The Galois Module Structure of Certain Arithmetic Principal Homogeneous Spaces

M. J. TAYLOR

Department of Mathematics, UMIST, Manchester, England

Communicated by A. Fröhlich

Received February 20, 1991

1. INTRODUCTION AND STATEMENT OF RESULTS

In this paper we obtain Galois module results for rings of integers of certain abelian extensions of cyclotomic extensions and of division fields for elliptic curves with complex multiplication. In the cyclotomic case we consider the rings of integers of non-ramified extensions, and in the elliptic case we are concerned with extensions arising from the Selmer group of the curve. In each case we can describe those rings of integers which are free Galois modules, by means of $L$-function congruences. This then is a further instance of how Galois module structure is dominated by $L$-functions, with the classic case being the tame theory (see [F], [T3]), where it is the root numbers of the sympletic characters of the Galois group which determine the Galois module structure. In broad terms, the results of this paper arise from marrying the algebraic results in [T1] and certain powerful results from Iwasawa theory (both cyclotomic and elliptic).

For aesthetic reasons, as well as for the sake of brevity, we introduce notation which will simultaneously cover both the cyclotomic and the elliptic case. We begin by defining the notation for

**The cyclotomic case.** $p$ denotes an odd prime number, $\mu_p$ is the group of $p$th roots of unity in $\mathbb{Q}^c$, the algebraic closure of $\mathbb{Q}$ in $\mathbb{C}$, and for a number field $M \subset \mathbb{Q}^c$ we put $\Omega_M = \text{Gal}(\mathbb{Q}^c/M)$. We define $p = p\mathbb{Z} = p^*$, $K = \mathbb{Q}$, $N = F = \mathbb{Q}(\mu_p)$, $A = \text{Gal}(N/K)$. Let $\kappa: A \to \mathbb{Z}_p^\times$ denote the $p$-adic character given by the action of $A$ on $\mu_p$, i.e., $\zeta^\delta = \zeta^{\kappa(\delta)}$ for all $\delta \in A$.

In the sequel we let $G$ denote an isomorphic copy of $\mu_p$, which we always view as an $\Omega_\mathbb{Q}$ module in the natural way: the point here is that, in due course, $\mu_p$ will naturally occur as a Galois group and it will be advantageous to use the symbol $G$ for such occurrences.

Let $A$ denote the group algebra $N[G]$, and let $B = \text{Map}(G, N)$, the $N$-algebra of all maps from $G$ to $N$; then $A$ and $B$ are Cartier dual to each
other. Let $\mathfrak{U} = \mathcal{O}_N[G]$, $\mathfrak{B} = \text{Map}(G, \mathcal{O}_N)$, so that $\mathfrak{U}$ and $\mathfrak{B}$ are Hopf orders in $A$ and $B$, respectively; moreover $\mathfrak{U}$ and $\mathfrak{B}$ are $\mathcal{O}_N$-Cartier dual to each other.

The elliptic case. $E$ denotes an elliptic curve defined over an imaginary quadratic number field $K$, which has complex multiplication by $\mathcal{O}_K$; note that this implies that $K$ must have class number one, since by complex multiplication theory $K$ must coincide with its Hilbert classfield.

Let $\phi$ denote the Grössencharakter associated to $E/K$ and let $\mathfrak{f}$ denote its conductor; thus for any prime ideal $p$ of $\mathcal{O}_K$ not dividing $\mathfrak{f}$, the endomorphism $\phi(p) \in \mathcal{O}_K$ induces the Frobenius on $E$ mod $p$. Let $\ast$ denote complex conjugation. Let $p > 3$ denote a prime number which is coprime to $\mathfrak{f}$ and which splits in $K$, with $p\mathcal{O}_K = p\mathcal{O}_K$. Let $\pi = \phi(p)$, so that $p = \pi\mathcal{O}_K$, $p^* = \pi^*\mathcal{O}_K$, and suppose that $\pi + \pi^* \neq 1$, i.e., that $p$ is not anomalous for $E/K$.

Let $E_\pi$ resp. $E_{\pi^*}$ denote the group of $\pi$ resp. $\pi^*$ division points in $E(\mathbb{Q}^c)$; for the same reasons as those given in the cyclotomic case, it will be advantageous to let $G$ denote an isomorphic copy of $E_{\pi^*}$, endowed with the natural $\mathcal{O}_K$ action. We then define number fields $F = K(E_\pi)$, $F_\ast = K(E_{\pi^*})$, $N = F(\mu_p) = F_\ast(\mu_p)$. We put $\mathcal{A} = \text{Gal}(N/F_\ast)$, and we remark that from time to time we shall abuse notation a little and view $\mathcal{A}$ as $\text{Gal}(F/K)$ (since $F$ and $F_\ast$ are linearly disjoint over $K$ by Corollary 1.7, Chapter II, in [dS]).

We let $\kappa$ denote the $\mathbb{Z}_p^\times$ valued character which gives the action of $A = \text{Gal}(N/K)$ on $E_\pi$.

By Theorem 2 in [CW] it is known that $E/F$ has everywhere good reduction; this implies that the group scheme $E_{\pi^*}/\mathcal{O}_N$ is finite and flat. Since $E_{\pi^*} \subset E(N)$, the group scheme $E_{\pi^*}/N$ is constant, and therefore there is a unique Hopf order $\mathfrak{B}$ in $B = \text{Map}(G, N)$ with $\text{Spec}(\mathfrak{B}) = E_{\pi^*}/\mathcal{O}_N$. We then put $A = N[G]$ and we let $\mathfrak{U}$ denote the $\mathcal{O}_N$-Cartier dual of $\mathfrak{B}$ in $A$; thus of course $\mathfrak{U}$ is a Hopf order in $A$.

From this point on we shall frequently be able to treat the two cases together. Before proceeding further, we need to introduce various groups of units:

(1a) For each prime $\mathfrak{B}|p$, we let $v_{\mathfrak{B}} : N^\times \rightarrow \mathbb{Z}$ denote the associated discrete valuation. We define semi-local unit groups

$$U_N = \left\{ u \in \prod_{\mathfrak{B}|p} N_{\mathfrak{B}} \mid v_{\mathfrak{B}}(u - 1) \geq 1 \quad \forall \mathfrak{B}|p \right\}$$

$$U_N^{(p)} = \left\{ u \in \prod_{\mathfrak{B}|p} N_{\mathfrak{B}} \mid v_{\mathfrak{B}}(u - 1) \geq p \quad \forall \mathfrak{B}|p \right\}.$$
The groups $U_F$, $U_F^{(p)}$ are defined in the same way, so that, because $p$ is unramified in $N/F$,

$$U_F = F_p \cap U_N, \quad U_F^{(p)} = F_p \cap U_N^{(p)}.$$  

(1b) $Y_F = \mathcal{O}_F^\times \cap U_F$, $Y_N = \mathcal{O}_N^\times \cap U_N$, and $Y_F^{(p)} = \mathcal{O}_F^{(p)} \cap U_F^{(p)}$, $Y_N^{(p)} = \mathcal{O}_N^{(p)} \cap U_N^{(p)}$.  

(1c) $V_N$ is the subgroup of elements $v \in N^\times$ that have the property that for each prime $q$ of $\mathcal{O}_N$, we can write $v = u_q x_q^p$ with $x_q \in N_q^\times$ and

$$u_q \in \begin{cases} \mathcal{O}_{N,q}^\times & \text{if } q \nmid p \\ U_{N,q}^{(p)} & \text{if } q | p. \end{cases}$$  

(1d) $C_F$ denotes the groups of cyclotomic resp. elliptic units in $F$ which lie in $U_N$ (see Chapter 8 in [Wn] and Section 2, Chapter II, in [dS] for their definitions).

Recall that an $\mathcal{O}_F$ order $\mathfrak{C}$ in a Galois algebra $D/N$ (with Gal$(D/N) = G$), which is stable under the action of $\mathfrak{A}$, is called a principal homogeneous space (p.h.s) for $\mathfrak{A}$ if there exists an isomorphism of Galois algebras

$$\mathfrak{C} \otimes_{\mathcal{O}_N} \mathfrak{C}' \cong \mathfrak{B} \otimes_{\mathcal{O}_N} \mathcal{O}'$$

which respects $\mathfrak{A}$ action on the left factors, $\mathcal{O}'$ action on the right factors, for some extension ring of integers $\mathcal{O}'$ of $\mathcal{O}$. The set of isomorphism classes of such orders is written $PH(\mathfrak{B})$, and this has a natural group structure. (To reconcile this definition with the usual definition of a p.h.s. see [T1].)

We write $PH(\mathfrak{B})$ for the group of p.h.s. for the $N$-algebra $\mathfrak{B}$: thus $PH(\mathfrak{B})$ is the same thing as the group of isomorphism classes of Galois algebras over $N$ with Galois group $G$. A standard Galois descent argument shows that

$$PH(\mathfrak{B}) \cong H^1(\Omega_N, G) = \text{Hom}(\Omega_N, G).$$

We also note, for future reference, that by the faithful flatness over $\mathcal{O}_N$ of any p.h.s. for $\mathfrak{B}$, extension of scalars induces an injection

$$PH(\mathfrak{B}) \to PH(\mathfrak{B}).$$

By a standard result (see [S]), $\mathfrak{B}$ is always locally free over $\mathfrak{A}$; it then follows from (2) that $\mathfrak{C}$ is a locally projective $\mathfrak{A}$-module; since $A$ is a commutative separable algebra and since by the Normal Basis Theorem $D \cong A$ as $A$-modules, it follows that $\mathfrak{C}$ is a locally free $\mathfrak{A}$-module of rank one.

Writing $\mathfrak{C}(\mathfrak{A})$ for the locally free class group of $\mathfrak{A}$, we obtain a homomorphism

$$\psi : PH(\mathfrak{B}) \to \mathfrak{C}(\mathfrak{A}).$$
For details of the general version of this homomorphism for arbitrary finite commutative group schemes see [W]; for details concerning the elliptic case see [T2]; for the cyclotomic case see [C].

The groups of p.h.s. in the cyclotomic and elliptic cases arise very naturally in the following two ways: In the cyclotomic case, \( \mathfrak{B} \) has trivial \( \mathfrak{O}_N \)-discriminant, and so by (2) it follows easily that a p.h.s. \( \mathfrak{C} \) of \( \mathfrak{B} \) occurs as the ring of integers of a non-ramified extension of \( N \) (i.e., a Galois algebra extension, and not necessarily a field extension). In the elliptic case it can be shown that each p.h.s. \( \mathfrak{C} \) of \( \mathfrak{B} \) occurs as an order of a Galois extension \( C \) of \( N \) coming from the \( \pi \)-part of the Selmer group of \( E/N \); more precisely, in Proposition 5 of [T2] it is shown that \( \mathfrak{C} \) is the largest \( \mathfrak{A} \)-module contained in \( \mathfrak{O}_C \), the integral closure of \( \mathfrak{O}_N \) in \( C \). (For a more complete account of the role of p.h.s. as Galois modules see [T4].) Thus, in summary, we see that the \( \mathfrak{A} \)-module structure of p.h.s. \( \mathfrak{C} \) of \( \mathfrak{B} \) is a natural and important invariant of \( \mathfrak{B} \). The aim of this article is to derive estimates for \( \text{Ker } \psi \), that is to say we shall describe the number of p.h.s. \( \mathfrak{C} \) which are free \( \mathfrak{A} \)-modules.

From Théorème 2 in [T1] (and see also [H]) we know that we can use the unit groups of (1) to parameterise both \( \text{PH} \) and \( \text{Ker } \psi \) in the cyclotomic and in the elliptic cases.

**Theorem 1.** The composite isomorphism

\[
\theta : \text{PH}(B) \cong H^1(\Omega_N, G) = \text{Hom}(\Omega_N, G) \cong \text{Hom}(\Omega_N, \mu_p) \cong N^x/N^x_p
\]

induces isomorphisms

\[
\text{PH}(\mathfrak{B}) \cong V_N/N^x_p
\]

\[
\text{Ker}(\psi) \cong \frac{Y_N^{(p)}N^x_p}{N^x_p}.
\]

In the sequel we view \( \Delta \) as acting on \( \text{PH}(B) \) via the isomorphism \( \text{PH}(B) \cong \text{Hom}(\Omega_N, G) \). Thus in the cyclotomic case \( \theta \) is \( \Delta \)-equivariant; however, in the elliptic case, an isomorphism \( G \cong \mu_p \) is obtained by composing with \( W(-, P) \) for \( P \in E_\kappa \), where \( W(, ) \) is the Weil-pairing; thus in this case \( \theta \) twists the \( \Delta \)-action by \( \kappa \); so explicitly, if \( f \in \text{Hom}(\Omega_N, G) \), then for \( \delta \in \Delta, \omega \in \Omega_N, f^\delta(\omega) = f(\omega^{\delta^{-1}})^\delta \) and

\[
W(f, P)^\delta(\omega) = W(f(\omega^{\delta^{-1}}), P)^\delta = W(f^\delta(\omega), P^\delta) = W(f^\delta, P)^{\kappa(\delta)}(\omega).
\]

Note that from Theorem 1 it is clear that in both cases \( \text{PH}(\mathfrak{B}) \) is \( \Delta \)-stable—because \( V_N \) is.
Recall $A = \text{Gal}(N/K)$ has order coprime to $p$. Given any $\mathbb{Z}_p A$-module $M$, we write $M_i$ for the eigenspace of $M$ on which $A$ acts via $\kappa^i$ (so that $i$ should be read as an element of $\mathbb{Z}/(p-1)\mathbb{Z}$).

Explicitly, if $e_i = (1/|A|) \sum_{\lambda \in A} \kappa^i(\lambda) \lambda^{-1}$, then

$$M_i = Me_i.$$ 

We claim that, by restriction, $\theta$ induces

$$(5) \quad \text{Ker} \; \psi_i \cong \left( \frac{Y_F^{(p)} F^{\times p}}{F^{\times p}} \right)_j = \left( \frac{Y_F F^{\times p}}{F^{\times p}} \right)_j,$$

where in the cyclotomic case $j = i$, and in the elliptic case $i + 1 = j$ (since here $\theta$ twists by $\kappa$). This is immediate from Theorem 1 in the cyclotomic case—since $N = F$; in the elliptic case this follows from the fact that, because $p$ is non-ramified in $N/F$, we have maps

$$\left( \frac{Y_N^{(p)} N^{\times p}}{N^{\times p}} \right)_j \cong \left( \frac{Y_F^{(p)} F^{\times p}}{F^{\times p}} \right)_j$$

and these will be isomorphisms since both sides are $p$-groups, while the field degree $[N:F]$ is coprime to $p$.

Our aim now is to study the $\text{Ker} \; \psi_i$ via (5). Recall that by Dirichlet's unit theorem, it is known that

$$\dim_{\mathbb{Q}}((Y_F \otimes \mathbb{Z}_p) e_j) = \begin{cases} 0 & \text{if either } j = 0 \text{ or also if } j \text{ is odd in the cyclotomic case;} \\ 1 & \text{otherwise.} \end{cases}$$

(6a) **Cyclotomic case.** Since $\mu_p$ is the torsion subgroup of $Y_F$, and since $\mu_p \cap Y_F^{(p)} = \{1\}$, from the above we conclude that

$$\dim_{F_p}(\text{Ker} \; \psi_i) = \begin{cases} 0 & \text{if } i \text{ odd or } i = 0 \\ \leq 1 & \text{if } i \text{ even and } i \neq 0. \end{cases}$$

(The fact that $\text{Ker} \; \psi_{\text{odd}} = (0)$ is also a consequence of results in [B].)

(6b) **Elliptic case.** Recall that in this case $\theta$ twists by $\kappa$; also, $Y_F^{(p)}$ contains no torsion, since it could contain only $p$-power torsion, but, of course, $p^*$ is unramified in $F/\mathbb{Q}$. The above therefore shows that

$$\dim_{F_p}(\text{Ker} \; \psi_i) = \begin{cases} 0 & \text{if } i \equiv p - 2 \\ \leq 1 & \text{if } i \not\equiv p - 2. \end{cases}$$

Let $h_{F,i}$ denote the cardinality of the $i$-part of the $p$-Sylow subgroup of the
classgroup of $F$, and we write $L_p(s, \kappa')$ for the $p$-adic $L$-function associated to $\kappa'$.

The first of the two main theorems of the paper is:

**Theorem 2 (Cyclotomic).** (a) In all cases $\dim_{\mathbb{F}_p}(\ker \psi_i) \leq 1$.

(b) If $i = 0$ or if $i$ is odd, then $\ker \psi_i = \{0\}$.

(c) If $i$ is even and $i \neq 0$, then $\ker \psi_i = \{0\}$ if, and only if, $L_p(1, \kappa') h_{F,i}^{-1} \not\equiv 0 \mod(p)$. So, in particular if $L_p(1, \kappa')$ is a $p$-adic unit then $\ker \psi_i = \{0\}$.

**Remark 1.** According to Vandiver's conjecture, the $h_{F,i}$ are all 1 for all even $i$.

**Remark 2.** Theorem 2 may be seen as a (partial) answer to the questions raised at the end of [C].

Let $L_{p,i}$ denote the $p$-adic $L$-function defined on the Grössencharaktere of the Galois group over $K$ of the union of all ray classfields of $K$ whose conductor is $i$ times a power of $p$; we abuse notation (slightly) and write $\kappa$ for the $\mathbb{Z}_p^\times$ valued character which gives the action of this Galois group on $E_\pi$. As per the previous theorem, $h_{F,i}$ denotes the cardinality of the $i$-part of the $p$-Sylow subgroup of the classgroup of $F$.

Our second main result is

**Theorem 3.** (a) In all cases $\dim_{\mathbb{F}_p}(\ker \psi_i) \leq 1$.

(b) $\ker \psi_{p-2} = \{0\}$.

(c) For $i \neq 0$, $\ker \psi_{i-1} = \{0\}$ if, and only if,

$$L_{p,i}(\kappa^{-1}) h_{F,i}^{-1} \not\equiv 0 \mod(p).$$

In particular, if $L_{p,i}(\kappa^{-1}) \not\equiv 0 \mod(p)$, then $\ker \psi_{i-1} = \{0\}$.

**Remark.** If $p$ is anomalous, then the statement of the theorem holds for all $i \neq 1$.

It is important to note that, in contradistinction to the cyclotomic situation, here there is always a non-trivial element in $\ker \psi$. More precisely from [ST] we have

**Theorem 4.** The image of $E_{\pi,i}$ in $\text{PH}(\mathfrak{B})$ is always contained in $\ker \psi$.

The remainder of this article is structured as follows: In Section 2 we consider the cyclotomic case and prove Theorem 2; then in Section 3 we deal with elliptic case and prove Theorem 3.
2. CYCLOTOMIC CASE

In both this and the next section, for $x, y \in \mathbb{Q}_p^{\times}$, we say $x \sim y$ iff $xy^{-1}$ is a unit in $\mathfrak{O}_p^\times$, the ring of integers of $\mathbb{Q}_p$.

Parts (a) and (b) of the theorem follow at once from (6a). Suppose now that $i$ is even and $i \neq 0$.

From (5) we know that

$$\text{Ker } \psi_i \cong \left( \frac{Y(p)\mathbb{F}_p^\times}{Y(p)\mathbb{F}_p^{\times \mathfrak{p}}} \right)_i.$$

Let $\bar{Y}_p$ denote the closure of $Y_p$ in $U_p$. Recall that by a theorem of Brumer $\bar{Y}_{F,i} \cong \mathbb{Z}_p$ (see [Br]). By standard theory (see, for instance, Section 8, Chapter 13, in [Wn]), $U_{F,i}$ is $\mathbb{Z}_p$-cyclic and moreover

$$U_{F,i}^{(p)} = (U_{F,i})^p.$$

Thus we have a commutative diagram

$$
\begin{array}{cccccc}
0 & \to & p\mathbb{Z}_p & \to & \mathbb{Z}_p & \to & \mathbb{F}_p & \to & 0 \\
& & 1 & \to & U_{F,i}^{(p)} & \to & U_{F,i} & \to & U_{F,i} / U_{F,i}^{(p)} & \to & 1 \\
& & 1 & \to & \bar{Y}_{F,i}^{(p)} & \to & \bar{Y}_{F,i} \\
\end{array}
$$

From (7) we know that $\text{Ker } \psi_i = 0$ iff

$$
\left( \frac{Y(p)\mathbb{F}_p^\times}{Y(p)\mathbb{F}_p^{\times \mathfrak{p}}} \right)_i = 0 \iff \left( \frac{Y(p)\mathbb{F}_p^\times}{Y(p)} \right)_i = 0
$$

since by using (8) we easily obtain the equality $Y_{F,i}^{(p)} \cap \mathbb{F}_p^{\times \mathfrak{p}} = Y_{F,i}^p$. This then shows that $\text{Ker } \psi_i = 0$ iff $\bar{Y}_{F,i}^{(p)} = \bar{Y}_{F,i}^p$. On the one hand this occurs iff $U_{F,i} = \bar{Y}_{F,i}$: indeed, using the commutative diagram we see that if $U_{F,i} = \bar{Y}_{F,i}$, then $\bar{Y}_{F,i}^{(p)} = \bar{Y}_{F,i}^p$; on the other hand if $U_{F,i} \neq \bar{Y}_{F,i}$, then $\bar{Y}_{F,i} \subset U_{F,i}^{(p)}$, and so $\bar{Y}_{F,i} = \bar{Y}_{F,i}^p$.

As in (1d) we let $C_F$ denote the cyclotomic units of $F$; note that, in the usual way, we have

$$(U_{F,i} : Y_{F,i}) = (U_{F,i} : C_F)(\bar{Y}_{F,i} : C_{F,i})^{-1}.$$
However, by the celebrated result of Mazur and Wiles in [MW] (or see Kolyvagin’s proof in [K])

\[ h_{F,i} = (\bar{Y}_{F,i}, \bar{C}_{F,i}). \]

Thus it now remains to show that for such \( i \)

\[ (U_{F,i}, \bar{C}_{F,i}) \sim L_p(1, \kappa^i). \tag{9} \]

From this limit formula for the \( p \)-adic \( L \)-function at 1 (see Theorem 5.18 in [Wn]), it is known that for even \( i \neq 0 \),

\[ L_p(1, \kappa^i) = -\frac{\tau(\kappa^i)}{p} \sum_{a=1}^{p-1} \kappa^{-i}(a) \log_p(1 - \zeta^a). \tag{10} \]

Here \( \zeta \) denotes a primitive \( p \)-th root of unity in \( \mathbb{Q}_p^\ast \), \( \log_p \) is any branch of the \( p \)-adic logarithm, \( \kappa \) is viewed as a \( (p \)-adic valued) Dirichlet character \( \mod(p) \) in the usual way, and \( \tau(\kappa^i) \) denotes the Gauss sum

\[ \tau(\kappa^i) = \sum_{a=1}^{p-1} \kappa^i(a) \zeta^a. \tag{11} \]

Let \( g \) denote a generator of the cyclic group \( (\mathbb{Z}/p\mathbb{Z})^\times \), and set

\[ \eta = \frac{1 - \zeta^g}{1 - \zeta}. \]

Then \( \bar{C}_{F,i} \), the closure of the cyclotomic units of \( F \) in \( U_F \), is generated by \( \eta^{p-1} \) and \( \zeta \) over \( \mathbb{Z}_p \Delta \). We note that, by definition, \( \zeta \in \bar{C}_{F,1} \) so that \( \eta^{(p-1)} \in \Delta \), will generate \( \bar{C}_{F,i} \) over \( \mathbb{Z}_p \Delta \) for all even \( i \neq 0 \). Since

\[ \log_p(\eta) = \log_p(1 - \zeta^a) - \log_p(1 - \zeta), \]

where \( \sigma \in \Delta \) has the property that \( \zeta^a = \zeta^g \), we deduce from (10) that

\[ (1 - \kappa^i(g)) L_p(1, \kappa^i) = \frac{\tau(\kappa^i)}{p} \sum_{a=1}^{p-1} \kappa^{-i}(a) \log_p(\eta^a\sigma). \tag{12} \]

Next we need two standard cyclotomic results:

**Proposition 1.** \( p^{-1} \tau(\kappa^i) \sim (1 - \zeta)^{-i} \) for \( 0 < i \leq p - 1 \).

*Proof.* See [IV, Sect. 3] of [L].

**Proposition 2.** For \( 2 \leq i \leq p - 1 \), the map \( \alpha: u \rightarrow p^{-1} \tau(\kappa^i) \log_p(u) \) is an isomorphism \( \alpha: U_{F,i} \cong \mathbb{Z}_p \).
Proof. By the very definition of $U_{F,i}$, $\Delta$ acts on $\log_p(U_{F,i})$ via $\kappa^i$. However, from (11), it follows that $\Delta$ acts on $\tau(\kappa^i)$ via $\kappa^{-i}$, and so

\begin{equation}
\alpha(U_{F,i}) \subset \mathbb{Q}_p.
\end{equation}

It is well known that for $i \neq 0,1$, $U_{F,i}$ is generated by a local unit $u \in 1 + \mathcal{O}_i$, $u \notin 1 + \mathcal{O}_i^+$ (see, for instance, Lemma 9 in [CW]). Now for such $i$ and for $x \in \mathcal{O}_i$, $\log_p(1+x) \equiv x \mod \mathcal{O}_i^+$, and so the logarithm induces an isomorphism $U_{F,i}/U_{F,i}^p \cong \mathcal{O}_i / \mathcal{O}_i^+$. We therefore conclude from Proposition 1 and from (13) that $\alpha(U_{F,i}) = \mathbb{Z}_p$.

The proof of (9) now follows easily: from Proposition 2 we know that

\begin{equation}
(U_{F,i}; C_{F,i}) \sim \alpha(\eta^{(p-1)i}),
\end{equation}

by (12)

\begin{align*}
&= (1 - \kappa^i(g)) L_p(1, \kappa^i) \\
&\sim L_p(1, \kappa^i).
\end{align*}

3. ELLIPTIC CASE

Parts (a) and (b) of Theorem 3 follow from (6b). So now fix $i \neq 0$. Recall that by Lemma 12 in [CW], $U_{F,i}$ will be $\mathbb{Z}_p$ cyclic and (8) holds, for all $i$, in this case, since $p$ is not anomalous. So, reasoning exactly as in the cyclotomic case—but taking into account the fact that $\theta$ twists by $\kappa$—it follows that $\text{Ker} \psi_{i-1} = 0$ iff $U_{F,i} = \mathcal{O}_{F,i}$.

Again we have

\begin{equation}
(U_{F,i}; \mathcal{O}_{F,i}) = (U_{F,i}; \mathcal{C}_{F,i})(\mathcal{O}_{F,i}; \mathcal{C}_{F,i})^{-1},
\end{equation}

where this time $\mathcal{C}_F$ denotes the closure of the group of elliptic units of $F$ (see (II, Sect. 2) in [dS]). By a result of Kolyvagin (see Theorem 8 of [R], or [K])

\begin{equation}
(U_{F,i}; \mathcal{C}_{F,i}) = h_{F,i}
\end{equation}

and so, in this case, we are reduced to showing that

\begin{equation}
(U_{F,i}; C_{F,i}) \sim L_p(\kappa^{-i}).
\end{equation}

Let $g = f_p$ and let $K(g)$ denote the ray classfield of $K$ with conductor $g$. By Theorem 5.2, Chapter II, of [dS] we have a $p$-adic Kronecker limit
formula, which, in our situation, gives the following: fix an embedding of \( \mathbb{Q}^c \) into \( \mathbb{Q}_p^c \); then

\[
L_{p, i}(\kappa^{-i}) = \frac{-1}{12} \frac{G(\kappa^i)}{g} \sum_{\sigma \in \text{Gal}(K(g)/K)} \kappa^{-i}(\sigma) \log_p(\phi(1)^{\sigma}),
\]

where \( g \) is the positive generator of \( \mathfrak{g} \cap \mathbb{Z} \) (so that \( p \) divides \( g \) exactly once); \( \phi_g(1) \) denotes the Robert elliptic unit associated to \( g \); for \( 0 < i < p - 1 \), \( G(\kappa^i) \) is the normalised Gauss sum

\[
G(\kappa^i) = v \sum_{\gamma \in \mathfrak{d}} \kappa^i(\gamma) \zeta^{-\kappa^i(\gamma)},
\]

where \( v \) denotes a certain \((p - 1)\)st root of unity (see (11.3.11) in [dS]). As previously, we know that, for \( 0 < i < p - 1 \), \( G(\kappa^i) \sim (1 - \zeta)^{-i} \). Next we obtain an analogue for Proposition 2.

**Proposition 3.** For \( 1 < i < p - 1 \), the map

\[
\alpha: u \rightarrow G(\kappa^i) \log_p(u)
\]

is an isomorphism from \( U_{F,i} \) to \( v\mathbb{Z}_p \), for some \( p \)-adic unit \( v \in \mathbb{Q}_p^c \).

**Remark.** Since \( G(\kappa^i) \in \mathbb{Q}_p^c(\mu_p) \) and since \( F_p \) contains no \( p \)th roots of unity (because \( p \) is not anomalous), it follows that \( v \notin \mathbb{Q}_p^c \).

**Proof.** By Lemmas 9 and 12 in [CW], \( U_{F,i} \) is \( \mathbb{Z}_p \) cyclic and is generated by an element of the form \( 1 + x \) for \( x \in \mathfrak{d} \backslash \mathfrak{d}^{i+1} \). Again \( \log_p \) induces an isomorphism

\[
U_{F,i}/U_{F,i}^p \cong \mathfrak{d}^i/\mathfrak{d}^{i+1}
\]

(for \( i = 1 \), we again use the fact that \( p \) is not anomalous); and so the reasoning of Proposition 2 again holds.

**Lemma.** Let \( I \) denote the augmentation ideal in \( \mathbb{Z}_p \mathcal{A} \). Then \( \mathcal{C}_p \) coincides with the \( p \)-adic closure of

\[
N \kappa(1)^{(p-1)i}.
\]

**Proof.** Set \( H = \text{Gal}(K(g)/K) \) and by linearity extend \( \phi_g \) to a \( \mathbb{Z}H \)-homomorphism

\[
\phi_g: \mathbb{Z}H \rightarrow \mathfrak{d}_K^c.
\]

For an \( \mathfrak{d}_K \)-ideal \( a \) coprime to \( Ng \), let \( \sigma_a \in H \) denote the corresponding
Artin automorphism. Let \( J \) denote the \( \mathbb{Z}H \) ideal generated by all elements of the form \( \sigma_a - Na \) for integral \( a \) coprime to \( Ng \). We claim that

\[
\mathbb{Z}H \supseteq J \supseteq m\mathbb{Z}H
\]

with \( m \) coprime to \( p \): for by classfield theory \( J \) identifies as the annihilator of the group of roots of unity of \( K(g) \); since \( p^* \) is unramified in \( K(g) \) there are no non-trivial \( p \)-power roots of unity in \( K(g) \). This then establishes (16).

Let \( I' \) denote the augmentation ideal of \( \mathbb{Z}H \), and let \( J_0 = J \cap I' \). Then \( (I': J_0) \) divides \( (\mathbb{Z}H: J) \), which is prime to \( p \). However, because \( p \nmid 6 \), from the very definition of the elliptic units (see Section 5 of [CW] and also II.2.6 of [dS]), \( \mathbb{C}_p^* \) is equal to the \( p \)-adic closure of

\[
N_{K(g)/F}(\phi_g(J_0)) \cap U_F.
\]

This, together with the fact that \( (I': J_0) \) is prime to \( p \) gives the result.

By the above lemma it now follows that

\[
(U_{F,i}; \mathcal{C}_i) \sim \frac{1}{p} \alpha(N_{K(g)/F}(\phi_g(1))(p - 1) e_i)
\]

\[
= \frac{G(\kappa^i)}{p} \sum_{\sigma \in \text{Gal}(K(g)/K)} \kappa^{-i}(\sigma) \log_p(\phi_g(1)^{\sigma})
\]

since \( p \sim g \) and using (15)

\[
(U_{F,i}; \mathcal{C}_i) \sim L_{p,i}(\kappa^{-i}).
\]

This then establishes (14), as required.

REFERENCES


