mathrm{Gal}(\Xi^{\mathrm{ab}}/\Xi)$, and $\tau\in\mathrm{Gal}(\bar{\boldsymbol{Q}}/\boldsymbol{Q})$, the image of $\bar{\tau}^{-1}x\otimes\tau y\otimes\tau z\tau^{-1}$ under (7.9.1) coincides with that of $x\otimes y\otimes z$. Let $x\in\Lambda_{m,n}$, $y\in T^*$, $z\in\mathrm{Gal}(\Xi^{\mathrm{ab}}/\Xi)$. Then we have $cy=\sum_\tau a_\tau\cdot\tau\mu$ for some finite family (τ) of elements of $\mathrm{Gal}(\bar{\boldsymbol{Q}}/\boldsymbol{Q})$ and for some $a_\tau\in O_F$. The image of $c\cdot(x\otimes y\otimes z)$ under (7.9.1) coincides with that of $\sum_\tau a_\tau\bar{\tau}x\otimes\mu\otimes\tau^{-1}z\tau$, i.e. with the image of $\sum_\tau a_\tau\bar{\tau}x\otimes\tau^{-1}z\tau$ under (7.7.1).

§8. A finiteness result

The aim of §8 is to prove the following finiteness result Theorem 8.1 under a certain additional assumption "$w\neq 0,-2$". A complete proof of Theorem 8.1

will be given in §13. In fact, in §13, we prove a finiteness result Theorem 13.3 which is a little stronger than Theorem 8.1.

THEOREM 8.1. *Let* (F, T, N, N') *be as in* 0.1, *and let* $(z_m)_m$ *be an Euler system for* (F, T, N). *Assume that the conditions* (i), (ii), (iii), *in* 0.6 *are satisfied, and that the image of* ξ (*cf.* 0.7) *in* $H^1(\boldsymbol{Z}[1/N], T)$ *is not a torsion element. Then the kernel of*

$$H^2\left(\boldsymbol{Z}\left[\frac{1}{N}\right], T\right) \to \bigoplus_{l|N} H^2(\boldsymbol{Q}_l, T)$$

is finite.

COROLLARY 8.2. *Under the assumption in Theorem* 8.1, *if* $H^0(\boldsymbol{Q}_l, V^*(1)) = 0$ *for any prime divisor* l *of* N, *then* $H^2(\boldsymbol{Z}[1/N], T)$ *is a finite group.*

(*Here* $V^* = \mathrm{Hom}_F(V, F)$ *endowed with the dual action of* $\mathrm{Gal}(\bar{\boldsymbol{Q}}/\boldsymbol{Q})$.)

Corollary 8.2 follows from Theorem 8.1 and from the local Tate duality which says that $\boldsymbol{Q} \otimes H^2(\boldsymbol{Q}_l, T)$ is the dual F-vector space of $H^0(\boldsymbol{Q}_l, V^*(1))$.

In this §8, we prove Theorem 8.1 under the assumption that the integer w in the condition (iii) in 0.6 for V satisfies $w \neq 0, -2$.

8.3. Assuming that the condition (ii) in 0.6 is satisfied, we fix $\sigma \in \mathrm{Gal}(\bar{\boldsymbol{Q}}/\boldsymbol{Q}^{\mathrm{ab}})$ such that $\dim_F(\mathrm{Ker}(\sigma - 1; V \to V)) = 1$ and O_F-homomorphisms $\mu : T \to O_F$ and $\nu : O_F \to T$ satisfying the conditions in 5.4. Fix a basis η of $\boldsymbol{Z}_p(1)$. Let

$$\alpha : \mathrm{Gal}(\Omega^{\mathrm{ab}}/\Omega) \to \mathrm{Hom}_{O_F}\left(H^1\left(\boldsymbol{Z}\left[\frac{1}{N}\right], T\right), O_F\right)$$

$$\beta : \mathrm{Gal}(\Omega^{\mathrm{ab}}/\Omega) \to \mathrm{Ker}\left(H^2\left(\boldsymbol{Z}\left[\frac{1}{N}\right], T\right) \to \bigoplus_{l|N} H^2(\boldsymbol{Q}_l, T)\right)$$

be the homomorphism induced by the case $m = 1$, $M = N$ of (7.5.1) and (7.5.2), respectively.

LEMMA 8.4. *Assume that the conditions* (i) *and* (ii) *with* $w \neq 0, -2$ *in* 0.6 *are satisfied. Then* $\mathrm{Coker}(\alpha)$ *and* $\mathrm{Coker}(\beta)$ *are finite groups.*

Proof. If $H^0(\boldsymbol{Q}^{\mathrm{ab}}, T) = 0$, this follows from Proposition 7.7.

Assume $H^0(\boldsymbol{Q}^{\mathrm{ab}}, T) \neq 0$. Then $\mathrm{Gal}(\bar{\boldsymbol{Q}}/\boldsymbol{Q}^{\mathrm{ab}})$ acts trivially on T (cf. 7.8). Let $\varepsilon : \tilde{\Lambda} \to O_F$ be the unique continuous O_F-homomorphism which sends all elements of $\mathrm{Gal}(\boldsymbol{Q}^{\mathrm{ab}}/\boldsymbol{Q})$ in $\tilde{\Lambda}$ to $1 \in O_F$. If the annihilator $I \subset \tilde{\Lambda}$ of the $\tilde{\Lambda}$-module $T \oplus T^*(1)$ satisfies $\varepsilon(I) \neq 0$, then Lemma 8.4 follows from Proposition 7.7. If $\varepsilon(I) = 0$, then $T = O_F$ (with the trivial action of $\mathrm{Gal}(\bar{\boldsymbol{Q}}/\boldsymbol{Q})$) or $T = O_F(1)$. But this contradicts the assumption $w \neq 0, -2$.

PROPOSITION 8.5. *Let* (F, T, N, N') *be as in* 0.1, *and let* $(z_m)_m$ *be an Euler system for* (F, T, N, N'). *Assume that the conditions* (ii) *and* (iii) *with* $w \neq 0, -2$ *in* 0.6 *are satisifed. Let* $\bar{\xi}$ *be the image of* ξ *in* $H^1(\boldsymbol{Z}[1/N], T)$. *Then*:

$$(1) \qquad \alpha(x)(\bar{\xi}) \cdot \beta(x) \in H^2\left(\boldsymbol{Z}\left[\frac{1}{N}\right], T\right)_{\mathrm{tor}} \quad \textit{for any } x \in \mathrm{Gal}(\Omega^{\mathrm{ab}}/\Omega)$$

where $\alpha(x)(\bar{\xi}) \in O_F$ *means the image of* $\bar{\xi}$ *under the homomorphism* $\alpha(x)$, *and* $H^2(\boldsymbol{Z}[1/N], T)_{\mathrm{tor}}$ *denotes the torsion part of* $H^2(\boldsymbol{Z}[1/N], T)$.

$$(2) \quad \alpha(x)(\bar{\xi}) \cdot \beta(y) + \alpha(y)(\bar{\xi}) \cdot \beta(x) \in H^2\left(\boldsymbol{Z}\left[\frac{1}{N}\right], T\right)_{\mathrm{tor}} \quad \textit{for any } x, y \in \mathrm{Gal}(\Omega^{\mathrm{ab}}/\Omega).$$

8.6. We deduce the case $w \neq 0, -2$ of Theorem 8.1 from Proposition 8.5. Since $\mathrm{Coker}(\alpha)$ is finite (cf. Lemma 8.4) and $\bar{\xi}$ is not a torsion element, there exists $x \in \mathrm{Gal}(\Omega^{\mathrm{ab}}/\Omega)$ such that $\alpha(x)(\bar{\xi}) \neq 0$. By Proposition 8.5 (1), this shows $\beta(x) \in H^2(\boldsymbol{Z}[1/N], T)_{\mathrm{tor}}$. Let y be any element of $\mathrm{Gal}(\Omega^{\mathrm{ab}}/\Omega)$. By Proposition 8.5 (2) and by $\beta(x) \in H^2(\boldsymbol{Z}[1/N], T)_{\mathrm{tor}}$, we have $\alpha(x)(\bar{\xi}) \cdot \beta(y) \in H^2(\boldsymbol{Z}[1/N], T)_{\mathrm{tor}}$. Since $\alpha(x)(\bar{\xi}) \neq 0$, this shows $\beta(y) \in H^2(\boldsymbol{Z}[1/N], T)_{\mathrm{tor}}$. Thus the image of β is contained in the finite group $H^2(\boldsymbol{Z}[1/N], T)_{\mathrm{tor}}$. Since $\mathrm{Coker}(\beta)$ is a finite group (cf. Lemma 8.4), this shows that $\mathrm{Ker}(H^2(\boldsymbol{Z}[1/N], T) \to \oplus_{l|N} H^2(\boldsymbol{Q}_l, T))$ is a finite group.

We deduce Proposition 8.5 from

PROPOSITION 8.7. *Let* Ω' *be as in* 5.1, *and let*

$$\alpha' : \mathrm{Gal}((\Omega')^{\mathrm{ab}}/\Omega') \to \mathrm{Hom}_{O_F}\left(H^1\left(\boldsymbol{Z}\left[\frac{1}{N}\right], T\right), O_F\right)$$

$$\beta' : \mathrm{Gal}((\Omega')^{\mathrm{ab}}/\Omega') \to H^2\left(\boldsymbol{Z}\left[\frac{1}{N}\right], T\right)$$

be the homomorphisms induced by the case $m = 1$, $M = N$ *of* (7.5.1) *and* (7.5.2), *respectively. Then for any* $x \in \mathrm{Gal}((\Omega')^{\mathrm{ab}}/\Omega')$ *whose image in* $\mathrm{Gal}(\Omega/\Omega')$ *coincides with the image of* σ, *we have*

$$\alpha'(x)(\bar{\xi}) \cdot \beta'(x) \in H^2\left(\boldsymbol{Z}\left[\frac{1}{N}\right], T\right)_{\mathrm{tor}}.$$

8.8. We prove Proposition 8.5 assuming Proposition 8.7. It is sufficient to prove Proposition 8.5 (1). Fix an element τ of $\mathrm{Gal}((\Omega')^{\mathrm{ab}}/\Omega')$ whose image in $\mathrm{Gal}(\Omega/\Omega')$ coincides with that of σ. Let $x \in \mathrm{Gal}(\Omega^{\mathrm{ab}}/\Omega)$ and let x' be the image of x in $\mathrm{Gal}((\Omega')^{\mathrm{ab}}/\Omega')$. Then for any $n \in \boldsymbol{Z}$, the image of the product $\tau(x')^n$ in $\mathrm{Gal}(\Omega/\Omega')$ is the image of σ. Hence

$$\alpha'(\tau(x')^n)(\bar{\xi}) \cdot \beta'(\tau(x')^n) \in H^2\left(\boldsymbol{Z}\left[\frac{1}{N}\right], T\right)_{\mathrm{tor}}$$

by Proposition 8.7. This implies

$$\alpha'(\tau)(\bar{\xi})\cdot\beta'(\tau)+n\{\alpha'(\tau)(\bar{\xi})\cdot\beta(x)+\alpha(x)(\bar{\xi})\cdot\beta'(\tau)\}$$
$$+n^2\alpha(x)(\bar{\xi})\cdot\beta(x)\in H^2\left(\boldsymbol{Z}\left[\frac{1}{N}\right],T\right)_{\mathrm{tor}}.$$

By making n vary, we obtain Proposition 8.5 (1).

To prove Proposition 8.7, we prove first

LEMMA 8.9. *Let $n'\geq n\geq 1$, and assume that the condition (2.1.1) for $m=N$ is satisfied. Let l be a good prime number for (σ,N,n'), and let $\bar{\xi}(l)_n$ be the image of $\bar{\xi}\in H^1(\boldsymbol{Z}[1/N],T)$ in $H^1(\boldsymbol{F}_l,T/p^n)$. Then $\psi_l(\bar{\xi}(l)_n)$ belongs to $\partial_l(H^1(\boldsymbol{Z}[1/Nl],T/p^n))$.*

Proof. By the remark after Lemma 5.3, $\kappa_l\in H^1(\boldsymbol{Z}[\zeta_N,1/N],T/p^nT)$ is defined. Consider the commutative diagram

$$\begin{array}{ccc}
H^1\left(\boldsymbol{Z}\left[\zeta_N,\frac{1}{Nl}\right],T/p^n\right) & \xrightarrow{\text{norm}} & H^1\left(\boldsymbol{Z}\left[\frac{1}{Nl}\right],T/p^n\right)\\
\downarrow{\scriptstyle\partial_l} & & \downarrow{\scriptstyle\partial_l}\\
H^0(\boldsymbol{F}_l\otimes\boldsymbol{Z}[\zeta_N],T/p^n) & \xrightarrow{\text{norm}} & H^0(\boldsymbol{F}_l,T/p^n)\\
\uparrow{\scriptstyle\psi_l} & & \uparrow{\scriptstyle\psi_l}\\
H^1(\boldsymbol{F}_l\otimes\boldsymbol{Z}[\zeta_N],T/p^n) & \xrightarrow{\text{norm}} & H^1(\boldsymbol{F}_l,T/p^n).
\end{array}$$

By Theorem 4.5, κ_l is sent by ∂_l (on the left hand side) to $\psi_l(z_N(l)_n)$, where $z_N(l)_n$ denotes the image of z_N in $H^1(\boldsymbol{F}_l\otimes\boldsymbol{Z}[\zeta_N],T/p^n)$. Since $\bar{\xi}(l)_n$ is the image of $z_N(l)_n$ in $H^1(\boldsymbol{F}_l,T/p^n)$ under the norm map, the diagram shows that the image of κ_l in $H^1(\boldsymbol{Z}[1/N],T/p^n)$ under the norm map is sent by ∂_l (on the right hand side) to $\psi_l(\bar{\xi}(l)_n)$.

8.10. We prove Proposition 8.7.

Take a non-zero integer t having the property described in Proposition 5.5. We show that for any $x\in\mathrm{Gal}((\Omega')^{\mathrm{ab}}/\Omega')$ whose image in $\mathrm{Gal}(\Omega/\Omega')$ coincides with that of σ and for any $n\geq 1$, the image of $t^2\cdot\alpha(x)(\bar{\xi})\cdot\beta(x)$ in $H^2(\boldsymbol{Z}[1/N],T/p^nT)$ is zero. This implies $t^2\cdot\alpha(x)(\bar{\xi})\cdot\beta(x)=0$ in $H^2(\boldsymbol{Z}[1/N],T)$.

Since $w\neq 0$, $H^0(\boldsymbol{Q}(\zeta_N),\ T\otimes\boldsymbol{Q}/\boldsymbol{Z})$ is a finite group. Hence there exists $n'\geq n$ satisfying (2.1.1) for $m=N$.

The group $\Pi_N(\Omega'_{N,n'})/p^{n'}$ (cf. 7.3) is finite, for it is the Pontragin dual of the finite group $H^1(O_{\Omega'_{N,n'}}[1/N],\boldsymbol{Z}/p^{n'})$. Hence by Chevotarev's density theorem, there is a maximal ideal v of $O_{\Omega'_{N,n'}}[1/NN']$ whose Frobenius substitutions in the Galois groups

$$\Pi_N(\Omega'_{N,n'})/p^{n'}\quad\text{and}\quad\mathrm{Gal}(\Omega_{N,n'}(\zeta_{p^{n'}})/\Omega'_{N,n'}),$$

coincide with the images of x, respectively, and which is of degree one over $\boldsymbol{Q}$. Then, v is a good maximal ideal for (σ, N, n') in the sense of 5.2. Let l be the prime ideal lying under v. Then by Lemma 7.6 (1), the element $\alpha(x)(\bar{\xi}) \bmod p^n \in O_F/p^n$ coincides with $\mu_v(\bar{\xi}(l)_n)$ where $\mu_v : H^1(\boldsymbol{F}_l, T/p^n) \to O_F/p^n$ is as in 5.4, and by Lemma 7.6 (2), the element $\beta(x) \bmod p^n \in H^2(\boldsymbol{Z}[1/N], T/p^n)$ belongs to the image of $\iota_l : H^0(\boldsymbol{F}_l, (T/p^n)(-1)) \to H^2(\boldsymbol{Z}[1/N], T/p^n)$. Thus it is sufficient to prove that $t^2 \cdot \mu_v(\bar{\xi}(l)_n)$ kills the image of the last map ι_l. Since ι_l kills the image of $\partial_l : H^1(\boldsymbol{Z}[1/Nl], T/p^n) \to H^0(\boldsymbol{F}_l, (T/p^n)(-1))$ (cf. 7.2), it is sufficient to prove that the cokernel of this map ∂_l is killed by $t^2 \cdot \mu_v(\bar{\xi}(l)_n)$. But this follows from Proposition 5.6 and Lemma 8.9.

§9. Torsion property of H^2

Let (F, T, N) be as in 0.1. For d and Λ as in 0.4, it is conjectured by many people (Schneider, Greenberg, Jannsen, Perrin-Riou, ...) that the Λ-module

$$\boldsymbol{H}^2 = \boldsymbol{H}^2(T) = \varprojlim_n H^2\left(\boldsymbol{Z}\left[\zeta_{dp^n}, \frac{1}{N}\right], T\right)$$

is a torsion module, i.e., killed by a non-zero-divisor of Λ (at least in the case T comes from a motif). (See for example, [Ja, §4]).

The aim of §9 is to prove the following Theorem 9.1 concerning this conjecture.

THEOREM 9.1. *Let (F, T, N, N') be as in* 0.1, *let d, Λ be as in* 0.4, *and let $(z_m)_m$ be an Euler system for (F, T, N, N'). Assume that the conditions* (i), (ii), (iii) *in* 0.6 *are satisfied. Let* $\mathfrak{q}$ *be a prime ideal of Λ of height zero (i.e. a prime ideal of Λ such that $\Lambda_{\mathfrak{q}}$ is a field), and assume that the image $\xi_{\mathfrak{q}}$ of ξ (cf.* 0.7) *in $\boldsymbol{H}^1_{\mathfrak{q}}$ is not zero. Then*

$$\boldsymbol{H}^2_{\mathfrak{q}} = (0).$$

We give some preliminaries for the proof of Theorem 9.1, in 9.2–9.7.

9.2. We discuss the notion "the twist of an Euler system by a character".

Let F' be a finite extension of F, let $\chi : \mathrm{Gal}(\boldsymbol{Q}(\zeta_{dp^\infty})/\boldsymbol{Q}) \to (O_{F'})^\times$ be a continuous homomorphism, and let T' be the following $O_{F'}$-module endowed with a continuous $O_{F'}$-linear action of $\mathrm{Gal}(\bar{\boldsymbol{Q}}/\boldsymbol{Q})$. As an $O_{F'}$-module, $T' = O_{F'} \otimes_{O_F} T$. An element σ of $\mathrm{Gal}(\bar{\boldsymbol{Q}}/\boldsymbol{Q})$ acts on T' by $\chi(\sigma)^{-1} \otimes \sigma$.

We obtain an Euler system $(z'_m)_m$ for (F', T', N, N'), called the twist of the Euler system $(z_m)_m$ by the character χ, in the following way. For an integer $m \geq 1$ such that $N|m$ and $(m, N') = 1$, we define the element z'_m of $H^1(\boldsymbol{Z}[\zeta_m, 1/N], T')$ by

$$z'_m = (z'_{m,n})_n \in \varprojlim_n H^1\left(\boldsymbol{Z}\left[\zeta_m, \frac{1}{N}\right], T'/p^n\right)$$

where $z'_{m,n}$ is the following element of $H^1(\boldsymbol{Z}[\zeta_m, 1/N], T'/p^n)$. For an integer $n > 0$, there is $i \geq 1$ such that the homomorphism $\mathrm{Gal}(\bar{\boldsymbol{Q}}/\boldsymbol{Q}(\zeta_{mp^i})) \to (O_F/p^n)^\times$ induced by χ is trivial. We define $z'_{m,n}$ to be the image of $z_{mp^i} \in H^1(\boldsymbol{Z}[\zeta_{mp^i}, 1/N], T)$ under

$$H^1\left(\boldsymbol{Z}\left[\zeta_{mp^i}, \frac{1}{N}\right], T/p^n\right) \longrightarrow H^1\left(\boldsymbol{Z}\left[\zeta_{mp^i}, \frac{1}{N}\right], T'/p^n\right)$$
$$\xrightarrow{\text{norm}} H^1\left(\boldsymbol{Z}\left[\zeta_m, \frac{1}{N}\right], T'/p^n\right).$$

(The first arrow is induced by the canonical map $T/p^n \to T'/p^n$ which is a $\mathrm{Gal}(\bar{\boldsymbol{Q}}/\boldsymbol{Q}(\zeta_{mp^i}))$-homomorphism.) It is checked easily that $(z'_m)_m$ is an Euler system for (F', T', N, N').

LEMMA 9.3. *Let the notation be as in* 9.2. *Let*

$$\Lambda' = O_{F'}[[\mathrm{Gal}(\boldsymbol{Q}(\zeta_{dp^\infty})/\boldsymbol{Q})]].$$

(1) *There is an isomorphism of Λ'-modules*

$$\Lambda' \otimes_\Lambda \boldsymbol{H}^q(T) \cong \boldsymbol{H}^q(T')$$

where $\Lambda \to \Lambda'$ is the unique continuous O_F-homomorphism which sends $\sigma \in \mathrm{Gal}(\boldsymbol{Q}(\zeta_{dp^\infty})/\boldsymbol{Q}) \subset \Lambda$ to $\chi(\sigma)\sigma$.

(2) *If the conditions* (i), (ii) *in* 0.6 *are satisfied, then (F', T', N, N') also satisfies the conditions* (i), (ii).

(3) *Assume that the condition* (iii) *in* 0.6 *is satisfied and that there are an integer r and a continuous homomorphism λ: $\mathrm{Gal}(\boldsymbol{Q}(\zeta_{dp^\infty})/\boldsymbol{Q}) \to (O_{F'})^\times$ of finite order such that the product $\chi\lambda$ coincides with the r-th power of the cyclotomic character. (The cyclotomic character means the homomorphism $\mathrm{Gal}(\boldsymbol{Q}(\zeta_{dp^\infty})/\boldsymbol{Q}) \to (\boldsymbol{Z}_p)^\times$ defined by the action on p^n-th roots of 1 for all $n \geq 0$.) Then (F', T', N, N') satisfies the condition* (iii).

Proof. (1) and (3) are easy, and (2) follows from

LEMMA 9.4. *Let k be a field, G a group, and let U be a finite dimensional k-vector space endowed with a k-linear action of G. Assume that there exists $\sigma \in G$ such that*

$$\dim_k(\mathrm{Ker}(1 - \sigma : U \to U)) = 1.$$

Then the following (i) (ii) *are equivalent.*

(i) *U is irreducible as a representation of G over k.*

(ii) $\mathrm{Ker}(1 - \sigma : U \to U)$ *generates U as a $k[G]$-module, and* $\mathrm{Ker}(1 - \sigma : U^* \to U^*)$ *generates U^* as a $k[G]$-module. Here U^* denotes* $\mathrm{Hom}_k(U, k)$ *endowed with the dual action of G.*

Proof. It is clear that (i) implies (ii). Assume (ii). Let W be a $k[G]$-submodule of U such that $W \neq U$. Then by the assumption, W does

not contain $\mathrm{Ker}(1-\sigma : U \to U)$. Hence $1-\sigma : W \to W$ is bijective. Thus $\dim_k(\mathrm{Ker}(1-\sigma : U/W \to U/W)) = 1$, and hence $\dim_k(\mathrm{Ker}(1-\sigma : (U/W)^* \to (U/W)^*) = 1$. This means that the $k[G]$-submodule $(U/W)^*$ of U^* contains $\mathrm{Ker}(1-\sigma : U^* \to U^*)$, and hence we have $(U/W)^* = U^*$. Hence $W = 0$.

We use the following module theoretic lemma for the proof of Theorem 9.1.

LEMMA 9.5. *Let R be a Noetherian integral domain, and let M be a finitely generated R-module.*

(1) *Assume that there exists a prime ideal $\mathfrak{p}$ of R such that $\kappa(\mathfrak{p}) \otimes_R M = 0$ ($\kappa(\mathfrak{p})$ here denotes the residue field of $\mathfrak{p}$). Then M is a torsion R-module.*

(2) *Let x be an element of M, and assume that x is not an R-torsion element (that is, if $a \in R$ and $ax = 0$, then $a = 0$). Then for almost all prime ideals $\mathfrak{p}$ of R of height one, the images of x in $\kappa(\mathfrak{p}) \otimes_R M$ are non-zero.*

(3) *If M is a torsion R-module, $\kappa(\mathfrak{p}) \otimes_R M = 0$ for almost all prime ideals $\mathfrak{p}$ of R of height one.*

Proof. (1) If $\kappa(\mathfrak{p}) \otimes_R M = 0$, we have $R_{\mathfrak{p}} \otimes_R M = 0$ and hence M is a torsion R-module.

(2) For some non-zero element f of R, $R[1/f]x$ becomes an $R[1/f]$-direct summand of $R[1/f] \otimes_R M$ and is a free $R[1/f]$-module of rank one. For any prime ideal $\mathfrak{p}$ of R which does not contain f (note there are only finitely many $\mathfrak{p}$ which contain f), the image of x in $\kappa(\mathfrak{p}) \otimes_R M$ is not zero

(3) There exists a non-zero element f of R which kills M. For any prime ideal $\mathfrak{p}$ of R which does not contain f, we have $\kappa(\mathfrak{p}) \otimes_R M = 0$.

9.6. Let $m \geq 1$ be an integer which divides dp^i for some i. Then there exist spectral sequences

$$E_2^{i,j} = \mathrm{Tor}_{-i}^{\Lambda}(\Lambda_m, \boldsymbol{H}^j) \quad \Rightarrow \quad E_\infty^i = H^i\left(\boldsymbol{Z}\left[\zeta_m, \frac{1}{N}\right], T\right) \quad (m \geq 3 \text{ or } p \neq 2)$$

$$E_2^{i,j} = \boldsymbol{Q} \otimes \mathrm{Tor}_{-i}^{\Lambda}(\Lambda_m, \boldsymbol{H}^j) \quad \Rightarrow \quad E_\infty^i = \boldsymbol{Q} \otimes H^i\left(\boldsymbol{Z}\left[\zeta_m, \frac{1}{N}\right], T\right) \quad (\text{any } m)$$

which comes from the isomorphism

$$\Lambda_m \otimes_\Lambda^L R \varprojlim_{i,n} R\Gamma(\boldsymbol{Z}[\zeta_{dp^i}], T/p^nT) \cong R \varprojlim_n R\Gamma\left(\boldsymbol{Z}\left[\zeta_m, \frac{1}{N}\right], T/p^nT\right)$$

for $m \geq 3$ or $p \neq 2$ ([BO, Appendix B]). (The strange condition "$m \geq 3$ or $p \neq 2$" appears here to have the finiteness of the cohomological dimension. If $m \geq 3$ (then F has no real place) or if $p \neq 2$, the p-cohomological dimension of $\mathrm{Spec}(\boldsymbol{Z}[\zeta_m, 1/N])$ is 2 ([Ma]).

9.7. Now we prove Theorem 9.1.

Let Δ be the torsion part of $\mathrm{Gal}(\boldsymbol{Q}(\zeta_{dp^\infty})/\boldsymbol{Q})$, and let F' be the subfield of $\Lambda_\mathfrak{q}$ generated by the image of $\boldsymbol{Z}_p[\Delta]$ in $\Lambda_\mathfrak{q}$. Let Θ be the set of all continuous homomorphisms

$$\chi : \mathrm{Gal}(\boldsymbol{Q}(\zeta_{dp^\infty})/\boldsymbol{Q}) \to (O_{F'})^\times$$

satisfying the following conditions (9.7.1) and (9.7.2).

(9.7.1) For $\sigma \in \Delta$, $\chi(\sigma)$ coincides with the image of σ under the canonical map $\Delta \subset \boldsymbol{Z}_p[\Delta] \to F' \subset \Lambda_\mathfrak{q}$.

(9.7.2) There are an integer r and a continuous homomorphism λ: $\mathrm{Gal}(\boldsymbol{Q}(\zeta_{dp^\infty})/\boldsymbol{Q}) \to (O_{F'})^\times$ of finite order such that $\chi\lambda$ coincides with the r-th power of the cyclotomic character.

If $\chi \in \Theta$ is given, define T', $(z'_m)_m$, Λ' as in 9.2 with respect to χ. We regard Λ' as a ring over Λ with respect to the unique continuous O_F-homomorphism which sends $\sigma \in \mathrm{Gal}(\boldsymbol{Q}(\zeta_{dp^\infty})/\boldsymbol{Q})$ to $\chi(\sigma)\sigma$. Let $\mathfrak{q}'$ be the ideal of Λ' generated by the image of $\mathfrak{q}$. Then $\mathfrak{q}' \cap \Lambda = \mathfrak{q}$. Since $\Lambda' \otimes_\Lambda \boldsymbol{H}^2(T) \cong \boldsymbol{H}^2(T')$ (cf. Lemma 9.3 (1)), $\boldsymbol{H}^2(T)_\mathfrak{q} = 0$ is equivalent to $\boldsymbol{H}^2(T')_{\mathfrak{q}'} = 0$. Furthermore (F', T', N, N') satisfies the conditions (i), (ii), (iii) by Lemma 9.3 (2), (3). Thus Theorem 9.1 for $(F, T, N, N', (z_m)_m, d, \mathfrak{q})$ is equivalent to Theorem 9.1 for $(F', T', N, N', (z'_m)_m, d, \mathfrak{q}')$. By the condition (9.7.1), $\mathfrak{q}'$ is contained in the kernel of the unique continious $O_{F'}$-homomorphism $\varepsilon : \Lambda' \to F'$ which sends $\mathrm{Gal}(\boldsymbol{Q}(\zeta_{dp^\infty})/\boldsymbol{Q}) \subset \Lambda'$ to 1.

Consider the spectral sequence

$$E_2^{i,j} = \mathrm{Tor}_{-i}^{\Lambda'}(F', \boldsymbol{H}^j(T')) \quad \Rightarrow \quad E_\infty^k = H^k\left(\boldsymbol{Z}\left[\frac{1}{N}\right], V'\right), \tag{9.7.3}$$

where F' is regarded as a Λ'-module with respect to $\varepsilon : \Lambda' \to F'$, and $V' = \boldsymbol{Q} \otimes T'$ (the case $m = 1$ of the second spectral sequence in 9.6). We obtain from (9.7.3)

$$F' \otimes_{\Lambda'} \boldsymbol{H}^2(T') \cong H^2\left(\boldsymbol{Z}\left[\frac{1}{N}\right], V'\right).$$

By Lemma 9.5 (1) applied to $R = \Lambda'/\mathfrak{q}'$ and $\mathfrak{p} = \mathrm{Ker}(\Lambda'/\mathfrak{q}' \to F')$, we see the following fact: If $H^2(\boldsymbol{Z}[1/N], T')$ is a finite group, then $\Lambda'/\mathfrak{q}' \otimes_{\Lambda'} \boldsymbol{H}^2(T')$ is a torsion $\Lambda'/\mathfrak{q}'$-module and hence $\boldsymbol{H}^2(T')_{\mathfrak{q}'} = 0$. Hence for the proof of Theorem 9.1, it is sufficient to prove that there exists $\chi \in \Theta$ for which $H^2(\boldsymbol{Z}[1/N], T')$ is a finite group.

For $\chi \in \Theta$, let $\mathfrak{p}_\chi$ be the kernel of $\Lambda/\mathfrak{q} \to F'$ which is induced by the unique continuous O_F-homomorphism $\Lambda \to F'$ which sends $\sigma \in \mathrm{Gal}(\boldsymbol{Q}(\zeta_{dp^\infty})/\boldsymbol{Q})$ to $\chi(\sigma)$. Then $\mathfrak{p}_\chi$ is a prime ideal of height one. By Lemma 9.5 (2) applied to $R = \Lambda/\mathfrak{q}$, $M = \Lambda/\mathfrak{q} \otimes_\Lambda \boldsymbol{H}^1$, $x =$ the image of ξ in M, we see that the image of ξ in $\kappa(\mathfrak{p}_\chi) \otimes_\Lambda \boldsymbol{H}^1$ is not zero for almost all $\chi \in \Theta$. On the other hand, by Lemma 9.5 (3) applied to $R = \Lambda/\mathfrak{q}$ and to the R-modules

$$\Lambda/\mathfrak{q} \otimes_\Lambda \varprojlim_n H^2(\boldsymbol{Q}_l \otimes \boldsymbol{Q}(\zeta_{dp^n}), T)$$

for prime divisors l of N, which are torsion R-modules by Remark 0.5.2, we see that $\kappa(\mathfrak{p}_\chi) \otimes_\Lambda \varprojlim_n H^2(\boldsymbol{Q}_l \otimes \boldsymbol{Q}(\zeta_{dp^n}), T) = 0$ for almost all $\chi \in \Theta$. These things show that there exists $\chi \in \Theta$ satisfying the following conditions (9.7.4)–(9.7.6).

(9.7.4) The image of ξ in $\kappa(\mathfrak{p}_\chi) \otimes_\Lambda \boldsymbol{H}^1$ is not zero.

(9.7.5) $\kappa(\mathfrak{p}_\chi) \otimes_\Lambda \varprojlim_n H^2(\boldsymbol{Q}_l \otimes \boldsymbol{Q}(\zeta_{dp^n}), T) = 0$ for all prime divisors l of N.

(9.7.6) V' (defined by χ) is not of weight $\neq 0, -2$.

We prove that $H^2(\boldsymbol{Z}[1/N], T')$ is a finite group for T' defined by χ, by using the part of Theorem 8.1 already proved in §8. Since we have a commutative diagram

$$\begin{array}{ccc} \boldsymbol{Q} \otimes \Lambda/\mathfrak{q} & \xrightarrow{\cong} & \boldsymbol{Q} \otimes \Lambda'/\mathfrak{q}', \\ \downarrow & & \downarrow \\ \kappa(\mathfrak{p}_\chi) & \xrightarrow{\cong} & F' \end{array}$$

in which the horizontal rows are isomorphisms, (9.7.4) (resp. (9.7.5)) is rewritten as the following (9.7.7) (resp. (9.7.8)).

(9.7.7) Define $\xi' \in \boldsymbol{H}^1(T')$ for $(F', T', N, N', (z'_m)_m, d)$ just as ξ for $(F, T, N, N', (z_m)_m, d)$. Then the image of ξ' in $F' \otimes_{\Lambda'} \boldsymbol{H}^1(T')$ is not zero.

(9.7.8) $\boldsymbol{Q} \otimes H^2(\boldsymbol{Q}_l, T') = 0$ (equivalently, $H^0(\boldsymbol{Q}_l, (T')^*(1)) = 0$) for all prime divisors l of N.

(9.7.9) By (9.7.3), we have an injection

$$F' \otimes_{\Lambda'} \boldsymbol{H}^1(T') \to \boldsymbol{Q} \otimes H^1\left(\boldsymbol{Z}\left[\frac{1}{N}\right], T'\right).$$

Hence (9.7.7) is rewritten as

(9.7.10) The image of ξ' in $H^1(\boldsymbol{Z}[1/N], T')$ is not a torsion element.

By (9.7.6), (9.7.9) and (9.7.10), the case $w \neq 0, -2$ of Theorem 8.1 proved in §8 shows that $H^2(\boldsymbol{Z}[1/N], T')$ is a finite group.

§10. Ring theoretic preliminaries

10.1. In this §10, we prove some ring theoretic propositions which are used in later sections. In Propositions 10.2 and 10.3, let R be a Noetherian commutative ring, and let $\mathfrak{p}$ be a prime ideal of R such that the local ring $R_\mathfrak{p}$ is a discrete valuation ring. Fix an element π of R whose image in $R_\mathfrak{p}$ is a prime element, and let Ψ be the set of all ideals $\mathfrak{a}$ of R such that the image of π in $R/\mathfrak{a}$ is a non-zero-divisor.

PROPOSITION 10.2. *Let M be a finitely generated R-module. Then there exists an element t of $R\backslash\mathfrak{p}$ having the following property: For any $\mathfrak{a} \in \Psi$ and any $q \geq 1$, t annihilates $\mathrm{Tor}_q^R(R/\mathfrak{a}, M)$.*

Proof. We have $M_{\mathfrak{p}} \cong N_{\mathfrak{p}}$ for some R-module N of the form

$$N = R^{\oplus r} \oplus \left(\bigoplus_{i=1}^{s} R/(\pi^{n(i)}) \right).$$

There are R-homomorphisms

$$f : M \to N, \quad g : N \to M$$

and an element t of $R\backslash\mathfrak{p}$ such that $g \circ f : M \to M$ coincides with the multiplication by t. This t has the desired property. In fact, for any $\mathfrak{a} \in \Phi$ and any $q \geq 1$, the composite

$$\mathrm{Tor}_q^R(R/\mathfrak{a}, M) \xrightarrow{f} \mathrm{Tor}_q^R(R/\mathfrak{a}, N) \xrightarrow{g} \mathrm{Tor}_q^R(R/\mathfrak{a}, M)$$

coincides with the multiplication by t. But $\mathrm{Tor}_q^R(R/\mathfrak{a}, N) = 0$.

PROPOSITION 10.3. *Let M be a finitely generated R-module, let $s_1, \ldots, s_k$ be elements of M, let $I_1, \ldots, I_k$ be ideals of R, and assume that for $1 \leq i \leq k$, the annihilator of*

$$s_i \bmod \sum_{j=1}^{i-1} R_{\mathfrak{p}} \cdot s_j$$

in $R_{\mathfrak{p}}$ and the annihilator of the $R_{\mathfrak{p}}$-module $(\sum_{j=1}^{k} R_{\mathfrak{p}} \cdot s_j)/(\sum_{j=1}^{i-1} R_{\mathfrak{p}} \cdot s_j)$ both coincide with $(I_i)_{\mathfrak{p}}$. Then there exists $t \in R\backslash\mathfrak{p}$ having the following property: If $\mathfrak{a} \in \Psi$, $1 \leq i \leq k$, $c_j \in R$ $(1 \leq j \leq i)$, $b_{jq} \in tJ(R) + I_i$ $(1 \leq j \leq i, 1 \leq q \leq k$, $J(R)$ denotes the Jacobson radical of R, that is, $J(R)$ is the intersection of all maximal ideal of R), and if

$$\sum_{j=1}^{i} c_j \left(s_j + \sum_{q=1}^{k} b_{jq} s_q \right) \in \mathfrak{a}M$$

then

$$tc_j \in \mathfrak{a} + I_i \quad \text{for } 1 \leq j \leq i.$$

Proof. Let $N = \sum_{j=1}^{k} R \cdot s_j$.

First take $t_1 \in R\backslash\mathfrak{p}$ which kills $\mathrm{Tor}_1^R(R/\mathfrak{a}, M/N)$ for any $\mathfrak{a} \in \Psi$ (cf. 10.1). Since there exists an exact sequence

$$\mathrm{Tor}_1^R(R/\mathfrak{a}, M/N) \to N/\mathfrak{a}N \to M/\mathfrak{a}M,$$

t_1 kills the kernel of $N/\mathfrak{a} \to M/\mathfrak{a}M$ for any $\mathfrak{a} \in \Psi$.

Next we show that there exist $t_2 \in R\backslash\mathfrak{p}$ and R-homomorphisms

$$h_{ji} : N \to R/I_i$$

defined for j, i such that $1 \leq j \leq i \leq k$, satisfying the following condition:

$$h_{ji}(s_j) = t_2 \bmod I_i$$

$$h_{ji}(s_q) = 0 \quad \text{for any } q \text{ such that } 1 \leq q \leq i \text{ and } q \neq j.$$

Indeed, for $1 \leq i \leq k$, $\sum_{j=1}^{i} R_{\mathfrak{p}} \cdot s_j$ is an $R_{\mathfrak{p}}$-direct summand of $N_{\mathfrak{p}}$ and $(\sum_{j=1}^{i} R_{\mathfrak{p}} \cdot s_j)/(I_i)_{\mathfrak{p}}(\sum_{j=1}^{i} R_{\mathfrak{p}} \cdot s_j)$ is a free $R_{\mathfrak{p}}/(I_i)_{\mathfrak{p}}$-module with basis $(s_q \bmod (I_i)_{\mathfrak{p}}(\sum_{j=1}^{i} R_{\mathfrak{p}} \cdot s_j))_{1 \leq q \leq i}$. Hence there exist $R_{\mathfrak{p}}$-homomorphisms

$$h'_{ji} : N_{\mathfrak{p}} \to R_{\mathfrak{p}}/(I_i)_{\mathfrak{p}} \quad (1 \leq j \leq i)$$

satisfying

$$h'_{ji}(s_j) = 1,$$

$$h'_{ji}(s_q) = 0 \quad \text{for any } q \text{ such that } 1 \leq q \leq i \text{ and } q \neq j.$$

This proves the existence of h_{ji}.

Now let t_1 and t_2 be as above. We show that $t = t_1 t_2$ has the property stated in Proposition 10.3. Let $1 \leq i \leq k$ and assume

$$\sum_{j=1}^{i} c_j \left(s_j + \sum_{q=1}^{k} b_{jq} s_q \right) \in \mathfrak{a}M,$$

$$c_j \in R \ (1 \leq j \leq i), \quad b_{jq} \in t \cdot J(R) + I_i \ (1 \leq j \leq i, 1 \leq q \leq k).$$

Then we have

$$\sum_{j=1}^{i} t_1 \cdot c_j \left(s_j + \sum_{q=1}^{k} b_{jq} s_q \right) \in \mathfrak{a}N.$$

By applying h_{mi} $(1 \leq m \leq i)$, we obtain

$$t \cdot \left(c_m + \sum_{j=1}^{i} c_j a_{mj} \right) \in \mathfrak{a} + I_i \quad (a_{mj} \in J(R))$$

for $1 \leq m \leq i$. Since the matrix $1_i + (a_{mj})_{1 \leq m \leq i, 1 \leq j \leq i}$ (1_i denotes the unit matrix of degree i) is invertible, we have $t \cdot c_m \in \mathfrak{a} + I_i$ for $1 \leq m \leq i$.

10.4. In later sections, we will apply the above propositions to the following situation: Let (F, T, N, N') be as in 0.1, and let d, Λ be as in 0.4. We will take the ring Λ as R in the above propositions. In the rest of §10, we prove preliminary results Propositions 10.5–10.7 concerning this situation.

PROPOSITION 10.5. *Let the situation be as in* 10.4.

(1) $\Lambda[1/p]$ *is a finite product of principal ideal domains.*

(2) *The following three conditions* (i)–(iii) *are equivalent.*

(i) Λ *is a regular ring.*

(ii) *Let* Δ *be the torsion part of* $\mathrm{Gal}(\boldsymbol{Q}(\zeta_{dp^\infty})/\boldsymbol{Q})$. *Then the order of* Δ *is prime to* p.

(iii) *There exists a prime ideal* $\mathfrak{p}$ *of* Λ *such that* $p \in \mathfrak{p}$ *and such that* $\Lambda_{\mathfrak{p}}$ *is a discrete valuation ring.*

(3) *The equivalent conditions in* (2) *are satisfied if* $p \neq 2$ *and* $d = 1$.

(4) *The equivalent conditions in* (2) *are not satisfied if* $p = 2$.

Proof. (1) Since $\mathrm{Gal}(\boldsymbol{Q}(\zeta_{dp^\infty})/\boldsymbol{Q}) \cong \Delta \times \boldsymbol{Z}_p$,

$$\Lambda \cong O_F[[\Delta \times \boldsymbol{Z}_p]] \cong O_F[[X]][\Delta].$$

From this we have that $\Lambda[1/p]$ is isomorphic to a finite product of rings of the form $O_{F'}[[X]][1/p]$ for finite extensions F' of F. These rings $O_{F'}[[X]][1/p]$ are principal ideal domains.

(2) It is easy to see that (ii) implies (i) and that (i) implies (iii). We show that (iii) implies (ii). Identify Λ with $O_F[[X]][\Delta]$. Let $\mathfrak{p}$ be a prime ideal as in (iii). Then $\mathfrak{p}' = O_F[[X]] \cap \mathfrak{p}$ coincides with the prime ideal of $O_F[[X]]$ generated by the maximal ideal of O_F. Write $\Delta = \Delta_1 \times \Delta_2$ where the order of Δ_1 is a power of p and the order of Δ_2 is prime to p. Since $O_F[[X]][\Delta_1] \to (O_F[[X]][\Delta_1])[\Delta_2] = \Lambda$ is étale, the regular ring $\Lambda_{\mathfrak{p}}$ is étale over the local ring $O_F[[X]]_{\mathfrak{p}'}[\Delta_1]$. Hence $O_F[[X]]_{\mathfrak{p}'}[\Delta_1]$ is regular, and this implies $\Delta_1 = \{1\}$.

(3) If $p \neq 2$ and $d = 1$, Δ is isomorphic to $(\boldsymbol{Z}/p\boldsymbol{Z})^\times$ whose order is prime to p.

(4) The complex conjugation in $\mathrm{Gal}(\boldsymbol{Q}(\zeta_{dp^\infty})/\boldsymbol{Q})$ is of order 2.

COROLLARY 10.6. *Let the situation be as in* 10.4, *and let* $\mathfrak{p}$ *be a prime ideal of* Λ *such that* $\Lambda_{\mathfrak{p}}$ *is a discrete valuation ring. Then, if* $\mathfrak{p}$ *does not contain* p (*resp. if* $p \in \mathfrak{p}$), $\mathfrak{p}\Lambda[1/p]$ (*resp.* $\mathfrak{p}$) *is a principal ideal.*

Proof. The case $\mathfrak{p}$ does not contain p follows from Proposition 10.5 (1). In the case $p \in \mathfrak{p}$, Λ is a regular semi-local ring by Proposition 10.5 (2), and hence any prime ideal of Λ of height one is principal.

PROPOSITION 10.7. *Let the situation be as in* 10.4, *and let* $\mathfrak{p}$ *be a prime ideal of* Λ *such that* $\Lambda_{\mathfrak{p}}$ *is a discrete valuation ring. Let* Σ_d *be the set of all positive integers which are divisors of* dp^i *for some* $i \geq 0$. *Assume that* $\mathfrak{p}$ *does not contain* $\mathrm{Ker}(\Lambda \to \Lambda_m)$ *for any* $m \in \Sigma_d$. ($\Lambda_m = O_F[\mathrm{Gal}(\boldsymbol{Q}(\zeta_m)/\boldsymbol{Q})]$ *as before.*) *Then there exists an element* t *of* $\Lambda \backslash \mathfrak{p}$ *which kills the kernel and the cokernel of*

$$\Lambda_m \otimes_\Lambda \boldsymbol{H}^1 \to H^1\left(\boldsymbol{Z}\left[\zeta_m, \frac{1}{N}\right], T\right).$$

for any $m \in \Sigma_d$.

Proof. We may assume $m \geq 3$. (The norm argument reduces the cases $m = 1$ or 2 to the case $m \geq 3$).

If $\mathfrak{p}$ does not contain p, take an element π of Λ which generates the ideal $\Lambda[1/p]\mathfrak{p}$ of $\Lambda[1/p]$. If $p \in \mathfrak{p}$, let π be a generator of the ideal $\mathfrak{p}$. (Such π exists by Proposition 10.5.) We apply Proposition 10.2 to the case $R = \Lambda$, $M = \boldsymbol{H}^2$, and to $\mathfrak{p}$ and π here. Then the ideal $\mathfrak{a} = \mathrm{Ker}(\Lambda \to \Lambda_m)$ belongs to the set Ψ in 10.1. Take t of Proposition 10.2 for the Λ-module $\boldsymbol{H}^2$. By 9.6, we have an exact sequence

$$\mathrm{Tor}_2^\Lambda(\Lambda_m, \boldsymbol{H}^2) \to \Lambda_m \otimes_\Lambda \boldsymbol{H}^1 \to H^1\left(\boldsymbol{Z}\left[\zeta_m, \frac{1}{N}\right], T\right) \to \mathrm{Tor}_1^\Lambda(\Lambda_m, \boldsymbol{H}^2) \to 0.$$

Since t kills $\mathrm{Tor}_q^\Lambda(\Lambda_m, \boldsymbol{H}^2)$ for $q \geq 2$, t has the property described in Proposition 10.7.

§11. Proof of Theorem 0.8, (I)

In this §11, we deduce Theorem 0.8 from Proposition 11.6, and reduce the proof of Proposition 11.6 to Proposition 11.14 which will be proved in §12.

In §11 and §12, let the assumptions and the notations be as in Theorem 0.8.

Fix a prime ideal $\mathfrak{p}$ of Λ such that $\Lambda_\mathfrak{p}$ is a discrete valuation ring.

11.1. By Theorem 9.1 applied to the unique prime ideal $\mathfrak{q}$ of Λ of height zero such that $\mathfrak{p} \supset \mathfrak{q}$, we see that $\boldsymbol{H}^2_\mathfrak{p}$ is of finite length as a $\Lambda_\mathfrak{p}$-module.

11.2. The inequality

$$\mathrm{length}_{\Lambda_\mathfrak{p}}(\boldsymbol{H}^2_{0,\mathfrak{p}}) \leq \mathrm{length}_{\Lambda_\mathfrak{p}}(\boldsymbol{H}^1_\mathfrak{p}/\Lambda_\mathfrak{p}\xi_\mathfrak{p})$$

in Theorem 0.8 under the condition $(\mathrm{iv}_\mathfrak{p})$ is deduced from the inequality

$$\mathrm{length}_{\Lambda_\mathfrak{p}}(\boldsymbol{H}^2_{0,\mathfrak{p}}) \leq \mathrm{length}_{\Lambda_\mathfrak{p}}(\Lambda_\mathfrak{p}/J(\xi)_\mathfrak{p})$$

in Theorem 0.8, as follows. Under the condition $(\mathrm{iv}_\mathfrak{p})$,

$$\mathrm{rank}_{\Lambda_\mathfrak{p}}(\boldsymbol{H}^1_\mathfrak{p}) = \mathrm{rank}_{\Lambda_\mathfrak{p}}(\boldsymbol{H}^2_\mathfrak{p}) + n(V, \mathfrak{p}) = 0 + 1 = 1,$$

(cf. 0.5) and hence

$$\boldsymbol{H}^1_\mathfrak{p} \cong \Lambda_\mathfrak{p} \oplus N$$

as a $\Lambda_\mathfrak{p}$-module with N a $\Lambda_\mathfrak{p}$-module of finite length. Let $pr_1 : \boldsymbol{H}^1_\mathfrak{p} \to \Lambda_\mathfrak{p}$ be the first projection. Then $J(\xi)_\mathfrak{p} = \Lambda_\mathfrak{p} pr_1(\xi_\mathfrak{p})$, and hence

$$\begin{aligned}\mathrm{length}_{\Lambda_\mathfrak{p}}(\Lambda_\mathfrak{p}/J(\xi)_\mathfrak{p}) &= \mathrm{length}_{\Lambda_\mathfrak{p}}(\Lambda_\mathfrak{p}/\Lambda_\mathfrak{p} pr_1(\xi_\mathfrak{p})) \\ &\leq \mathrm{length}_{\Lambda_\mathfrak{p}}(\boldsymbol{H}^1_\mathfrak{p}/\Lambda_\mathfrak{p}\xi_\mathfrak{p}).\end{aligned}$$

11.3. For the proof of Theorem 0.8, we may replace T by the Tate twist $T(r)$ $(r \in \boldsymbol{Z})$. (Twist the Euler system by a power of the cyclotomic character (cf. 9.2).) Hence we may assume that the following conditions (11.3.1)–(11.3.4) are satisfied. Let Σ_d be the set of all positive integers which divide dp^i for some $i \geq 0$.

(11.3.1) The integer w in the condition (iii) in 0.6 is not $0, -2$.

(11.3.2) For any $m \in \Sigma_d$, $H^2(\boldsymbol{Z}[\zeta_m, 1/N], T)$ is a finite group.

(11.3.3) For any $m \in \Sigma_d$, $\mathfrak{p}$ does not contain $\mathrm{Ker}(\Lambda \to \Lambda_m)$.

(11.3.4) The following does not hold: The action of $\mathrm{Gal}(\bar{\boldsymbol{Q}}/\boldsymbol{Q})$ on T factors through $\mathrm{Gal}(\boldsymbol{Q}(\zeta_{dp^\infty})/\boldsymbol{Q})$, and the induced action of Λ on T factors through $\Lambda/\mathfrak{p}$.

In the rest of §11, we assume that the conditions (11.3.1)–(11.3.4) are satisfied.

11.4. Take an element π of Λ as follows. If $\mathfrak{p}$ does not contain p, let π be an element of Λ which is a generator of the ideal $\mathfrak{p}\Lambda[1/p]$ of $\Lambda[1/p]$. If $p \in \mathfrak{p}$, let π be a generator of $\mathfrak{p}$. (Such π exists by Corollary 10.6.)

11.5. For a commutative ring R, an R-module M, and an element x of M, define an ideal $J_R(x, M)$ of R by

$$J_R(x, M) = \{h(x); h \text{ is an } R\text{-homomorphism } M \to R\}.$$

If R is injective as an R-module, and N is an R-module containing M, we have $J_R(x, M) = J_R(x, N)$. In this case we sometimes denote $J_R(x, M)$ simply by $J_R(x)$. The ring $\Lambda_{m,n} = O_F[\mathrm{Gal}(\boldsymbol{Q}(\zeta_m)/\boldsymbol{Q})/p^n]$ is injective as a $\Lambda_{m,n}$-module.

PROPOSITION 11.6. *For $m \in \Sigma_d$ and $n \geq 1$, let $\xi_{m,n}$ be the image of ξ in $H^1(\boldsymbol{Z}[\zeta_m, 1/N], T/p^nT)$. Let $e = \mathrm{length}_{\Lambda_\mathfrak{p}}((\boldsymbol{H}^2_0)_\mathfrak{p})$. Then there exists an element t of $\Lambda\backslash\mathfrak{p}$ such that for any $m \in \Sigma_d$ and $n \geq 1$, we have the following inclusion between ideals of $\Lambda_{m,n}$*

$$t \cdot J_{\Lambda_{m,n}}(\xi_{m,n}) \subset \pi^e \Lambda_{m,n}. \tag{11.6.1}$$

We deduce Theorem 0.8 from this Proposition 11.6.

We prove first some lemmas.

LEMMA 11.7. *There exists $t \in \Lambda\backslash\mathfrak{p}$ such that for any $m \in \Sigma_d$, the image of $t \cdot J_\Lambda(\xi, \boldsymbol{H}^1)$ in Λ_m is contained in $J_{\Lambda_m}(\xi_m, H^1(\boldsymbol{Z}[\zeta_m, 1/N], T))$. Here ξ_m denotes the image of ξ in $H^1(\boldsymbol{Z}[\zeta_m, 1/N], T)$.*

Proof. By Proposition 10.7, there exists $s \in \Lambda \backslash \mathfrak{p}$ which kills the kernel and the cokernel of

$$\boldsymbol{H}^1 \otimes_\Lambda \Lambda_m \to H^1\left(\boldsymbol{Z}\left[\zeta_m, \frac{1}{N}\right], T\right)$$

for any $m \in \Sigma_d$. Let h be a Λ-homomorphism $\boldsymbol{H}^1 \to \Lambda$. Then there exists a Λ_m-homomorphism $H^1(\boldsymbol{Z}[\zeta_m, 1/N], T) \to \Lambda_m$ which induces $s^2 h$ on $\boldsymbol{H}^1 \otimes_\Lambda \Lambda_m$. This shows that the image of $s^2 J_\Lambda(\xi, \boldsymbol{H}^1)$ in Λ_m is contained in $J_{\Lambda_m}(\xi_m, H^1(\boldsymbol{Z}[\zeta_m, 1/N], T))$. So we can take $t = s^2$.

LEMMA 11.8. *Let t be as in Lemma 11.7. Then for any $m \in \Sigma_d$ and any $n \geq 1$, the image of $t \cdot J_\Lambda(\xi, \boldsymbol{H}^1)$ in $\Lambda_{m,n}$ is contained in $J_{\Lambda_{m,n}}(\xi_{m,n}, H^1(\boldsymbol{Z}[\zeta_m, 1/N], T/p^n))$.*

Proof. The image of $J_{\Lambda_m}(\xi_m, H^1(\boldsymbol{Z}[\zeta_m, 1/N], T))$ in $\Lambda_{m,n}$ is contained in $J_{\Lambda_{m,n}}(\xi_m \bmod p^n, H^1(\boldsymbol{Z}[\zeta_m, 1/N], T)/p^n))$. By the exactness of

$$0 \to H^1\left(\boldsymbol{Z}\left[\zeta_m, \frac{1}{N}\right], T\right)\Big/p^n \to H^1\left(\boldsymbol{Z}\left[\zeta_m, \frac{1}{N}\right], T/p^n\right)$$

and by the injectivity of $\Lambda_{m,n}$ as a $\Lambda_{m,n}$-module, we have

$$J_{\Lambda_{m,n}}\left(\xi_m \bmod p^n, H^1\left(\boldsymbol{Z}\left[\zeta_m, \frac{1}{N}\right], T\right)\Big/p^n\right)$$
$$= J_{\Lambda_{m,n}}\left(\xi_{m,n}, H^1\left(\boldsymbol{Z}\left[\zeta_m, \frac{1}{N}\right], T/p^n\right)\right).$$

Hence Lemma 11.8 follows from Lemma 11.7.

11.9. Now we deduce Theorem 0.8 from Proposition 11.6. By Proposition 11.6 and Lemma 11.8, there exists $t \in \Lambda \backslash \mathfrak{p}$ having the following property: For any $m \in \Sigma_d$ and any $n \geq 1$, the image of $t \cdot J_\Lambda(\xi, \boldsymbol{H}^1)$ in $\Lambda_{m,n}$ is contained in $\pi^e \Lambda_{m,n}$. By taking $\varprojlim$ for various m and n, we have that $t \cdot J_\Lambda(\xi, \boldsymbol{H}^1) = t \cdot J(\xi)$ is contained in $\pi^e \Lambda$. This proves $e \leq \mathrm{length}_{\Lambda_\mathfrak{p}}(\Lambda_\mathfrak{p}/J(\xi)_\mathfrak{p})$, and hence proves Theorem 0.8.

11.10. In the rest of §11, we reduce Proposition 11.6 to Proposition 11.14 which will be proved in §12.

In 11.10–11.13, we fix notations which are necessary to state Proposition 11.14.

First, take an element σ of $\mathrm{Gal}(\bar{\boldsymbol{Q}}/\boldsymbol{Q}^{\mathrm{ab}})$ such that $\dim_F(\mathrm{Ker}(1 - \sigma : V \to V)) = 1$. In the case $p \in \mathfrak{p}$, we take σ such that $\mathrm{Coker}(1 - \sigma : T \to T)$ is torsion free. We fix such σ.

Fix homomorphisms $\mu : T \to O_F$ and $\nu : O_F \to T$ having the properties stated in 5.4. Fix a $\boldsymbol{Z}_p$-basis η of $\boldsymbol{Z}_p(1)$.

Let the notations $\Omega, \Omega', \Omega_{m,n}, \Omega'_{m,n}$ be as in 5.1.

11.11. We fix elements $\tau_1, \ldots, \tau_k$ of $\mathrm{Gal}((\Omega')^{\mathrm{ab}}/\Omega')$ and an open subgroup U of $\mathrm{Gal}(\Omega^{\mathrm{ab}}/\Omega)$ as follows. Consider the homomorphism

$$\beta : \mathrm{Gal}((\Omega')^{\mathrm{ab}}/\Omega')) \to \boldsymbol{H}^2$$

obtained from $\beta_n(\Omega'/\boldsymbol{Q}(\zeta_m), T, \nu\eta^{-1})$ $(m \in \Sigma, n_d \geq 1)$. By 7.7, $(\boldsymbol{H}^2_0)_{\mathfrak{p}}$ coincides with the $\Lambda_{\mathfrak{p}}$-submodule of $\boldsymbol{H}^2_{\mathfrak{p}}$ generated by the image of $\mathrm{Gal}(\Omega^{\mathrm{ab}}/\Omega)$ under β. Hence $(\boldsymbol{H}^2_0)_{\mathfrak{p}}$ coincides with the $\Lambda_{\mathfrak{p}}$-submodule of $\boldsymbol{H}^2_{\mathfrak{p}}$ generated by $\beta(\tau)$ when τ ranges over all elements of $\mathrm{Gal}((\Omega')^{\mathrm{ab}}/\Omega')$ whose images in $\mathrm{Gal}(\Omega'/\Omega)$ coincide with the image of σ. By this fact, we can find inductively, elements $\tau_1, \tau_2, \ldots$ of $\mathrm{Gal}((\Omega')^{\mathrm{ab}}/\Omega')$ satisfying the following conditions (11.11.1), (11.11.2).

(11.11.1) For any i, the image of τ_i in $\mathrm{Gal}(\Omega/\Omega')$ coincides with that of σ.

(11.11.2) For $i \geq 1$, the annihilator of

$$\beta(\tau_i) \bmod \sum_{j=1}^{i-1} \Lambda_{\mathfrak{p}} \cdot \beta(\tau_j)$$

in $\Lambda_{\mathfrak{p}}$ coincides with the annihilator of the $\Lambda_{\mathfrak{p}}$-module $\boldsymbol{H}^2_{0,\mathfrak{p}}/(\sum_{j=1}^{i-1} \Lambda_{\mathfrak{p}} \cdot \beta(\tau_j))$.

Then for some $k \geq 1$, $\sum_{i=1}^{k} \Lambda_{\mathfrak{p}} \cdot \beta(\tau_i) = \boldsymbol{H}^2_{0,\mathfrak{p}}$. We fix such k.

For $1 \leq i \leq k$, let $e(i)$ be the length of the $\Lambda_{\mathfrak{p}}$-module $(\sum_{j=1}^{i} \Lambda_{\mathfrak{p}} \cdot \beta(\tau_j))/(\sum_{j=1}^{i-1} \Lambda_{\mathfrak{p}} \cdot \beta(\tau_j))$. (So the sum of $e(i)$ for $1 \leq i \leq k$ coincides with the length of the $\Lambda_{\mathfrak{p}}$-module $\boldsymbol{H}^2_{0,\mathfrak{p}}$.)

If we denote Λ by R, the image of $\boldsymbol{H}^2$ in $\boldsymbol{H}^2_{\mathfrak{p}}$ by M, the image of $\beta(\tau_i)$ in M by s_i, and $\pi^{e(i)}R$ by I_i, then the assumptions of Proposition 10.3 are satisfied. Let t_0 be the element $t \in \Lambda \backslash \mathfrak{p}$ of Proposition 10.3. The Jacobson radical $J(\Lambda)$ of Λ is an open ideal of Λ, and hence $t_0 \cdot (\sum_{i=1}^{k} J(\Lambda)s_i)$ is an open subset of $\sum_{i=1}^{k} \Lambda \cdot s_i$. Hence there exists an open subgroup U of $\mathrm{Gal}(\Omega^{\mathrm{ab}}/\Omega)$ whose image under β is contained in $t_0 \cdot (\sum_{i=1}^{k} J(\Lambda)s_i)$, such that the extension Ξ of Ω in Ω^{ab} corresponding to U is Galois over $\boldsymbol{Q}$. We fix t_0 and U.

11.12. For $m, n \geq 1$ and for an integer i such that $0 \leq i \leq k$, let $\Upsilon_{m,n,i}$ be the set of maps ω from $\{1, \ldots, i\}$ to the set of all good maximal ideals for (σ, m, n) (cf. 5.2) satisfying the following conditions (11.12.1) and (11.12.2).

(11.12.1) For each $j = 1, \ldots, i$, there exists an element u_j of U such that the image of $u_j\tau_j$ in $\prod_N(\Omega'_{m,n})/p^n$ (cf. 7.3) coincides with the Frobenius of $\omega(j)$.

(11.12.2) For $j = 1, \ldots, i$, let $\bar{\omega}(j)$ be the prime number lying under $\omega(j)$. Then the map $\bar{\omega}$ from the set $\{1, \ldots, i\}$ to the set of prime numbers is an injective map.

For $\omega \in \Upsilon_{m,n,i}$, let $r(\omega)$ be the product $\prod_{1 \leq j \leq i} \bar{\omega}(j)$.

(We interpret $\Upsilon_{m,n,0}$ to consist of one element ω which satisfies $r(\omega) = 1$.)

11.13. For $m \in \Sigma_d$ and $r, n \geq 1$ such that there exists $n' \geq n$ for which the 4-ple (mN, n, n', r) has the properties (2.1.1)–(2.1.3) (m in 2.1 is replaced here by

mN) let

$$\kappa_{r,m,n} \in H^1\left(\boldsymbol{Z}\left[\zeta_m, \frac{1}{N}\right], T/p^n\right)$$

be the image of $\kappa_r \in H^1(\boldsymbol{Z}[\zeta_{mN}, 1/N], T/p^n)$ under the norm map.

For example, $\kappa_{1,m,n} = \xi_{m,n}$.

PROPOSITION 11.14. *There exists $t \in \Lambda\backslash\mathfrak{p}$ having the following property: Let $m \in \Sigma_d, n \geq 1$. Then for any sufficiently large n', and any $1 \leq i \leq k$ and any $\omega \in \Upsilon_{mN,n',i-1}$, we have the inclusion*

$$t \cdot J_{\Lambda_{m,n}}(\kappa_{r(\omega),m,n}) \subset \sum_{\omega'} \pi^{e(i)} \cdot J_{\Lambda_{m,n}}(\kappa_{r(\omega'),m,n}),$$

where ω' ranges over the subset of $\Upsilon_{mN,n',i}$ consisting of elements whose restrictions to $\{1, \ldots, i-1\}$ coincide with ω.

Now we deduce Corollary 11.6 from this Proposition 11.14.

By downward induction on i, Proposition 11.14 implies the following Proposition 11.15. (Note the case $i = k$ of Proposition 11.15 is clear.)

PROPOSITION 11.15. *There exists an element t of $\Lambda\backslash\mathfrak{p}$ having the following property: Let $m \in \Sigma_d, n \geq 1$. Then for any sufficiently large n', for any $0 \leq i \leq k$ and for any $\omega \in \Upsilon_{mN,n',i}$, we have the following inclusion between ideals of $\Lambda_{m,n}$*

$$t \cdot J_{\Lambda_{m,n}}(\kappa_{r(\omega),m,n}) \subset \pi^{e(i+1)+\cdots+e(k)}\Lambda_{m,n}. \tag{11.15.1}$$

Consider the case $i = 0$ of Proposition 11.15. For $m \in \Sigma_d$ and $n \geq 1$, since $H^0(\boldsymbol{Q}(\zeta_{mN}), T \otimes (\boldsymbol{Q}/\boldsymbol{Z}))$ is finite by the assumption $w \neq 0$ (cf. 11.3.1), there exists $n' \geq n$ such that (mN, n, n') satisfies (2.1.1). Since the unique element ω of $\Upsilon_{mN,n',0}$ satisfies $\kappa_{r(\omega),m,n} = \xi_{m,n}$, the case $i = 0$ of Proposition 11.15 implies Corollary 11.6.

§12. The proof of Theorem 0.8, (II)

The aim of §12 is to complete the proof of Theorem 0.8.

In §12, we have reduced Theorem 0.8 to Proposition 11.14. In this §12, we prove Proposition 11.14. Let the notation and the assumption be as in Proposition 11.14 (in particular, we assume (11.3.1)–(11.3.4)).

Proposition 11.14 is clearly reduced to the following Proposition 12.1 and Proposition 12.2.

PROPOSITION 12.1. *There exists an element t of $\Lambda\backslash\mathfrak{p}$ having the following property: Let $m \in \Sigma_d, n \geq 1$. Then for any sufficiently large n', for any $1 \leq i \leq k$ and for any $\omega \in \Upsilon_{mN,n',i-1}$,*

$$t \cdot J_{\Lambda_{m,n}}(\kappa_{r(\omega),m,n}) \subset \sum_{\omega'} \Lambda_{m,n} \cdot \mu_{\omega'(i)}(\kappa_{r(\omega),m,n}(\bar{\omega}'(i)))$$

where ω' ranges over elements of $\Upsilon_{mN,n',\iota}$ whose restrictions to $\{1,\dots,i-1\}$ coincide with ω and which satisfy $\bar{\omega}'(i) \equiv 1 \bmod r(\omega)$. ($\kappa_{r(\omega),m,n}(\bar{\omega}'(i))$ denotes the image of $\kappa_{r(\omega),m,n}$ in $H^1(\boldsymbol{F}_{\bar{\omega}'(i)} \otimes \boldsymbol{Z}[\zeta_m], T/p^n)$.)

PROPOSITION 12.2. *There exists $t \in \Lambda\backslash\mathfrak{p}$ having the following property: Let $m \in \Sigma_d, n \geq 1$. Then for any sufficiently large n', for any $1 \leq i \leq k$ and for any $\omega \in \Upsilon_{mN,n',\iota-1}$, $\omega' \in \Upsilon_{mN,n',\iota}$ such that ω is the restriction of ω' to $\{1,\dots,i-1\}$ and such that $\bar{\omega}'(i) \equiv 1 \bmod r(\omega)$, we have*

$$t \cdot \mu_{\omega(i)}(\kappa_{r(\omega),m,n}(\bar{\omega}'(i))) \in \pi^{e(i)} \cdot J_{\Lambda_{m,n}}(\kappa_{r(\omega'),m,n}).$$

Proposition 12.1 follows from

LEMMA 12.3. *There exists an element t of $\Lambda\backslash\mathfrak{p}$ having the following property: Let $m \in \Sigma_d, n' \geq n \geq 1$, $1 \leq i \leq k$, $\omega \in \Upsilon_{mN,n',\iota-1}$. Let $h: H^1(\boldsymbol{Z}[\zeta_m, 1/Nr(\omega)], T/p^n) \to \Lambda_{m,n}$ be a $\Lambda_{m,n}$-homomorphism. Then $t \cdot h$ is a $\Lambda_{m,n}$-linear combination of $\Lambda_{m,n}$-homomorphisms of the form*

$$H^1\left(\boldsymbol{Z}\left[\zeta_m, \frac{1}{Nr(\omega)}\right], T/p^nT\right) \to H^1(\boldsymbol{F}_{\bar{\omega}'(i)} \otimes \boldsymbol{Z}[\zeta_m], T/p^nT) \xrightarrow{\mu_{\omega'(i)}} \Lambda_{m,n}$$

where ω' ranges over elements of $\Upsilon_{mN,n',\iota}$ whose restrictions to $\{1,\dots,i-1\}$ coincide with ω and which satisfy, $\bar{\omega}'(i) \equiv 1 \bmod r(\omega)$.

Proof of Lemma 12.3. We will deduce from Proposition 7.7 that there exists $t \in \Lambda\backslash\mathfrak{p}$ having the following property (12.3.1).

(12.3.1) For any $m, n \geq 1$ and any multiple M of N, the cokernel of

$$\Lambda_{m,n} \otimes U \to \mathrm{Hom}_{\Lambda_{m,n}}\left(H^1\left(\boldsymbol{Z}\left[\zeta_m, \frac{1}{M}\right], T/p^n\right), \Lambda_{m,n}\right)$$

is killed by t.

This t has the property stated in 12.4. Indeed, $t \cdot h$ is a $\Lambda_{m,n}$-linear combination of $\alpha_n(u)$ with $u \in U$, where $\alpha_n = \alpha_{n,Nr(\omega)}(\Omega'/\boldsymbol{Q}(\zeta_m), T, \mu)$ (cf. 7.3). Since $\alpha_n(u) = \alpha_n(u\tau_\iota) - \alpha_n(\tau_\iota)$, $t \cdot h$ is a $\Lambda_{m,n}$-linear combination of $\alpha_n(u\tau_\iota)$ with $u \in U$. Take a maximal ideal v of $O_{\Omega'_{mN,n'}}[1/mN'r(\omega)]$ satisfying the following (12.3.2) and (12.3.3).

(12.3.2) The Frobenius substitutions of v in the Galois groups

$$\Pi_{Nr(\omega)}(\Omega'_{mN,n'})/p^n \quad \text{and} \quad \mathrm{Gal}(\Omega_{mN,n'}(\zeta_{p^{n'}r(\omega)})/\Omega'_{mN,n'})$$

coincide with the images of $u\tau_\iota$, respectively.

(12.3.3) v is of degree one over $\boldsymbol{Q}$.

Such v exists by Chebotarev's density theorem, since these Galois groups are finite groups. This v is a good maximal ideal for (σ, m, n').

Define $\omega' \in \Upsilon_{mN,n',\iota}$ by $\omega'(j) = \omega(j)$ for $1 \leq j < i$ and by $\omega'(i) = v$. Then $\bar{\omega}'(i) \equiv 1 \bmod r(\omega)$ because the Frobenius of $\bar{\omega}'(i)$ in $\mathrm{Gal}(\boldsymbol{Q}(\zeta_{r(\omega)})/\boldsymbol{Q})$ coincides with the image of $u\tau_\iota$ which is the identity element. By Lemma 7.6 (1), $\alpha_n(u\tau_\iota)$ coincides with the composite map

$$H^1\left(\boldsymbol{Z}\left[\zeta_m, \frac{1}{Nr(\omega)}\right], T/p^nT\right) \to H^1(\boldsymbol{F}_{\bar{\omega}'(i)} \otimes \boldsymbol{Z}[\zeta_m], T/p^nT) \xrightarrow{\mu_{\omega'(i)}} \Lambda_{m,n}.$$

It remains to prove the existence of t satisfying (12.3.1). Consider the part of Proposition 7.7 concerning the map (7.7.1). Let $\mathfrak{a}, \boldsymbol{b}_1, \ldots, \boldsymbol{b}_r$ be as there. Then the image of $\mathfrak{a}$ under $\tilde{\Lambda} \to \Lambda$ is not contained in $\mathfrak{p}$ by (11.3.4), and the images of $\mathfrak{b}_i$ $(1 \leq i \leq r)$ under $\tilde{\Lambda} \to \Lambda$ is not contained in $\mathfrak{p}$ since the images are open in Λ. If $p \in \mathfrak{p}$, take $c = 1$ in Proposition 7.7 (we can take $c = 1$ since $T = \langle \nu \rangle$ and $T^* = \langle \mu \rangle$ by $(\mathrm{i}_{\mathrm{str}})$ and $(\mathrm{ii}_{\mathrm{str}})$ of 0.6). Then by what we have seen, there exists an element of $c\boldsymbol{a}\boldsymbol{b}_1 \cdots \boldsymbol{b}_r$ whose image t under $\tilde{\Lambda} \to \Lambda$ is not contained in $\mathfrak{p}$. By Proposition 7.7, this t has the property (12.3.1).

12.4. For the proof of Proposition 12.2, it is sufficient to prove that there exists $t \in \Lambda \backslash \mathfrak{p}$ having the following property: For $m, n, n', i, \omega, \omega'$ as in Proposition 12.2, there exists a $\Lambda_{m,n}$-homomorphism

$$g : H^1\left(\boldsymbol{Z}\left[\zeta_m, \frac{1}{Nr(\omega')}\right], T/p^n\right) \to \Lambda_{m,n}$$

such that the image of $\kappa_{r(\omega),m,n}(\bar{\omega}'(i))$ under

$$t\mu_{\omega'(i)} : H^1(\boldsymbol{F}_{\bar{\omega}'(i)} \otimes \boldsymbol{Z}[\zeta_m], T/p^n) \to \Lambda_{m,n}$$

is contained in $\pi^{e(i)} g(\kappa_{r(\omega'),m,n}) \cdot \Lambda_{m,n}$.

12.5. As a preliminary for the definition of g in 12.4, we define first $\Lambda_{m,a}$-homomorphisms $h_a : H^1(\boldsymbol{Z}[\zeta_m, 1/Nr(\omega')], T/p^a) \to \Lambda_{m,a}$ for integers a such that $1 \leq a \leq n'$. By 5.5, there exists an element $t_1 \in \Lambda \backslash \mathfrak{p}$ having the following property: For any $m, a \geq 1$, and for any good maximal ideal v for (σ, m, a) lying over a prime number l, t_1 kills the kernel and the cokernel of the homomorphisms

$$\psi_l : H^1(\boldsymbol{F}_l \otimes \boldsymbol{Z}[\zeta_m], T/p^a) \to H^0(\boldsymbol{F}_{l'} \otimes \boldsymbol{Z}[\zeta_m], T/p^a)$$
$$\mu_v : H^1(\boldsymbol{F}_l \otimes \boldsymbol{Z}[\zeta_m], T/p^a) \to \Lambda_{m,a}.$$

Fix such t_1, and define a $\Lambda_{m,a}$-homomorphism

$$h_a : H^1\left(\boldsymbol{Z}\left[\zeta_m, \frac{1}{Nr(\omega')}\right], T/p^a\right) \to \Lambda_{m,a} \quad (1 \leq a \leq n')$$

as follows. Let $v = \omega'(i)$, $l = \bar{\omega}'(i)$. Let $x \in H^1(\boldsymbol{Z}[\zeta_m, 1/Nr(\omega')], T/p^a)$. Then there exists $y \in H^1(\boldsymbol{F}_l \otimes \boldsymbol{Z}[\zeta_m], T/p^a)$ such that

$$t_1 \cdot \partial_l(x) = \psi_l(y)$$

$$\text{in } H^0(\boldsymbol{F}_l \otimes \boldsymbol{Z}[\zeta_m], T/p^a(-1)) \underset{(*)}{\cong} H^0(\boldsymbol{F}_l \otimes \boldsymbol{Z}[\zeta_m], T/p^a)$$

where $(*)$ is obtained by the basis η of $\boldsymbol{Z}_p(1)$. We regard $(*)$ as identification. Then $t_1 y$ depends only on x (is independent of the choice of y). Define

$$h_a(x) = \mu_v(t_1 y) \in \Lambda_{m,a}.$$

LEMMA 12.6. *The image of $t_1 h_a$ (which is an ideal of $\Lambda_{m,a}$) kills the cokernel of*

$$\partial_l : H^1\left(\boldsymbol{Z}\left[\zeta_m, \frac{1}{Nr(\omega')}\right], T/p^a\right) \to H^0(\boldsymbol{F}_l \otimes \boldsymbol{Z}[\zeta_m], T/p^a).$$

Proof. Let $x \in H^1(\boldsymbol{Z}[\zeta_m, 1/Nr(\omega')], T/p^a)$, and let y be as in 12.5. Since $\psi_l(y) \in \partial_l(H^1(\boldsymbol{Z}[\zeta_m, 1/Nr(\omega')], T/p^a)$, we have by Proposition 5.6 that $t_1 h_a(x) = t_1^2 \mu_v(y)$ kills the cokernel of ∂_l.

LEMMA 12.7. *There exists $t \in \Lambda \backslash \mathfrak{p}$ having the following property: Let $m, n, n', i, \omega, \omega'$ be as in Proposition* 12.2, *let $1 \le a \le n'$, and assume p^a kills $H^2(\boldsymbol{Z}[\zeta_m, 1/N], T)$. Let b be an element of Λ which kills the cokernel of*

$$(12.7.1) \quad \partial_{\bar{\omega}'(i)} : H^1\left(\boldsymbol{Z}\left[\zeta_m, \frac{1}{Nr(\omega')}\right], T/p^a\right) \to H^0(\boldsymbol{F}_{\bar{\omega}'(i)} \otimes \boldsymbol{Z}[\zeta_m], (T/p^a)(-1)).$$

Then

$$tb \bmod \mathfrak{a}_m \in \pi^{e(i)} \Lambda_m$$

where $\mathfrak{a}_m = \mathrm{Ker}(\Lambda \to \Lambda_m = O_F[\mathrm{Gal}(\boldsymbol{Q}(\zeta_m)/\boldsymbol{Q})])$.

Proof of Lemma 12.7. By Proposition 5.5, there exists $t_1 \in \Lambda \backslash \mathfrak{p}$ which kills the cokernel of $v_v : \Lambda_{m,a} \to H^0(\boldsymbol{F}_l \otimes \boldsymbol{Z}[\zeta_m], T/p^a)$ for any $m, a \ge 1$ and for any good maximal ideal v for (σ, m, a) lying over a prime number l. On the other hand, let $t_0 \in \Lambda \backslash \mathfrak{p}$ be as in 11.11. We show that $t = t_0 t_1$ (resp. $t = 2 t_0 t_1$) has the property stated in Lemma 12.7 if $m \ge 3$ or $p \ne 2$ (resp. if $m \le 2$ and $p = 2$). (If $p = 2$, then 2 is not contained in $\mathfrak{p}$ by Proposition 10.5 (4).)

Let $b \in \Lambda$ and assume b kills the cokernel of (12.7.1). By the localizing exact sequence

$$H^1\left(\boldsymbol{Z}\left[\zeta_m, \frac{1}{Nr(\omega')}\right], T/p^a\right) \to \bigoplus_{j=1}^{I} H^0(\boldsymbol{F}_{\bar{\omega}'(j)} \otimes \boldsymbol{Z}[\zeta_m], T/p^a(-1))$$

$$\to H^2\left(\boldsymbol{Z}\left[\zeta_m, \frac{1}{N}\right], T/p^a\right),$$

we have

$$b \cdot \mathrm{Im}\left(\iota_{\bar{\omega}'(i)} : H^0(\boldsymbol{F}_{\bar{\omega}'(i)} \otimes \boldsymbol{Z}[\zeta_m], T/p^a(-1)) \to H^2\left(\boldsymbol{Z}\left[\zeta_m, \frac{1}{N}\right], T/p^a\right)\right)$$
$$\subset \sum_{j=1}^{i-1} \mathrm{Im}\left(\iota_{\bar{\omega}(j)} : H^0(\boldsymbol{F}_{\bar{\omega}(j)} \otimes \boldsymbol{Z}[\zeta_m], T/p^a)(-1)) \to H^2\left(\boldsymbol{Z}\left[\zeta_m, \frac{1}{N}\right], T/p^a\right)\right).$$

Hence by 7.6 (2), we have

$$(12.7.2) \quad t_1 b \cdot \alpha_{n'}(u_i \tau_i) = \sum_{j=1}^{i-1} c_j \alpha_{n'}(u_j \tau_j) \text{ for some } c_j \in \Lambda \text{ in } H^2\left(\boldsymbol{Z}\left[\zeta_m, \frac{1}{N}\right], T/p^a\right)$$

with $u_j \in U$ $(1 \leq j \leq i)$. Assume $m \geq 3$ or $p = 2$. Then by the fact p^a kills $H^2(\boldsymbol{Z}[\zeta_m, 1/N], T)$ and by the first spectral sequence in 9.6, we have

$$\boldsymbol{H}^2/\mathfrak{a}_m \boldsymbol{H}^2 \xrightarrow{\cong} H^2\left(\boldsymbol{Z}\left[\zeta_m, \frac{1}{N}\right], T\right) \xrightarrow{\cong} H^2\left(\boldsymbol{Z}\left[\zeta_m, \frac{1}{N}\right], T/p^a\right).$$

Let M be the image of $\boldsymbol{H}^2$ in $\boldsymbol{H}^2_{\mathrm{p}}$, and let s_j $(1 \leq j \leq k)$ be the image of τ_j in M. Let $c_i = -t_1 b$. Then from (12.7.2), we obtain

$$\sum_{j=1}^{i} c_j(s_j + z_j) \in \mathfrak{a}_m M \quad \text{with } z_j \in t_0\left(\sum_{q=1}^{k} J(\Lambda) s_q\right).$$

By Proposition 10.3 (note $\mathfrak{a}_m \in \Psi$ by (11.3.3)), we have $t_0 c_i \in \mathfrak{a}_m + \pi^{e(i)}\Lambda$. Since $t_0 c_i = -t_0 t_1 b$, this implies $t_0 t_1 b \bmod \mathfrak{a}_m \in \pi^{e(i)}\Lambda_m$. In the case $m \leq 2$ and $p = 2$, by the reduction to the case $m \geq 3$ by norm argument, we have $2 t_0 t_1 b \bmod \mathfrak{a}_m \in \pi^{e(i)}\Lambda_m$.

12.8. Now we prove the existence of the homomorphism g having the property stated in 12.4 (this will prove Proposition 12.2 and hence 11.14 and Theorem 0.8).

Assume n' is sufficiently large. Then there exists an integer a such that $n \leq a \leq n'$, p^{a-n} kills $H^2(\boldsymbol{Z}[\zeta_m, 1/N], T)$ (note $H^2(\boldsymbol{Z}[\zeta_m, 1/N])$ is finite by 11.3.2), $p^{a-n} \in \pi^{e(i)}\Lambda_m$, and (mN, a, n') has the properties (2.1.1)–(2.1.3) ((m, n, n') in 2.1 is replaced here by (mN, a, n'); note $H^0(\boldsymbol{Q}(\zeta_{mN}), T \otimes (\boldsymbol{Q}/\boldsymbol{Z}))$ is finite because $w \neq 0$ by (11.3.1)).

Let t_1 be as in 12.5, and let t_2 be t of Lemma 12.7. By Lemmas 12.6 and 12.7, the image of $t_1 t_2 h_a$ is contained in $\pi^{e(i)}\Lambda_{m,a}$. Define a homomorphism

$$g' : H^1\left(\boldsymbol{Z}\left[\zeta_m, \frac{1}{Nr(\omega')}\right], T/p^a\right) \to \Lambda_{m,n}$$

as follows. For $x \in H^1(\boldsymbol{Z}[\zeta_m, 1/(Nr(\omega'))], T/p^a)$, write

$$t_1 t_2 \cdot h(x) = \pi^{e(i)} \cdot y \quad \text{with } y \in \Lambda_{m,a}$$

and let

$$g'(x) = \text{the image of } y \text{ in } \Lambda_{m,n}.$$

The image of y in $\Lambda_{m,n}$ depends only on x because

$$\mathrm{Ker}(\pi^{e(i)} : \Lambda_{m,a} \to \Lambda_{m,a}) \subset \mathrm{Ker}(p^{a-n} : \Lambda_{m,a} \to \Lambda_{m,a}) = p^n \Lambda_{m,a}.$$

This map g' factors as

$$H^1\left(\boldsymbol{Z}\left[\zeta_m, \frac{1}{Nr(\omega')}\right], T/p^a\right) \to H^1\left(\boldsymbol{Z}\left[\zeta_m, \frac{1}{Nr(\omega')}\right], T/p^n\right) \xrightarrow{g} \Lambda_{m,n}$$

for some $\Lambda_{m,n}$-homomorphism g. To see this, since $\Lambda_{m,n}$ is injective as a $\Lambda_{m,n}$-module and the sequence

$$H^1\left(\boldsymbol{Z}\left[\zeta_m, \frac{1}{Nr(\omega')}\right], T/p^{a-n}\right) \xrightarrow{p^n} H^1\left(\boldsymbol{Z}\left[\zeta_m, \frac{1}{Nr(\omega')}\right], T/p^a\right) \to H^1\left(\boldsymbol{Z}\left[\zeta_m, \frac{1}{Nr(\omega')}\right], T/p^n\right)$$

is exact, it is sufficient to show that g' kills the image of the above map "p^n". But this fact follows from the commutative diagram

$$\begin{array}{ccc} H^1\left(\boldsymbol{Z}\left[\zeta_m, \frac{1}{Nr(\omega')}\right], T/p^{a-n}\right) & \xrightarrow{t_1 t_2 h_{a-n}} & \pi^{e(i)}\Lambda_{m,a-n} \\ \downarrow{\scriptstyle p^n} & & \downarrow{\scriptstyle p^n} \\ H^1\left(\boldsymbol{Z}\left[\zeta_m, \frac{1}{Nr(\omega')}\right], T/p^a\right) & \xrightarrow{t_1 t_2 h_a} & \pi^{e(i)}\Lambda_{m,n}. \end{array}$$

Now we show that g has the property described in 12.4 for $t = t_1^3 t_2$. From Theorem 4.5, we obtain

$$\partial_l(\kappa_{r(\omega'),m,a}) = \psi_l(\kappa_{r(\omega),m,a}(l)) \quad (l = \bar{\omega}'(i)).$$

This shows

$$h_a(\kappa_{r(\omega'),m,a}) = t_1^2 \mu_v(\kappa_{r(\omega),m,a}(l)).$$

Hence

$$\pi^{e(i)} g(\kappa_{r(\omega'),m,n}) = t_1^3 t_2 \mu_v(\kappa_{r(\omega),m,n}(l)).$$

This proves Proposition 12.2.

§13. Selmer groups and finiteness theorems

In this section, we prove a finiteness theorem for the Selmer group of $T^*(1)$ (Theorem 13.2), a finiteness theorem for H^2 of T (Theorem 13.3) which is an improvement of Theorem 8.1.

13.1. Let T be a free $\boldsymbol{Z}_p$-module of finite rank on which $\mathrm{Gal}(\bar{\boldsymbol{Q}}/\boldsymbol{Q})$ acts continuously. Let $V = \boldsymbol{Q}_p \otimes_{\boldsymbol{Z}_p} T$. The Selmer group $\mathrm{Sel}(T)$ of T is defined as a subgroup of $H^1(\boldsymbol{Q}, V/T)$ in the following way ([BK]). For each prime number l, a $\boldsymbol{Q}_p$-subspace $H^1_f(\boldsymbol{Q}_l, V)$ of $H^1(\boldsymbol{Q}_l, V)$ is defined in [BK, 3.7] as follows. If $l \neq p$,

$$H^1_f(\boldsymbol{Q}_l, V) = \mathrm{Ker}(H^1(\boldsymbol{Q}_l, V) \to H^1(\boldsymbol{Q}_{l,\mathrm{ur}}, V))$$

where $\boldsymbol{Q}_{l,\mathrm{ur}}$ is the maximal unramified extension of $\boldsymbol{Q}_l$. For $l = p$,

$$H^1_f(\boldsymbol{Q}_p, V) = \mathrm{Ker}(H^1(\boldsymbol{Q}_p, V) \to H^1(\boldsymbol{Q}_p, B_{\mathrm{crys}} \otimes_{\boldsymbol{Q}_p} V))$$

where B_{crys} is the ring defined by Fontaine in [Fo]. $\mathrm{Sel}(T)$ is defined by

$$\mathrm{Sel}(T) = \mathrm{Ker}(H^1(\boldsymbol{Q}, V/T) \to \prod_l H^1(\boldsymbol{Q}_l, V/T)/\mathrm{Im}(H^1_f(\boldsymbol{Q}_l, V)))$$

where l ranges over all prime numbers.

For example, if T is the p-adic Tate module of an abelian variety A over $\boldsymbol{Q}$, $\mathrm{Sel}(T)$ coincides with the p-primary part of the classical Selmer group of A.

If $N \geq 1$, $p|N$, and the action of $\mathrm{Gal}(\bar{\boldsymbol{Q}}/\boldsymbol{Q})$ on T is unramified outside prime divisors of N, we have

$$\mathrm{Sel}(T) = \mathrm{Ker}\left(H^1\left(\boldsymbol{Z}\left[\frac{1}{N}\right], V/T\right) \to \bigoplus_{l|N} H^1(\boldsymbol{Q}_l, V/T)/\mathrm{Im}(H^1_f(\boldsymbol{Q}_l, V))\right).$$

In this case,

$$\mathrm{Sel}(T) \cong (\boldsymbol{Q}_p/\boldsymbol{Z}_p)^r \oplus (\text{finite group})$$

for some $r \geq 0$, because $H^1(\boldsymbol{Z}[1/N], V/T) \cong (\boldsymbol{Q}_p/\boldsymbol{Z}_p)^{r'} \oplus (\text{finite group})$ for some $r' \geq 0$.

THEOREM 13.2. *Let (F, T, N, N') be as in* 0.1, *let $(z_m)_m$ be an Euler system for (F, T, N, N'), and let $V = F \otimes_{O_F} T$. Assume that the conditions* (i), (ii), (iii) *in* 0.6 *are satisfied. Furthermore, assume that V is a de Rham representation as a representation of* $\mathrm{Gal}(\bar{\boldsymbol{Q}}_p/\boldsymbol{Q}_p)$ *over* $\boldsymbol{Q}_p$ ([Fo]), *that $H^1(\boldsymbol{Q}_p, V)/H^1_f(\boldsymbol{Q}_p, V)$ is one dimensional over F, and that the image of ξ* (cf. 0.7) *in $H^1(\boldsymbol{Q}_p, V)/H^1_f(\boldsymbol{Q}_p, V)$ is not zero. Then* $\mathrm{Sel}(T^*(1))$ *is a finite group.*

We will deduce Theorem 13.2 from the following finiteness Theorem 13.3.

THEOREM 13.3. *Let (F, T, N, N') be as in* 0.1, *let $(z_m)_m$ be an Euler system for (F, T, N, N'), and let $V = F \otimes_{O_F} T$. Assume that the conditions* (i), (ii), (iii) *in* 0.6 *are satisfied, and that the image of ξ (cf.* 0.7) *in $H^1(\boldsymbol{Z}[1/N], V)$ is not zero. Then the kernel of*

$$H^2\left(\boldsymbol{Z}\left[\frac{1}{p}\right], j_* T\right) \to H^2(\boldsymbol{Q}_p, T)$$

is a finite group, where j is the inclusion morphism from $\mathrm{Spec}(\boldsymbol{Z}[1/N])$ *to* $\mathrm{Spec}(\boldsymbol{Z}[1/p])$.

13.4. Theorem 8.1 is a consequence of Theorem 13.3. In fact, since the sequence

$$H^2\left(\boldsymbol{Z}\left[\frac{1}{p}\right], j_*T\right) \to H^2\left(\boldsymbol{Z}\left[\frac{1}{N}\right], T\right) \to \bigoplus_{\substack{l|N \\ l\neq p}} H^2(\boldsymbol{Q}_l, T)$$

is exact, $\mathrm{Ker}(H^2(\boldsymbol{Z}[1/N], T) \to \bigoplus_{l|N} H^2(\boldsymbol{Q}_l, T))$ is isomorphic to a quotient of $\mathrm{Ker}(H^2(\boldsymbol{Z}[1/p], j_*T) \to H^2(\boldsymbol{Q}_p, T))$, and hence the finiteness of the former follows from the finiteness of the latter.

13.5. The rest of §13 is devoted to the proofs of Theorem 13.2 and Theorem 13.3. Let the notation and the assumption be as in Theorem 13.3.

Define Λ (cf. 0.4) by taking $d = 1$. Let

$$\boldsymbol{H}^2(j_*T) = \varprojlim_n H^2\left(\boldsymbol{Z}\left[\zeta_{p^n}, \frac{1}{p}\right], j_*T\right).$$

For a prime number l, let

$$\boldsymbol{H}^q_l = \varprojlim_n H^q(\boldsymbol{Q}_l \otimes \boldsymbol{Q}(\zeta_{p^n}), T).$$

Let $W = \mathrm{Hom}_{O_F}(\varinjlim_n H^0(\boldsymbol{Q}(\zeta_{p^n}), T^*(1) \otimes_{O_F} F/O_F), F/O_F)$ which we regard as a Λ-module in the natural way.

We will use often the spectral sequences

$$E_2^{i,j} = \mathrm{Tor}_{-i}^{\Lambda}(F, \boldsymbol{H}^j(j_*T)) \quad \Rightarrow \quad E_\infty^i = H^i\left(\boldsymbol{Z}\left[\frac{1}{p}\right], j_*V\right) \tag{13.5.1}$$

$$E_2^{i,j} = \mathrm{Tor}_{-i}^{\Lambda}(F, \boldsymbol{H}^j) \quad \Rightarrow \quad E_\infty^i = H^i\left(\boldsymbol{Z}\left[\frac{1}{N}\right], V\right) \tag{13.5.2}$$

$$E_2^{i,j} = \mathrm{Tor}_{-i}^{\Lambda}(F, \boldsymbol{H}^j_l) \quad \Rightarrow \quad E_\infty^i = H^i(\boldsymbol{Q}_l, V) \tag{13.5.3}$$

where F is regarded as a Λ-module with respect to the O_F-homomorphism $\Lambda \to O_F$ which sends all elements of $\mathrm{Gal}(\boldsymbol{Q}(\zeta_{p^\infty})/\boldsymbol{Q})$ to 1.

Let $C = \{l; l \text{ is a prime number}, l|N, l \neq p\}$.

LEMMA 13.6. (1) $\boldsymbol{H}^1(j_*T) \cong \boldsymbol{H}^1$.

(2) *We have an exact sequence of* Λ*-modules*

$$0 \to \boldsymbol{H}^2(j_*T) \to \boldsymbol{H}^2 \to \bigoplus_{l\in C} \boldsymbol{H}^2_l.$$

(3) *We have an exact sequence of* Λ*-modules*

$$0 \to \boldsymbol{H}^2_0 \to \boldsymbol{H}^2(j_*T) \to \boldsymbol{H}^2_p \to W \to 0.$$

Proof. For $n \geq 0$, we have an exact sequence

$$\begin{aligned} 0 \to & H^1\left(\boldsymbol{Z}\left[\zeta_{p^n}, \frac{1}{p}\right], j_* T\right) \to H^1\left(\boldsymbol{Z}\left[\zeta_{p^n}, \frac{1}{N}\right], T\right) \\ & \to \bigoplus_{l \in C} H^0(\boldsymbol{F}_l \otimes \boldsymbol{Z}[\zeta_{p^n}], H^1(\boldsymbol{Q}_{l,\mathrm{ur}}, T)) \\ & \to H^2\left(\boldsymbol{Z}\left[\zeta_{p^n}, \frac{1}{p}\right], j_* T\right) \to H^2\left(\boldsymbol{Z}\left[\zeta_{p^n}, \frac{1}{N}\right], T\right) \\ & \to \bigoplus_{l \in C} H^2(\boldsymbol{Q}_l \otimes \boldsymbol{Q}(\zeta_{p^n}), T)). \end{aligned}$$

Here in $H^0(\boldsymbol{F}_l \otimes \boldsymbol{Z}[\zeta_{p^n}], H^1(\boldsymbol{Q}_{l,\mathrm{ur}}, T)), H^1(\boldsymbol{Q}_{l,\mathrm{ur}}, T)$ is regarded as a $\mathrm{Gal}(\bar{\boldsymbol{F}}_l/\boldsymbol{F}_l)$-module via the isomorphism $\mathrm{Gal}(\bar{\boldsymbol{F}}_l/\boldsymbol{F}_l) \cong \mathrm{Gal}(\boldsymbol{Q}_{l,\mathrm{ur}}/\boldsymbol{Q}_l)$, and regarded as an etale sheaf on $\mathrm{Spec}(\boldsymbol{F}_l \otimes \boldsymbol{Z}[\zeta_{p^n}])$. By taking the inverse limit of these exact sequences, (1) and (2) are reduced to

$$\varprojlim_n H^0(\boldsymbol{F}_l \otimes \boldsymbol{Z}[\zeta_{p^n}], H^1(\boldsymbol{Q}_{l,\mathrm{ur}}, T)) = 0 \tag{13.6.1}$$

for $l \in C$. We prove (13.6.1). By taking $\mathrm{Hom}_{O_F}(\ , F/O_F)$, (13.6.1) is equivalent to

$$\varinjlim_n H^1(\boldsymbol{F}_l \otimes \boldsymbol{Z}[\zeta_{p^n}], H^0(\boldsymbol{Q}_{l,\mathrm{ur}}, T^*(1) \otimes_{O_F} F/O_F)) = 0. \tag{13.6.2}$$

(13.6.2) follows from the fact that the degree of any finite extension of $\boldsymbol{F}_l(\zeta_{p^\infty})$ is prime to p.

Next (3) follows from the duality exact sequences

$$\begin{aligned} H^2\left(\boldsymbol{Z}\left[\zeta_{p^n}, \frac{1}{p}\right], j_* T\right) & \to H^2(\boldsymbol{Q}_p \otimes \boldsymbol{Q}(\zeta_{p^n}), T) \\ & \to \mathrm{Hom}_{O_F}(H^0(\boldsymbol{Q}(\zeta_{p^n}), T^*(1) \otimes F/O_F), F/O_F) \to 0 \end{aligned}$$

([Ma]).

LEMMA 13.7. *Let* $\mathfrak{p}$ *be the kernel of the* O_F*-homomorphism* $\Lambda \to O_F$ *which sends all elements of* $\mathrm{Gal}(\boldsymbol{Q}(\zeta_{p^\infty})/\boldsymbol{Q})$ *to* 1.

(1) *If* $\boldsymbol{H}^1_{\mathfrak{p}}$ *has a non-trivial torsion as a* $\Lambda_{\mathfrak{p}}$*-module,* $T \cong O_F$ *with the trivial action of* $\mathrm{Gal}(\bar{\boldsymbol{Q}}/\boldsymbol{Q})$.

(2) *If* $W_{\mathfrak{p}} \neq 0$, *then* $T \cong O_F(1)$ *as an* O_F*-module with an action of* $\mathrm{Gal}(\bar{\boldsymbol{Q}}/\boldsymbol{Q})$.

Proof. (1) The spectral sequence (13.5.2) shows

$$H^0(Q, V) = H^0\left(Z\left[\frac{1}{N}\right], V\right) \cong \mathrm{Tor}_1^{\Lambda_{\mathfrak{p}}}(F, \boldsymbol{H}^1_{\mathfrak{p}}).$$

If the $\Lambda_{\mathfrak{p}}$-module $H^1_{\mathfrak{p}}$ has a non-trivial torsion, then $\mathrm{Tor}_1^{\Lambda_{\mathfrak{p}}}(F, \boldsymbol{H}^1_{\mathfrak{p}}) \neq 0$ (note $\Lambda_{\mathfrak{p}}$ is a discrete valuation ring and F is the residue field of $\Lambda_{\mathfrak{p}}$), and hence

$H^0(Q, V) \neq 0$. By the simplicity of V (the condition (i) in 0.6), we see that $\dim_F(V) = 1$ and the action of $\mathrm{Gal}(\bar{\boldsymbol{Q}}/\boldsymbol{Q})$ on V is trivial.

(2) We have

$$W/\mathfrak{p}W \cong \mathrm{Hom}_{O_F}(H^0(\boldsymbol{Q}, T^*(1) \otimes_{O_F} F/O_F), F/O_F).$$

If $W_{\mathfrak{p}} \neq 0$, this shows that $H^0(\boldsymbol{Q}, T^*(1) \otimes_{O_F} F/O_F)$ is not a finite group, and hence $H^0(\boldsymbol{Q}, V^*(1)) \neq 0$. By the simplicity of V, we see that $\dim_F(V) = 1$ and the action of $\mathrm{Gal}(\bar{\boldsymbol{Q}}/\boldsymbol{Q})$ on $V^*(1)$ is trivial.

13.8. In the case $T = O_F$ (resp. $O_F(1)$), the map $H^2(\boldsymbol{Z}[1/p], j_*V) \to H^2(\boldsymbol{Q}_p, V)$ is injective. In fact, by duality [Ma], the kernel of this map is dual of $F \otimes_{\boldsymbol{Q}_p} \mathrm{Ker}(h_1)$ (resp. $F \otimes_{\boldsymbol{Q}_p} \mathrm{Ker}(h_0)$), where

$$h_r : H^1\left(\boldsymbol{Z}\left[\frac{1}{p}\right], \boldsymbol{Q}_p(r)\right) \to H^1(\boldsymbol{Q}_p, \boldsymbol{Q}_p(r)) \quad (r \in \boldsymbol{Z}).$$

h_1 is rewriten as $\boldsymbol{Z}[1/p]^\times \otimes \boldsymbol{Q}_p \to \boldsymbol{Q}_p^\times \otimes \boldsymbol{Q}$ and hence is injective. h_0 is injective as is seen by class field theory.

13.9. Now we prove Theorem 13.3. By Lemma 13.7 and 13.8, we may assume that $\boldsymbol{H}^1_{\mathfrak{p}}$ is torsion free as a $\Lambda_{\mathfrak{p}}$-module and $W_{\mathfrak{p}} = 0$. We assume these.

By the spectral sequence (13.5.2), $F \otimes_{\Lambda_{\mathfrak{p}}} \boldsymbol{H}^1_{\mathfrak{p}}$ is embedded in $H^1(\boldsymbol{Z}[1/N], V)$. Hence the image of ξ in $F \otimes_{\Lambda_{\mathfrak{p}}} \boldsymbol{H}^1_{\mathfrak{p}}$ is not zero. Since $\boldsymbol{H}^1_{\mathfrak{p}}$ is torsion free, this implies $J(\xi)_{\mathfrak{p}} = \Lambda_{\mathfrak{p}}$. By Theorem 0.8, this implies $\boldsymbol{H}^2_{0,\mathfrak{p}} = 0$. By the exact sequence in Lemma 13.6 (3) and by $W_{\mathfrak{p}} = 0$, we have

$$\boldsymbol{H}^2(j_*T)_{\mathfrak{p}} \xrightarrow{\cong} (\boldsymbol{H}^2_p)_{\mathfrak{p}}.$$

By the spectral sequences (13.5.1) and (13.5.3), $F \otimes_{\Lambda_{\mathfrak{p}}}$ of this isomorphism gives an isomorphism

$$\boldsymbol{H}^2\left(\boldsymbol{Z}\left[\frac{1}{p}\right], j_*V\right) \xrightarrow{\cong} \boldsymbol{H}^2(\boldsymbol{Q}_p, V).$$

This completes the proof of Theorem 13.3.

13.10. Now we prove Theorem 13.2. Let the assumption be as in Theorem 13.2. Let $S = \mathrm{Hom}_{\boldsymbol{Z}_p}(\boldsymbol{Q}_p, \mathrm{Sel}(T^*(1)))$. Then

$$S \cong \mathrm{Ker}\left(H^1\left(\boldsymbol{Z}\left[\frac{1}{p}\right], j_*V^*(1)\right) \to H^1(\boldsymbol{Q}_p, V^*(1))/H^1_f(\boldsymbol{Q}_p, V^*(1))\right).$$

Since $\mathrm{Sel}(T^*(1)) \cong (\boldsymbol{Q}_p/\boldsymbol{Z}_p)^r \oplus (\text{finite group})$ for some $r \geq 0$ and $\mathrm{Hom}_{\boldsymbol{Z}_p}(\boldsymbol{Q}_p, (\boldsymbol{Q}_p/\boldsymbol{Z}_p)^r \oplus (\text{finite group})) \cong (\boldsymbol{Q}_p)^r$, it is sufficient to show $S = 0$.

In the perfect pairing of Tate duality

$$H^1(\boldsymbol{Q}_p, V) \times H^1(\boldsymbol{Q}_p, V^*(1)) \to F,$$

$H^1_f(\boldsymbol{Q}_p, V)$ and $H^1_f(\boldsymbol{Q}_p, V^*(1))$ are the annihilators of each other ([BK, 3.8]). Hence, the duality exact sequence

$$H^1\left(\boldsymbol{Z}\left[\frac{1}{p}\right], j_*V\right) \to H^1(\boldsymbol{Q}_p, V) \to H^1\left(\boldsymbol{Z}\left[\frac{1}{p}\right], j_*V^*(1)\right)^*$$
$$\to H^2\left(\boldsymbol{Z}\left[\frac{1}{p}\right], j_*V\right) \to H^2(\boldsymbol{Q}_p, V)$$

([Ma]) gives an exact sequence

$$H^1\left(\boldsymbol{Z}\left[\frac{1}{p}\right], j_*V\right) \to H^1(\boldsymbol{Q}_p, V)/H^1_f(\boldsymbol{Q}_p, V) \to S^*$$
$$\to H^2\left(\boldsymbol{Z}\left[\frac{1}{p}\right], j_*V\right) \to H^2(\boldsymbol{Q}_p, V)$$

($S^* = \mathrm{Hom}_F(S, F)$). By Theorem 13.3, $H^2(\boldsymbol{Z}[1/p], j_*V) \to H^2(\boldsymbol{Q}_p, V)$ is injective. Hence, it is sufficient to prove that $H^1(\boldsymbol{Z}[1/p], j_*V) \to H^1(\boldsymbol{Q}_p, V)/H^1_f(\boldsymbol{Q}_p, V)$ is surjective. But $H^1(\boldsymbol{Q}_p, V)/H^1_f(\boldsymbol{Q}_p, V)$ is one-dimensional and the image of ξ in this space comes from $H^1(\boldsymbol{Z}[1/p], j_*V)$ because $\boldsymbol{H}^1(j_*T) = \boldsymbol{H}^1$ (Lemma 13.6 (1)).

Remark 13.11. We can apply the method in this paper to get the analogous results for the Selmer group over K where $K/\boldsymbol{Q}$ is a finite abelian extension, and for the second etale cohomology over $O_k[1/p]$ of j_*T. See [Ka$_2$].

References

[AV] Artin, M. and Verdier, J.-P., Seminar on étale cohomology of number fields, Wood Hole (1964).

[Be] Beilinson, A., Higher regulators and values of L-functions, J. Soviet Math., **30** (1985) 2036–2070.

[BK] Bloch, S. and Kato, K., L-functions and Tamagawa numbers of motives, The Grothendieck Festschrift, vol. 1, Birkhäuser, 1990, 334–400.

[BO] Berthelot, P and Ogus, A., Notes on Crystalline Cohomology, Princeton Univ. Press, 1978.

[Bo] Bourbaki, N., Groupes et Algèbras de Lie, Eléments de mathématique, **16**, Hermann, 1960.

[CE] Cartan, H. and Eilenberg, S., Homological Algebra, Princeton Math. Ser., **19**, Princeton Univ. Press, 1956.

[De] Deligne, P., La conjecture de Weil, I, Inst. Hautes Études Sci. Publ. Math., **43** (1974), 273–307; II, ibid., **52** (1980), 137–252.

[Fo] Fontaine, J.-M., Sur certains types de représentations p-adiques du groupe de Galois d'un corps local: constructuion d'un anneau de Barsotti-Tate, Ann. of Math., **115** (1982), 529–577

[Ja] JANNSEN, U., On the l-adic cohomology of varieties over number fields and its Galois cohomology, Galois Group over $\boldsymbol{Q}$, Springer, 1989, 315–360.

[Ka_1] KATO, K., Lectures on the approach to Iwasawa theory for Hasse-Weil L-functions via B_{dR}, Lecture Notes in Math., **1553**, Springer, 1993, 50–163.

[Ka_2] KATO, K., p-adic Hodge theory and special values of zeta functions of elliptic cusp forms, in preparation.

[Ko_1] KOLYVAGIN, V. A., Finiteness of $E(\boldsymbol{Q})$ and Ш$(E/\boldsymbol{Q})$ for a class of Weil curves, Izv. Acad. Nauk SSSR, **52** (1988), 522–540, 670–671.

[Ko_2] KOLYVAGIN, V A., Euler systems, The Grothendieck Festschrift, vol. 2, Birkhäuser, 1990 435–483.

[La] LAZARD, M., Groupes analytiques p-adiques, Inst. Hautes Études Sci. Publ. Math., **26** (1965), 1–219.

[Ma] MAZUR, B., Notes on étale cohomology of number fields, Ann. Sci. École. Norm. Sup., **6** (1973), 521–556.

[MW] MAZUR, B. AND WILES, A., Class fields of abelian extensions of $\boldsymbol{Q}$, Invent. Math., **76** (1984), 179–330.

[Pe] PERRIN-RIOU, B., Systèmes d'Euler p-adique et théorie d'Iwasawa, to appear.

[Ru_1] RUBIN, K., The main conjecture, Appendix to Lang, S., Cyclotomic Fields I and II, Grad. Texts in Math., **121**, Springer, 1990, 397–420.

[Ru_2] RUBIN, K., The "main conjecture" of Iwasawa theory for imaginary quadratic fields, Invent. Math., **103** (1991), 25–68.

[Ru_3] RUBIN, K., Stark units and Kolyvagin's "Euler systems", J. Reine Angew. Math., **425** (1992), 141–154.

[Ru_4] RUBIN, K., Euler systems and modular elliptic curves, London Math. Soc. Lecture Note Ser., **254**, Cambridge Univ. Press, Cambridge, 1998, 351–367.

[Se_1] SERRE, J.-P., Corps Locaux, Hermann, 1960.

[Se_2] SERRE, J.-P., Cohomologie Galoisienne, Lecture Notes in Math., **5**, Springer, 1964.

[Se_3] SERRE, J.-P., Sur les groupes de congruences des variétés, Izv. Akad. Nauk SSSR, **28** (1964) 3–18, II, ibid., **35** (1971), 731–735.

[Se_4] SERRE, J.-P., Abelian l-adic Representations and Elliptic Curves, Benjamin, 1968.

[Ta] TATE, J., On the conjectures of Birch and Swinnerton-Dyer and a geometric analog, Sém. Bourbaki, 1965–66, $n°306$, Bemjamin, 1966.

DEPARTMENT OF MATHEMATICAL SCIENCES
THE UNIVERSITY OF TOKYO
KOMABA, TOKYO 153-8914, JAPAN