On elliptic units and p-adic Galois representations attached to elliptic curves

Álvaro Lozano-Robledo

Colby College, Department of Mathematics
8800 Mayflower Hill, Waterville, ME 04901. Phone: (207) 859 5834

Abstract

Let K be a quadratic imaginary number field with discriminant $D_K \neq -3, -4$ and class number one. Fix a prime $p \geq 7$ which is not ramified in K and write h_p for the class number of the ray class field of K of conductor p. Given an elliptic curve A/K with complex multiplication by K, let $\overline{\rho_A}\colon \operatorname{Gal}(\overline{K}/K(\mu_{p^\infty})) \to \operatorname{SL}(2, \mathbb{Z}_p)$ be the representation which arises from the action of Galois on the Tate module. Herein it is shown that if $p \nmid h_p$ then the image of a certain deformation $\rho_A\colon \operatorname{Gal}(\overline{K}/K(\mu_{p^\infty})) \to \operatorname{SL}(2, \mathbb{Z}_p[[X]])$ of $\overline{\rho_A}$ is "as big as possible", that is, it is the full inverse image of a Cartan subgroup of $\operatorname{SL}(2, \mathbb{Z}_p)$. The proof rests on the theory of Siegel functions and elliptic units as developed by Kubert, Lang and Robert.

Key words: p-adic Galois representations, elliptic curves, elliptic units
1991 MSC: 11F80 (primary), 11G05, 11G16 (secondary).

1 Introduction

The theory of elliptic curves has produced very interesting families of "large" Galois representations which codify arithmetic information about the given curve itself, interesting in its own right. Let A be an elliptic curve over $\mathbb{Q}$, let p be a prime, and let

$$\overline{\rho_A}\colon \operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \operatorname{GL}(2, \mathbb{Z}_p)$$

be the natural representation coming from the Tate module of A. In his famous paper [21], J.-P. Serre proved that the image of such representations is "as large as possible", meaning that, if the curve does not have complex multiplication,

Email address: alozano@colby.edu (Álvaro Lozano-Robledo).

the image is an open subgroup of $\mathrm{GL}(2,\mathbb{Z}_p)$ and the representation is in fact surjective for almost all primes p. In the case that the elliptic curve A has complex multiplication by a quadratic imaginary field K, the image of $\overline{\rho_A}$ was studied in detail by M. Deuring [4], [5], Serre and J. Tate [22], and others. For example, if the curve has CM by the full ring of integers of K, it can be shown that the image of $\mathrm{Gal}(\overline{\mathbb{Q}}/K) \longrightarrow \mathrm{GL}(2,\mathbb{Z}_p)$ is isomorphic to $(\mathbb{Z}_p \otimes \mathcal{O}_K)^*$ (in particular, it is abelian).

More recently, D. Rohrlich considered the following. Fix a prime $p \geq 7$, let K be a number field, and write $\widetilde{K}$ for the extension of K generated by the roots of unity in $\overline{K}$ of p-power order. Given an elliptic curve E over $K(j)$ with transcendental invariant $j(E) = j$, Rohrlich [18] (see also [1] for an extension in a more general context) found that the universal deformation of $\overline{\rho_E}$, viewed in the first instance as a representation of $\mathrm{Gal}(\overline{K(j)}/\overline{K}(j))$ with appropriately constrained ramification, descends to a Galois representation

$$\rho_E\colon \mathrm{Gal}\left(\overline{K(j)}/\widetilde{K}(j)\right) \longrightarrow \mathrm{SL}(2,\mathbb{Z}_p[[X]])$$

such that the representation $\rho_E|_{X=0}$ is equivalent to the natural representation of $\mathrm{Gal}(\overline{K(j)}/\widetilde{K}(j))$ on $T_p(E)$, the Tate module of E.

Let A be an elliptic curve over K with $j(A) \neq 0, 1728$ and suppose that A coincides with the fiber of E at $j = j(A)$. Then ρ_E can be restricted to the decomposition group corresponding to a place extending $j = j(A)$ of $\widetilde{K}(j)$, to obtain a representation

$$\rho_A\colon \mathrm{Gal}(\overline{K}/\widetilde{K}) \longrightarrow \mathrm{SL}(2,\mathbb{Z}_p[[X]]).$$

In light of the results of Deuring, Serre and Tate, one would naturally want to know how large is the image of this representation. Let $\overline{\rho}_A\colon \mathrm{Gal}(\overline{K}/\widetilde{K}) \rightarrow \mathrm{SL}(2,\mathbb{F}_p)$ be the representation induced by the action of Galois on the points of order p on A. In [18], Rohrlich proved in the case $K = \mathbb{Q}$ that if $\overline{\rho}_A$ is surjective and $\nu_p(j(A)) = -1$ then ρ_A is surjective, where ν_p is the usual p-adic valuation on $\mathbb{Q}$. This result has been generalized in [9] to elliptic curves defined over arbitrary number fields with non-integral j-invariant at a prime above p.

The argument in [18] depends on the theory of Siegel functions as developed in [6]. D. S. Kubert and S. Lang studied the specialization of Siegel functions (by specializing j) in two cases: when the j-invariant is not integral (at p), and when j is integral with complex multiplication. The proof of Rohrlich's result above exploits the first case. The second case is the subject of this paper.

Let K be a quadratic imaginary number field with discriminant $D_K \neq -3, -4$ and class number $h_K = 1$. Fix a prime $p \geq 7$ which is not ramified in K. Let $\overline{K}$ be an algebraic closure of K and let $\widetilde{K}$ be defined as before. Given an elliptic curve A/K with complex multiplication by K (and precisely by the ring of integers $\mathcal{O}_K$), let $\overline{\rho_A}\colon \mathrm{Gal}(\overline{K}/\widetilde{K}) \longrightarrow \mathrm{SL}(2,\mathbb{Z}_p)$ be the representation determined up to equivalence by the action of $\mathrm{Gal}(\overline{K}/\widetilde{K})$ on $T_p(A)$. As mentioned earlier, the theory of complex multiplication describes the image of this map, which is a Cartan subgroup $\mathfrak{C}'$ of $\mathrm{SL}(2,\mathbb{Z}_p)$, unique up to isomorphism.

Also, let $\rho_A\colon \mathrm{Gal}(\overline{K}/\widetilde{K}) \longrightarrow \mathrm{SL}(2,\mathbb{Z}_p[[X]])$ be the deformation of $\overline{\rho_A}$ defined as above. We write $K(p)$ for the ray class field of K of conductor $p\mathcal{O}_K$, and let h_p be the class number of $K(p)$.

Theorem 1.1 *If $p \nmid h_p$ then $\rho_A\left(\mathrm{Gal}(\overline{K}/\widetilde{K})\right)$ is "as big as possible", that is, it is the full inverse image of $\mathfrak{C}'$ under the map*

$$\pi_X\colon \mathrm{SL}(2,\mathbb{Z}_p[[X]]) \longrightarrow \mathrm{SL}(2,\mathbb{Z}_p), \quad X \longmapsto 0.$$

1.1 Examples

Let $K = \mathbb{Q}(\sqrt{-19})$ and let A be the elliptic curve defined by the equation $y^2 + y = x^3 - 38x + 90$, which has complex multiplication by the maximal order of K. Let $p = 7$ and let $K(7)$ denote the ray class field of K of conductor $7\mathcal{O}_K$. The class number of $K(7)$ is one (this number was computed using PARI [11] and the Scientific Computing and Visualization facilities at Boston University). Since $p = 7$ does not divide $h_7 = 1$ we can use Theorem 1.1 to conclude that the image of the representation $\rho_A\colon \mathrm{Gal}(\overline{K}/\widetilde{K}) \to \mathrm{SL}(2,\mathbb{Z}_7[[X]])$ is the full inverse image of a Cartan subgroup of $\mathrm{SL}(2,\mathbb{Z}_7)$.

There are many other cases where the hypothesis of the theorem are known to be true. By proving an extension of Kummer's criterion for imaginary quadratic fields (see also [3], [19], [23] for similar criteria), G. Robert was able to give numerous examples of *regular* primes ([14], Appendix B, p. 352-363). For instance, he shows that $\gcd(h_7, 7) = 1$ for $K = \mathbb{Q}(\sqrt{-d})$ with $d = 1, 2, 11, 43, 67$, and 163 (7 is inert in all these fields; we saw above that this is true for $d = 19$ as well, and 7 splits in this case). For $K = \mathbb{Q}(\sqrt{-67})$, the class number h_p is relatively prime to p for (but not only) $5, 7$, while the primes $p = 19, 23, 37, 71, 89, 163$ are known to be irregular, i.e. $p \mid h_p$.

Remark 1.2 *Note that for the examples above such that p is split in K, say $p\mathcal{O}_K = \wp \cdot \overline{\wp}$, Robert gives the divisibility properties of the class number h'_p of the ray class field of K of conductor $\wp$. However, it is easy to prove that if $p \mid h'_p$ then $p \mid h_p$. Robert shows that $p \mid h'_p$ for $K = \mathbb{Q}(\sqrt{-67})$ and $p = 19, 23, 71, 89$ and 163. Since we know that $p = 37$ is a classical irregular prime, i.e. 37 divides the class number of $\mathbb{Q}(\zeta_{37})$, it can be shown that 37 also divides h_{37}, for any quadratic imaginary field K of class number one.*

Acknowledgements

I would like to thank David Rohrlich for his dedication as my advisor. I would also like to thank the referee for several helpful remarks which have made some of the proofs more efficient than in the original manuscript.

2 Surjectivity of a Galois Representation

Let K be a number field, fix $\overline{K}$, an algebraic closure of K, and let j be transcendental over K. Let E be an elliptic curve defined over the field $K(j)$ such that $j(E) = j$. Given a prime number $p \geq 7$, the natural action of $\mathrm{Gal}(\overline{K(j)}/\overline{K}(j))$ on the group of p-torsion points of E induces a representation $\widetilde{\pi_E}\colon \mathrm{Gal}(\overline{K(j)}/\overline{K}(j)) \longrightarrow \mathrm{SL}(2, \mathbb{F}_p)$. The universal deformation of $\widetilde{\pi_E}$, with respect to certain ramification conditions (see [15], [18]), is an epimorphism

$$\pi_E\colon \mathrm{Gal}(\overline{K(j)}/\overline{K}(j)) \longrightarrow \mathrm{SL}(2, \mathbb{Z}_p[[X]]).$$

Let $\widetilde{K}$ be the extension of K generated by all roots of unity of p-power order. In [16], [17], Rohrlich showed that π_E descends to an epimorphism

$$\rho_E\colon \mathrm{Gal}(\overline{K(j)}/\widetilde{K}(j)) \longrightarrow \mathrm{SL}(2, \mathbb{Z}_p[[X]]).$$

Notice that ρ_E encapsulates arithmetic information which was not present in π_E.

Let A be an elliptic curve defined over K with j-invariant $j(A) \neq 0, 1728$ and suppose that A coincides with the fiber of E at $j = j(A)$. Choose a place σ of $\overline{K(j)}$ extending the place $j = j(A)$ of $\widetilde{K}(j)$, and write D and I for the corresponding decomposition and inertia subgroups of $\mathrm{Gal}(\overline{K(j)}/\widetilde{K}(j))$. We "specialize" the representation ρ_E to $j = j(A)$ by restricting the map to the decomposition group D. By the ramification constraints of the universal deformation (see [17]), the map ρ_E is unramified outside $\{0, 1728, \infty\}$, thus $\rho_E|_D$ factors through $D/I \cong \mathrm{Gal}(\overline{K}/\widetilde{K})$. We obtain a representation:

$$\rho_A\colon \mathrm{Gal}(\overline{K}/\widetilde{K}) \longrightarrow \mathrm{SL}(2, \mathbb{Z}_p[[X]]).$$

If we write $\overline{\rho_A}\colon \mathrm{Gal}(\overline{K}/\widetilde{K}) \longrightarrow \mathrm{SL}(2, \mathbb{Z}_p)$ for the representation determined up to equivalence by the natural action of $\mathrm{Gal}(\overline{K}/\widetilde{K})$ on the Tate module of A, then, by construction, ρ_A is a deformation of $\overline{\rho_A}$, and in particular $\rho_A|_{X=0} = \overline{\rho_A}$. As we pointed out in the introduction, the image of $\overline{\rho_A}$ depends drastically on whether the elliptic curve A has complex multiplication or not.

From now on we let $K = \mathbb{Q}(\sqrt{-d})$ be a quadratic imaginary number field, where $d \in \mathbb{N}$ is square-free, and we assume K has discriminant $D_K \neq -3, -4$ and class number $h_K = 1$. We fix a $\mathbb{Z}$-basis of the ring of integers of K, such that $\mathcal{O}_K = \langle 1, \tau \rangle$, where

$$\tau = \begin{cases} \sqrt{-d}, & \text{if } -d \equiv 2, 3 \bmod 4; \\ \frac{1+\sqrt{-d}}{2}, & \text{if } -d \equiv 1 \bmod 4. \end{cases}$$

Suppose that $p \geq 7$ is not ramified in K. Also, we assume that the elliptic curve A/K has complex multiplication by K and precisely by $\mathcal{O}_K$ (thus the assumption on the discriminant implies that $j(A) \neq 0, 1728$). The theory of complex multiplication states that the image of the map $\overline{\rho_A}\colon \operatorname{Gal}(\overline{K}/\widetilde{K}) \longrightarrow \operatorname{SL}(2, \mathbb{Z}_p)$ is a Cartan subgroup $\mathfrak{C}'$ of $\operatorname{SL}(2, \mathbb{Z}_p)$, split or non-split according to the splitting of p in K, isomorphic to the subgroup $\mathcal{U}_1$ of $(\mathcal{O}_K \otimes \mathbb{Z}_p)^\times$ formed by all units of norm 1. The isomorphism is given by the map

$$\mathcal{U}_1 \longrightarrow \operatorname{SL}(2, \mathbb{Z}_p), \quad \alpha \mapsto M_\alpha$$

where M_α is the matrix for the map "multiplication by α" on $\mathcal{O}_K \otimes \mathbb{Z}_p$ with respect to a fixed $\mathbb{Z}_p$-basis.

Let $P_{\mathbb{Z}_p}\colon \operatorname{SL}(2, \mathbb{Z}_p) \to \operatorname{PSL}(2, \mathbb{Z}_p)$ and $P_\Lambda\colon \operatorname{SL}(2, \Lambda) \to \operatorname{PSL}(2, \Lambda)$ be the natural projections, where Λ stands for $\mathbb{Z}_p[[X]]$. We write $\mathfrak{C}$ for the image of $\mathfrak{C}'$ under $P_{\mathbb{Z}_p}$. We start with a simple lemma:

Lemma 2.1 *Let C be a closed subgroup of $\operatorname{PSL}(2, \mathbb{Z}_p)$, and let C' be its full inverse image in $\operatorname{SL}(2, \mathbb{Z}_p)$. Let $\mathfrak{X}$ be the full inverse image of C in $\operatorname{PSL}(2, \Lambda)$, and let Y be a closed subgroup of $\operatorname{SL}(2, \Lambda)$ such that $P_\Lambda(Y) = \mathfrak{X}$ and $\pi_X(Y) = C'$. Then Y is the full inverse image of C' in $\operatorname{SL}(2, \Lambda)$.*

PROOF. It suffices to show that $-I$ belongs to Y. By hypothesis, Y contains an element of the form $g = -I + X \cdot A$ with some 2×2 matrix A over Λ. Since Y is closed, Y also contains $\lim_{n\to\infty} g^{p^n} = -I$ which finishes the proof of the lemma. $\square$

Let $P\rho_A = P_\Lambda \circ \rho_A\colon \operatorname{Gal}(\overline{K}/\widetilde{K}) \longrightarrow \operatorname{PSL}(2, \mathbb{Z}_p[[X]])$, then the previous lemma reduces the proof of Theorem 1.1 to showing that the image of $P\rho_A$ is $\mathfrak{X}$, the full inverse image of $\mathfrak{C}$ under the natural projection $P\pi_X\colon \operatorname{PSL}(2, \mathbb{Z}_p[[X]]) \longrightarrow \operatorname{PSL}(2, \mathbb{Z}_p)$ which sends X to 0.

Analogously, let $P\rho_E\colon \mathrm{Gal}(\overline{K(j)}/\widetilde{K}(j)) \longrightarrow \mathrm{PSL}(2,\mathbb{Z}_p[[X]])$ be the projectivization of ρ_E. The kernel of ρ_E determines a fixed field $\mathbf{L}$, in particular $\mathrm{Gal}(\mathbf{L}/\widetilde{K}(j)) \cong \mathrm{PSL}(2,\mathbb{Z}_p[[X]])$. As before, the map $P\rho_A$ is obtained by restricting $P\rho_E$ to the decomposition group D and reducing modulo I. Hence, studying the image of $P\rho_A$ is equivalent to studying the image of D via $P\rho_E$. Notice that $P\rho_A$ is a continuous group homomorphism, therefore the image is a closed subgroup of $\mathrm{PSL}(2,\mathbb{Z}_p[[X]])$. For $i \geq 1$, let $\mathbf{L}_i \subseteq \mathbf{L}$ be the fixed field determined by the kernel of the reduction map

$$\mathrm{Gal}(\mathbf{L}/\widetilde{K}(j)) \cong \mathrm{PSL}(2,\mathbb{Z}_p[[X]]) \to \mathrm{PSL}(2,\mathbb{Z}_p[[X]]/(p,X)^i).$$

Recall that we have chosen a place σ of $\overline{K(j)}$ extending $j = j(A)$. Let ℓ_i be the residue class field of $\sigma\,|_{\mathbf{L}_i}$, i.e. $\ell_i = \sigma(\mathbf{L}_i)\backslash\{\infty\}$. We claim that in order to prove Theorem 1.1, it is enough to show the following:

Theorem 2.2 *Let $p \geq 7$ be a prime unramified in K and such that $p \nmid h_p$. Then the order of the field extension ℓ_2/ℓ_1 is p^4.*

We dedicate the rest of this section to prove that Theorem 2.2 implies the main theorem. It suffices to prove the following proposition.

Proposition 2.3 *If $[\ell_2 : \ell_1] = p^4$ then the image of $P\rho_A$ contains the kernel of the natural projection $P\pi_X$.*

In order to prove the proposition, we follow an argument due to N. Boston ([2], p. 262, Proposition 2) which makes use of the Burnside basis theorem: let G be a pro-p group and let $\overline{G}$ be its Frattini quotient. In other words, $\overline{G} = G/G^pG'$ where G^p is the subgroup of pth powers and G' is the subgroup of commutators $(g,h) = ghg^{-1}h^{-1}$, for all $g,h \in G$. If H is a closed subgroup of G and if the image of H in $\overline{G}$ is surjective, then $H = G$.

In our case we let G be the kernel of $P\pi_X$ (which is a pro-p group) and let H be the intersection of this kernel with the image of $P\rho_A$. Before we can apply Burnside's theorem, we study the Frattini quotient of G. Let $\Lambda = \mathbb{Z}_p[[X]]$ and $\mathcal{M} = (p,X)$. For every $n \geq 2$ we define groups H_n and $\widetilde{H}$ via the following exact sequences of groups:

$$1 \longrightarrow H_n \longrightarrow \mathrm{PSL}(2,\Lambda/(X^n)) \longrightarrow \mathrm{PSL}(2,\mathbb{Z}_p) \longrightarrow 1$$

$$1 \longrightarrow \widetilde{H} \longrightarrow \mathrm{PSL}(2,\Lambda/\mathcal{M}^2) \longrightarrow \mathrm{PSL}(2,\mathbb{Z}_p/(p^2)) \longrightarrow 1.$$

Lemma 2.4 *The kernel of the canonical surjection $\pi_n\colon H_{n+1} \twoheadrightarrow H_n$ lies in H'_{n+1}, the commutator subgroup of H_{n+1}. Thus, the induced homomorphism between the Frattini quotients $\overline{H_{n+1}}$ and $\overline{H_n}$ is an isomorphism.*

PROOF. One easily computes the following congruence for a commutator:

$$(1+XA+X^nB,\ 1+X^{n-1}C+X^nD) \equiv 1+X^n(AC-CA) \mod X^{n+1}$$

for arbitrary $A,\ B,\ C,\ D \in M_2^0(\mathbb{Z}_p)$, where M_2^0 denotes the set of all 2×2 trace zero matrices. Moreover, any element in $M_2^0(\mathbb{Z}_p)$ can be written as a finite sum of commutators $AC-CA$ using elementary matrices. Since the kernel of π_n is isomorphic to $(1+X^nM_2^0(\mathbb{Z}_p))$, the previous argument shows that the kernel of π_n lies in H'_{n+1}. The isomorphism between the Frattini quotients follows immediately. □

Corollary 2.5 *The Frattini quotient of G, the kernel of $P\pi_X$, is isomorphic to $\widetilde{H}$.*

PROOF. Notice that $H_2 \cong (1+XM_2^0(\mathbb{Z}_p)) \cong \mathbb{Z}_p^3$, therefore its Frattini quotient, $\overline{H_2}$, is isomorphic to $\mathbb{F}_p^3$. On the other hand, $\widetilde{H} \cong (1+XM_2^0(\mathbb{F}_p)) \cong \mathbb{F}_p^3$. Hence, by Lemma 2.4, $\overline{H_n} \cong \widetilde{H}$ for all $n \geq 2$. The corollary follows from the fact that G is the inverse limit of the H_n. □

Finally, we are ready to prove Proposition 2.3. By Burnside basis theorem and Corollary 2.5, it suffices to show that if $[\ell_2 : \ell_1] = p^4$ then the group $J = \mathrm{Gal}(\ell_2/\ell_1)$, regarded as a subgroup of $\mathrm{PSL}(2, \Lambda/\mathcal{M}^2)$, contains $\widetilde{H}$. For this, notice that the image of J in $\mathrm{PSL}(2, \mathbb{Z}/(p))$ is trivial by the definition of $\mathbf{L}_2$ and $\mathbf{L}_1$. Moreover, the image of $\mathrm{Gal}(\overline{K}/\ell_1)$ in $\mathrm{PSL}(2, \mathbb{Z}_p)$ is isomorphic to $\mathbb{Z}_p$. Hence the image of J in $\mathrm{PSL}(2, \mathbb{Z}/(p^2)$ is cyclic and either trivial or of order p. By assumption $|J| = p^4$ and since $\widetilde{H}$ was defined by the exact sequence:

$$1 \longrightarrow \mathbb{F}_p^3 \cong \widetilde{H} \longrightarrow \mathrm{PSL}(2, \Lambda/\mathcal{M}^2) \longrightarrow \mathrm{PSL}(2, \mathbb{Z}_p/(p^2)) \longrightarrow 1$$

and J has image of at most order p on the right, the proposition follows.

3 Siegel Functions

Theorem 2 in [18] provides an explicit description of the extension $\mathbf{L}_2/\mathbf{L}_1$ which will be the key ingredient to prove that $[\ell_2 : \ell_1] = p^4$. Before stating this theorem we introduce the Siegel functions. We follow Robert and Kubert-Lang in defining invariants as in [13] and [6], respectively.

Definition 3.1 (cf. [6] p. 26-29) *Let L be a lattice in $\mathbb{C}$, generated by w_1, w_2 and let $z \in \mathbb{C}$, $\gamma \in L$. We write $\sigma(z, L)$ and $\eta(\gamma, L)$ for the Weierstrass sigma* *and eta functions, respectively. Also, we define* $\eta_1 := \eta(w_1, L)$, $\eta_2 := \eta(w_2, L)$ *and for any* $z \in \mathbb{C}$ *with* $z = a_1w_1 + a_2w_2$, $a_i \in \mathbb{R}$, *we write* $\eta(z, L) := a_1\eta_1 + a_2\eta_2$. *The Klein forms are defined by*

$$\mathfrak{k}(z, L) = e^{\eta(z,L)z/2}\sigma(z, L).$$

Let $\tau \in \mathbb{C}$ *be in the upper half plane and* $a = (a_1, a_2) \in \mathbb{Q} \times \mathbb{Q}$, *with* $a \neq (0, 0)$. *Let* $L = \langle 1, \tau \rangle$ *and write* $z = a_1\tau + a_2$. *Then we write*

$$\mathfrak{k}_a(\tau) = \mathfrak{k}(z, L).$$

The Siegel functions are defined by

$$g_a(\tau) = \mathfrak{k}_a(\tau)\Delta(\tau)^{1/12}$$

where $\Delta(\tau)^{1/12} = (2\pi i) \cdot \eta(w)^2$ *and* $\eta(w)$ *is the Dedekind eta function. We may also define for any complex number* z *the functions:*

$$g^{12}(z, L) = \mathfrak{k}^{12}(z, L)\Delta(L).$$

Notice that if $L = \langle 1, \tau \rangle$ *and* $z = a_1\tau + a_2$ *then* $g^{12}(z, L) = g_a^{12}(\tau)$.

Finally, let $v_1, v_2 \in \mathbb{C}$ *be independent over* $\mathbb{R}$, *and write* $\varphi(z; v_1, v_2)$ *for the Robert invariants, as defined in [13], p. 7-9.*

Proposition 3.2 *Let* $\tau \in \mathbb{C}$ *be in the upper half plane,* $a = (a_1, a_2) \in \mathbb{Q} \times \mathbb{Q}$ *with* $a \neq (0, 0)$ *and let* $z = a_1\tau + a_2$. *Then*

$$g_a(\tau) = i \cdot \varphi(z; 1, \tau).$$

PROOF. It suffices to show that the q-product expansions agree. The result is easily verified from the expansion of g_a, which can be found at [6], p. 29, and the expansion for φ, which can be deduced from those of the functions Θ and Θ_1 in [13], p. 7-9. □

Therefore, it is clear that the 12th powers of the Siegel functions and the Robert invariants agree:

$$g_a^{12}(\tau) = \varphi^{12}(z; 1, \tau).$$

Theorem 3.3 (cf. [6], Theorems 1.1 and 1.2, p. 29-31) *Assume that* a *has a denominator dividing* N. *Then* g_a *is a modular function for* $\Gamma(2N^2)$, *and* g_a^{12N} *is a modular function on* $\Gamma(N)$.

In this section the $\mathbb{Z}$-module M and a number of submodules are introduced to help us understand the structure of the Siegel functions. We follow the definitions established in [18].

Definition 3.4 *Let $p \geq 7$ be a prime and define $R = \mathbb{F}_p^2 \backslash \{(0,0)\}$.*

(1) M is the set of all functions $m\colon R \to \mathbb{Z}$ with $m(r) = m(-r)$. M is clearly a $\mathbb{Z}$-module.
(2) We write N for the $\mathbb{Z}$-submodule of M consisting of all those $m \in M$ that reduce modulo p to a function defined by a homogeneous polynomial of degree two over $\mathbb{F}_p$.
(3) We define a submodule Q consisting of all elements of M which satisfy the "quadratic relations" of Kubert-Lang (see [6], p. 59), i.e. $m \in M$ belongs to Q if and only if $\sum_{r\in R} m(r)n(r) \equiv 0 \mod p$ for all $n \in N$. Note that $pM \subsetneq N \subsetneq Q$ (for the last inclusion, see Proposition 3 of [18]).

Remark 3.5 *There is an exact sequence of vector spaces over $\mathbb{F}_p$:*

$$\{0\} \to pM/pQ \to N/pQ \to N/pM \to \{0\}.$$

Since N/pM and M/Q are 3-dimensional, we have $|N/pQ| = p^6$.

Let $s = (s_1, s_2) \in \mathbb{Z}^2$ be fixed and put $a = a_s = \frac{1}{p}(s_1, s_2)$. If $s' \in s + p\mathbb{Z}^2$ and $a' = a_{s'}$ then the values

$$g_a^{12}(\tau) = g^{12}\left(\frac{s_1\tau + s_2}{p}, \mathcal{O}_K\right)$$

and $g_{a'}^{12}(\tau)$ only differ by a pth root of unity (for this see [6], Remark on p. 30). This leads to the definition of the symbol f_r for $r \in R$.

Definition 3.6 *Let $\iota\colon \mathbb{F}_p \times \mathbb{F}_p \to \mathcal{O}_K/p\mathcal{O}_K$ be the bijection defined by:*

$$\iota(r_1, r_2) = \begin{cases} r_1\tau + r_2, & \text{if } p \text{ is inert in } K; \\ r_1\alpha + r_2\alpha', & \text{if } p \text{ splits and } p\mathcal{O}_K = \wp \cdot \wp'. \end{cases}$$

where α is a fixed generator of $\wp$ and α' is the complex conjugate of α. We define the symbol $f_r(\tau)$ to be any function $g^{12}(I(r)/p, \mathcal{O}_K)$ where $I(r)$ is any lift of $\iota(r)$ to $\mathcal{O}_K$ (thus f_r is only well-defined up to multiplication by a pth root of unity).

Finally, for $m \in M$, we write $f^m = \prod_{r\in R} f_r^{m(r)}$.

Remark 3.7

(1) *The definition of ι in the split case was suggested by the referee. It simplifies the arguments of the proof considerably (see Section 6).*
(2) *Let U denote the set of all modular functions for $\Gamma(p)$ which are holomorphic and nowhere zero on the upper half of the complex plane. It turns out that $m \in Q$ if and only if f^m belongs to U (see [6], p. 68, Theorem 4.1).*

3.2 Rohrlich's Theorem

We are ready to state Theorem 2 of [18]:

Theorem 3.8 *The extension $\mathbf{L}_2/\mathbf{L_1}$ is generated by pth roots of Siegel units. More precisely, $\mathbf{L}_2 = \mathbf{L}_1(\{(f^m)^{1/p} : m \in N\})$.*

The previous theorem, Kummer theory and Remark 3.12 imply that $[\mathbf{L}_2 : \mathbf{L}_1] = |N/pQ| = p^6$. In order to simplify the proof of Theorem 2.2, define a map

$$\begin{aligned} \psi\colon Q/pQ &\longrightarrow \ell_1^*/(\ell_1^*)^p \\ m + pQ &\mapsto \sigma(f^m) \mod (\ell_1^*)^p. \end{aligned}$$

Even though the functions f^m are defined up to pth roots of unity, $\mu_p \subset (\ell_1^*)^p$ so ψ is well defined. Again, by Kummer theory we have $[\ell_2\colon \ell_1] \geq |\psi(N/pQ)|$, and recall that we needed $[\ell_2 : \ell_1] = p^4$. Since the image of $P\rho_A$ is included in $\mathfrak{X}$ (because the image of $P\overline{\rho_A}$ is $\mathfrak{C}$), the image of the decomposition group D in $\mathrm{PSL}(2, \Lambda/(p, X)^2)$ is included in $\mathfrak{X}_2$. Hence $[\ell_2 : \ell_1] \leq p^4$ so it suffices to show $|\psi(N/pQ)| \geq p^4$.

Recall that $\mathrm{Gal}(\ell_1/\widetilde{K}) \cong \mathfrak{C}_1$, so ℓ_1 corresponds with the extension of $\widetilde{K}$ obtained by adjoining the x-coordinates of p-torsion points on A. Therefore $\ell_1 = \widetilde{K(p)} = (K(p))(\mu_{p^\infty})$ where $K(p)$, as before, denotes the ray class field of K of conductor (p).

The place σ of $\overline{K(j)}$, $\sigma\colon \overline{K(j)} \to \overline{K} \cup \{\infty\}$ is chosen so that $\sigma(f_r) = f_r(\tau)$, and we are interested in the values of $f^m(\tau) \in \ell_1$ for $m \in N$. It turns out that some of those values are *elliptic units* in $K(p)$ and the work of Robert and Kubert-Lang will be key in order to prove that $|\psi(N/pQ)| \geq p^4$. We will describe the groups of elliptic units in Section 4, but first we need to introduce some other important aspects of the structure of M.

Definition 3.9 *Let $\overline{R} = R/\{\pm 1\}$ and let ι be the map defined in Def. 3.6. For $r \in R$, the class of r in $\overline{R}$ is denoted by $\bar{r}$. For each $\bar{r}$ in $\overline{R}$, let us fix a principal integral ideal $\mathfrak{A}_{\bar{r}}$ of $\mathcal{O}_K$ relatively prime to 6 and not divisible by p, such that $\mathfrak{A}_{\bar{r}} = (a)$ with $a \in \mathcal{O}_K$ and $a \equiv \pm\iota(r) \mod p$. For an integral ideal $\mathfrak{B} = (b)$ we define $\bar{r}(\mathfrak{B})$ to be the element $\bar{r}$ of $\overline{R}$ such that $b \equiv \pm\iota(r) \mod p$.*

Remark 3.10

(1) Recall that we are assuming $h_K = 1$, however principal ideals $\mathfrak{A}_{\bar{r}}$ with the required properties can be chosen even if the class number of K is arbitrary.

(2) Notice that if p is inert in K, we could simply require the ideals $\mathfrak{A}_{\bar{r}}$ to be prime to $6p$. However, in the split case, in order to be able to find ideals $\mathfrak{A}_{\bar{r}} = (a)$ such that $a \equiv \iota(r) \mod p$, we must allow some of the ideals to be divisible by $\wp$ or $\wp'$ (but not both), where $p\mathcal{O}_K = \wp \cdot \wp'$. We will come back to this later (see Definition 6.3 in Section 6.1).

Definition 3.11 *If $m \in M$, the degree and the norm of m are defined by:*

$$\deg(m) = \sum_{r \in R} m(r), \quad \mathrm{Norm}(m) = N(m) = \sum_{r \in R} m(r)\mathbf{N}(\mathfrak{A}_{\bar{r}})$$

Define, also, the following submodules of M:

$$M_0 = \{m \in M \mid \deg(m) = 0\}, \quad M_{0,p} = \{m \in M_0 \mid \mathrm{Norm}(m) \equiv 0 \bmod p\}$$

$$Q_0 = Q \cap M_0, \quad N_0 = N \cap M_0.$$

Remark 3.12

(1) M is a free $\mathbb{Z}$-module of rank $\frac{p^2-1}{2}$. Therefore, M_0 is free of rank $\frac{p^2-3}{2}$. Clearly $pM_0 \subset M_{0,p}$, thus $M_{0,p}$ is also free of the same rank as M_0.

(2) Notice that the function $r \in R \mapsto \mathbf{N}(\mathfrak{A}_{\bar{r}})$ reduces modulo p to a function defined by a homogeneous quadratic polynomial. Hence, by definition of Q, all $m \in Q$ satisfy the condition $\mathrm{Norm}(m) \equiv 0 \mod p$. Thus $Q_0 \subseteq M_{0,p}$.

As suggested by the referee, we will introduce an appropriate group action on M which will help us simplify the arguments which will follow. We use the definitions and notation of [18], p. 17, 18. Let $G = \mathrm{PSL}(2, \mathbb{F}_p)$. The $\mathbb{Z}$-modules M, N and Q can be made into $\mathbb{Z}[G]$-modules by defining:

$$(gm)(r) = m(r\tilde{g})$$

where $r = (r_1, r_2)$ is viewed as a column vector and $\tilde{g} \in \mathrm{SL}(2, \mathbb{F}_p)$ is any of the two preimages of $g \in G$. We also define $\mathbb{Z}_p[G]$-modules:

$$\mathcal{M} = \mathbb{Z}_p \otimes_{\mathbb{Z}} M, \quad \mathcal{N} = \mathbb{Z}_p \otimes_{\mathbb{Z}} N, \quad \mathcal{Q} = \mathbb{Z}_p \otimes_{\mathbb{Z}} Q.$$

Furthermore, let $\omega \colon \mathbb{F}_p^\times \to \mathbb{Z}_p^\times$ be the Teichmüller character and define the following $\mathbb{Z}_p[G]$-submodules of $\mathcal{M}$:

$$\mathcal{M}_{(j)} = \{m \colon R \to \mathbb{Z}_p \mid \forall \lambda \in \mathbb{F}_p^\times, r \in R : m(\lambda r) = \omega^j(\lambda) m(r)\}$$

where $0 \leq j \leq p-3$ and j is even. Let $\mathcal{W}_j \subset \mathcal{M}_{(j)}$ be the $\mathbb{Z}_p[G]$-submodule formed by those elements of $\mathcal{M}_{(j)}$ which reduce over $\mathbb{F}_p$ to a homogeneous polynomial of degree j. The notation $\mathcal{M}_0$ will be reserved to denote $\mathcal{M}_0 := M_0 \otimes_{\mathbb{Z}} \mathbb{Z}_p$. The following decompositions follow immediately from Prop. 7 in [18] by using the group action of G:

Lemma 3.13

$$\mathcal{M} \cong \bigoplus_{0 \leq j \leq p-3,\ even} \mathcal{M}_{(j)}, \tag{1}$$

$$\mathcal{N} \cong p\mathcal{M}_0 \oplus \mathcal{W}_2 \bigoplus_{4 \leq j \leq p-3,\ even} p\mathcal{M}_{(j)}, \tag{2}$$

$$\mathcal{Q} \cong \mathcal{W}_{p-3} \bigoplus_{0 \leq j \leq p-5,\ even} \mathcal{M}_{(j)} \tag{3}$$

The degree function extends from M to $\mathcal{M}$. For $m \in \mathcal{M}_{(j)}$ and $\lambda \in \mathbb{F}_p^\times$ one has

$$\deg(m) = \sum_{r \in R} m(r) = \sum_{r \in R} m(\lambda r) = \omega^j(\lambda) \deg(m)$$

and thus $(1 - \omega^j(\lambda)) \deg(m) = 0$. In particular for $j \neq 0$, the degree of m is always zero. Hence the condition $\deg(m) = 0$ cuts out a 1-codimensional subspace $\mathcal{M}^0_{(0)}$ of $\mathcal{M}_{(0)}$ (as free $\mathbb{Z}_p$-modules).

Similarly, if we consider the norm on $\mathcal{M}$, for $m \in \mathcal{M}_{(j)}$ and $\lambda \in \mathbb{F}_p^\times$ one has

$$\begin{aligned} N(m) &= \sum_{r \in R} m(r) \mathbf{N}(\mathfrak{A}_{\bar{r}}) = \sum_{r \in R} m(\lambda r) \mathbf{N}(\mathfrak{A}_{\lambda \bar{r}}) \\ &= \sum_{r \in R} \omega^j(\lambda) m(r) \omega^2(\lambda) \mathbf{N}(\mathfrak{A}_{\bar{r}}) = \omega^{j+2}(\lambda) N(m) \end{aligned}$$

and thus $(1 - \omega^{j+2}(\lambda)) N(m) = 0$. Therefore the condition $N(m) \equiv 0 \mod p$ defines a submodule $\mathcal{M}_{(p-3),p}$ of $\mathcal{M}_{(p-3)}$ such that $\mathcal{M}_{(p-3)}/\mathcal{M}_{(p-3),p} \cong \mathbb{F}_p$. Hence, under the isomorphism of Eq. (1), we obtain decompositions:

Lemma 3.14

$$M_0 \otimes_{\mathbb{Z}} \mathbb{Z}_p = \mathcal{M}_0 \cong \mathcal{M}^0_{(0)} \bigoplus_{2\le j\le p-3,\ even} \mathcal{M}_{(j)} \tag{4}$$

$$M_{0,p} \otimes_{\mathbb{Z}} \mathbb{Z}_p = \mathcal{M}_{0,p} \cong \mathcal{M}^0_{(0)} \oplus \mathcal{M}_{(p-3),p} \bigoplus_{2\le j\le p-5,\ even} \mathcal{M}_{(j)} \tag{5}$$

We define submodules $\mathcal{N}_0 = \mathcal{M}_0 \cap \mathcal{N}$, $\mathcal{Q}_0 = \mathcal{M}_0 \cap \mathcal{Q}$.

Note that N/pQ is 6-dimensional as $\mathbb{F}_p$-vector space and $Q_0 \subseteq M_{0,p}$ (see Remark 3.12). The latter implies that there is a well-defined map $\gamma\colon Q_0/pQ_0 \longrightarrow M_{0,p}/pM_{0,p}$ with kernel $pM_{0,p}/pQ_0$.

Lemma 3.15 *The $\mathbb{F}_p$-vector space N_0/pQ_0 is a 6-dimensional. Moreover, the image of N_0/pQ_0 in $M_{0,p}/pM_{0,p}$ via the map γ has size p^4.*

PROOF. We have a canonical identification $N_0/pQ_0 \cong \mathcal{N}_0/p\mathcal{Q}_0$ and by equations (2), (3) and (4) one has:

$$\mathcal{N}_0/p\mathcal{Q}_0 \cong \mathcal{W}_2/p\mathcal{M}_{(2)} \oplus p\mathcal{M}_{(p-3)}/p\mathcal{W}_{p-3} \cong \mathcal{N}/p\mathcal{Q} \cong N/pQ$$

and N/pQ is 6 dimensional over $\mathbb{F}_p$. For the second part of the lemma, it is clear that $\mathcal{W}_2/p\mathcal{M}_{(2)}$ injects via γ, while the intersection of $p\mathcal{M}_{(p-3)}/p\mathcal{W}_{p-3}$ and the kernel of γ is 2-dimensional (because we showed that $\mathcal{M}_{(p-3)}/\mathcal{M}_{(p-3),p} \cong \mathbb{F}_p$) which completes the proof of the lemma. □

4 The Robert Group of Elliptic Units

Let $g^{12}(z, L)$ be the Siegel functions defined in Definition 3.1 and let $\mathfrak{A}$ be an ideal of K, with $\mathfrak{A} = (\alpha) \subset K$ (recall that K is assumed to be of class number one). The ideals of K will be considered as lattices in $\mathbb{C}$. Then:

$$g^{12}(1, p\mathfrak{A}^{-1}) = g^{12}(1, p\mathfrak{A}^{-1}\mathcal{O}_K) = g^{12}(1, p(\alpha)^{-1}\mathcal{O}_K) = g^{12}(\frac{\alpha}{p}, \mathcal{O}_K)$$

where in the last equality we used that $g^{12}(z, L)$ is a modular function (of weight 0). In the rest of the article, the notation of Kubert-Lang (cf. [6], p. 255) will frequently be used:

$$g^{12}_p(\mathfrak{A}; \mathcal{O}_K) := g^{12}(1, p\mathfrak{A}^{-1}) = g^{12}(\frac{\alpha}{p}, \mathcal{O}_K).$$

Remark 4.1 *(1) Note that for $r \in R$, the numbers $f_r(\tau)$ and $g^{12}_p(\mathfrak{A}_{\bar{r}}; \mathcal{O}_K)$ only differ by a pth root of unity (see paragraph following Definition 3.4).*

(2) An ideal $\mathfrak{A} = (\alpha)$ *of* $\mathcal{O}_K$ *has two generators, namely* α *and* $-\alpha$*. However,* $g(z, L)$ *is an odd function of its first variable, therefore* $g^{12}(z, L)$ *is even. Consequently*

$$g^{12}(1, p\mathfrak{A}^{-1}) = g^{12}(\frac{\alpha}{p}, \mathcal{O}_K) = g^{12}(\frac{-\alpha}{p}, \mathcal{O}_K).$$

(3) If $\mathfrak{A}_1 = (\alpha_1), \mathfrak{A}_2 = (\alpha_2)$ *are two integral ideals such that* $\alpha_1 \equiv \pm\alpha_2 \mod p$ *then:*

$$g_p^{12}(\mathfrak{A}_1; \mathcal{O}_K) = g^{12}(\frac{\alpha_1}{p}, \mathcal{O}_K) = \zeta_p \cdot g^{12}(\frac{\alpha_2}{p}, \mathcal{O}_K) = \zeta_p \cdot g_p^{12}(\mathfrak{A}_2; \mathcal{O}_K)$$

for some pth root of unity ζ_p*, where the middle equality follows from [6], Remark on p. 30.*

4.1 The Primitive Robert Group

Next we define the *primitive Robert group* as in Kubert-Lang, [6] p. 256. Let I be the free abelian group on ideals of K which are prime to $6p$. We express $a \in I$ as formal sums:

$$a = \sum_{\mathfrak{A}} a(\mathfrak{A})\mathfrak{A}$$

with $a(\mathfrak{A}) \in \mathbb{Z}$ for all ideals $\mathfrak{A} \subseteq \mathcal{O}_K$, and define the degree and norm of a by the formulas:

$$\deg(a) = \sum_{\mathfrak{A}} a(\mathfrak{A}), \quad N(a) = \sum_{\mathfrak{A}} a(\mathfrak{A})\mathbf{N}(\mathfrak{A})$$

where $\mathbf{N}(\mathfrak{A}) = |\mathcal{O}_K/\mathfrak{A}|$ denotes the absolute norm of the ideal $\mathfrak{A}$. Also, for $a \in I$ write:

$$g_p^{12}(a; \mathcal{O}_K) := \prod_{\mathfrak{A}} g_p^{12}(\mathfrak{A}; \mathcal{O}_K)^{a(\mathfrak{A})} = \prod_{\mathfrak{A}=(\alpha)} g^{12}(\frac{\alpha}{p}, \mathcal{O}_K)^{a(\mathfrak{A})}.$$

Definition 4.2 *The primitive Robert group* $\mathfrak{R}_p^*$ *is the group of all elements:*

$$g_p^{12}(a; \mathcal{O}_K), \quad a \in I \text{ such that } \deg(a) = 0,\ N(a) = 0.$$

Lemma 4.3 *For* $p \geq 5$*, the primitive Robert group* $\mathfrak{R}_p^*$ *contains the group of pth roots of unity* μ_p*.*

PROOF. Let $\alpha = 6p\tau + 1$, $\beta = \overline{\alpha}$, the complex conjugate of α, and define ideals $\mathfrak{A} = (\alpha)$, $\mathfrak{B} = (\beta)$. Recall that τ equals $\sqrt{-d}$ or $(1+\sqrt{-d})/2$ according to the choice of $\mathbb{Z}$-basis for $\mathcal{O}_K$ made at the beginning of Section 2.1. Thus:

$$\beta = \begin{cases} (-6p\tau + 1), & \text{if } -d \equiv 2, 3 \bmod 4; \\ (6p(1-\tau) + 1), & \text{if } -d \equiv 1 \bmod 4. \end{cases}$$

Notice that both ideals are relatively prime to $6p$ (since they are of the form $(6p\gamma + 1)$, with $\gamma \in \mathcal{O}_K$). Let $a = \mathfrak{A} - \mathfrak{B}$. Then $\deg(a) = 0$, and $N(a) = 0$ because $\mathbf{N}(\mathfrak{A}) = \mathbf{N}(\mathfrak{B})$. Therefore, $g_p^{12}(a; \mathcal{O}_K)$ belongs to $\mathfrak{R}_p^*$. Moreover:

$$\alpha - \beta = \begin{cases} 12p\tau, & \text{if } -d \equiv 2, 3 \bmod 4; \\ 6p(2\tau - 1), & \text{if } -d \equiv 1 \bmod 4 \end{cases}$$

and in both cases $\alpha - \beta \in p\mathcal{O}_K$. Thus, by Remark 4.1:

$$g_p^{12}(\mathfrak{A}; \mathcal{O}_K) = \zeta_p \cdot g_p^{12}(\mathfrak{B}; \mathcal{O}_K)$$

for some pth root of unity ζ_p. In fact, using [6], p. 28, formula K2, one can explicitly calculate:

$$g_p^{12}(a; \mathcal{O}_K) = \frac{g_p^{12}(\frac{\alpha}{p}, \mathcal{O}_K)}{g_p^{12}(\frac{\beta}{p}, \mathcal{O}_K)} = e^{-12^2\pi i/p}$$

which, since $p \geq 5$, is a primitive pth root of unity. $\square$

Remark 4.4 *When* $p = 2$ *or* 3*, Lemma 4.3 does not hold, since all elements of the primitive Robert group are obtained as* 12*th powers.*

Let $\mathcal{E}_p^\times$ be the full group of units in $\mathcal{O}_{K(p)}$. Note that μ_p, the set of all p-th roots of unity, are in $\mathcal{E}_p^\times$ (this is because $K(\mu_p) \subseteq K(p)$). Also define

$$E_p^\times := \mathcal{E}_p^\times / \mu_p, \quad R_p^\times := \mathfrak{R}_p^* / \mu_p.$$

The ray class field of K of conductor p, $K(p)$, is a totally imaginary field of degree

$$[K(p) \colon \mathbb{Q}] = \begin{cases} p^2 - 1, & \text{if } p \text{ is inert in } K \\ (p-1)^2, & \text{if } p \text{ splits in } K. \end{cases}$$

Therefore, by Dirichlet's unit theorem, the free rank of $E_p^\times$ is

$$\begin{cases} \frac{p^2-1}{2} - 1 = \frac{p^2-3}{2}, & \text{if } p \text{ is inert in } K \\ \frac{(p-1)^2}{2} - 1 = \frac{p^2-2p-1}{2}, & \text{if } p \text{ splits in } K. \end{cases}$$

The work of Robert ([13]) implies the following:

Theorem 4.5 *(1)* $R_p^\times \subseteq E_p^\times, \quad \mathfrak{R}_p^* \subseteq \mathcal{E}_p^\times.$

(2) $[\mathcal{E}_p^\times : \mathfrak{R}_p^*] = [E_p^\times : R_p^\times] = \lambda h_p$ *where* $\lambda = 2^\alpha \cdot 3^\beta$*, for some non-negative integers* α, β*.*

In particular, the free rank of $R_p^\times$ *is the same as the free rank of* $E_p^\times$*.*

PROOF. Let us establish the correct correspondence between Lang and Kubert terminology ([6]) and Robert's terminology ([13]), namely:

$$V_p = \Phi_p(2p).$$

V_p is defined in [13], page 37, whereas $\Phi_p(2p)$ is defined in [6], page 257, in a very similar way with a slight change of notation. Note that $w_{K(p)}$ is defined in [6] as the number of roots of unity in $K(p)$. Since the discriminant of K is, by hypothesis, different from $-3, -4$, we have $w_{K(p)} = 2p$ (the only roots of unity are the $\pm$ p-th roots).

We prove that the group $\mathfrak{R}_p^*$, as defined above, coincides with Ω_p as defined by Robert ([13], page 40). Note that Ω_p is defined as the largest subgroup of $\mathcal{E}_p^\times$ such that $(\Omega_p)^p = V_p$ (in Robert's notation, [13] page 13, e_f denotes the number of roots of unity in K which are $1 \bmod p$, so $e_f = 1$). Moreover, in Theorem 4.3 of [6], Kubert and Lang prove that

$$(\mathfrak{R}_p^*)^p = \Phi_p(2p) = V_p$$

therefore $\mathfrak{R}_p^* \subseteq \Omega_p$. For the reverse inclusion, let $\omega \in \Omega_p$. By definition of Ω_p, $\omega^p \in V_p = (\mathfrak{R}_p^*)^p$ so there exists $r \in \mathfrak{R}_p^*$ such that $r^p = \omega^p$. Thus $r = \zeta_p \cdot \omega$ for some p-th root of unity ζ_p. Hence

$$\omega = \zeta_p^{-1} \cdot r \in \mu_p \mathfrak{R}_p^* = \mathfrak{R}_p^*$$

since $\mu_p \subseteq \mathfrak{R}_p^*$ by lemma 4.3. This concludes the proof of $\Omega_p = \mathfrak{R}_p^*$. Finally, the index of Ω_p in $\mathcal{E}_p^\times$ is analyzed in Robert's work, [13] page 47-49. □

5 The Inert Case

In this section let us assume that the prime $p \geq 7$ is inert in the quadratic imaginay field K. We start by giving a more concise characterization of $\mathfrak{R}_p^*$ in this case. Recall that I denotes the free abelian group on ideals of K which are prime to $6p$. Let $I_{\overline{R}}$ be the free abelian group on the ideals $\{\mathfrak{A}_{\bar{r}} : \bar{r} \in \overline{R}\}$ defined in Definition 3.9. Notice that the fact that p is inert in K implies that for every $\bar{r} \in \overline{R}$ the ideal $\mathfrak{A}_{\bar{r}}$ is relatively prime to $6p$, which will be implicitly used throughout this section.

The following proposition is due to Kubert-Lang (cf. [6], p. 258, proof of Theorem 4.3). We give an outline of a slightly different proof because this argument will be used in sections to follow.

Proposition 5.1 *The group $\mathfrak{R}_p^*$ is the group of all elements:*

$$\zeta_p \cdot g_p^{12}(b;\mathcal{O}_K), \quad b \in I_{\overline{R}} \textit{ such that } \deg(b)=0,\ N(b)\equiv 0 \mod 2p,\ \zeta_p \in \mu_p.$$

PROOF. Let $u \in \mathfrak{R}_p^*$. Then, by Definition 4.2, there exists $a \in I$, with $a = \sum a(\mathfrak{B})\mathfrak{B}$, such that $\deg(a)=0$, $N(a)=0$ and $u = g_p^{12}(a;\mathcal{O}_K) \in \mathfrak{R}_p^*$. So, in particular, $N(a)\equiv 0 \mod 2p$. Let $\mathfrak{B}$ be an ideal that appears in a, and let $\bar{r}(\mathfrak{B})$ be as in Definition 3.9. In particular, $\mathbf{N}(\mathfrak{B}) \equiv \mathbf{N}(\mathfrak{A}_{\bar{r}(\mathfrak{B})}) \mod p$. Also, since all ideals in a and the ideals $\mathfrak{A}_{\bar{r}}$ are assumed to be relatively prime to 2, we have $\mathbf{N}(\mathfrak{B}) \equiv \mathbf{N}(\mathfrak{A}_{\bar{r}(\mathfrak{B})}) \equiv 1 \mod 2$. Thus:

$$\mathbf{N}(\mathfrak{B}) \equiv \mathbf{N}(\mathfrak{A}_{\bar{r}(\mathfrak{B})}) \mod 2p.$$

Notice that by Remark 4.1, the elements $g_p^{12}(\mathfrak{B};\mathcal{O}_K)$ and $g_p^{12}(\mathfrak{A}_{\bar{r}(\mathfrak{B})};\mathcal{O}_K)$ only differ by a pth root of unity. Next we construct an element $b \in I_{\overline{R}}$. For any $\bar{s} \in \overline{R}$ let

$$b(\bar{s}) = b(\mathfrak{A}_{\bar{s}}) = \sum_{\bar{r}(\mathfrak{B})=\bar{s}} a(\mathfrak{B})$$

where the sum is over all ideals $\mathfrak{B}$ ocurring in a such that $\bar{r}(\mathfrak{B}) = \bar{s}$, and define $b := \sum_{\bar{s}\in\overline{R}} b(\bar{s})\mathfrak{A}_{\bar{s}}$. Then:

$$\begin{aligned}
\deg(b) &= \sum_{\bar{s}\in\overline{R}} b(\bar{s}) = \sum_{\bar{s}\in\overline{R}} \left(\sum_{\bar{r}(\mathfrak{B})=\bar{s}} a(\mathfrak{B}) \right) = \deg(a) = 0 \\
\mathrm{Norm}(b) &= \sum_{\bar{s}\in\overline{R}} b(\bar{s})\mathbf{N}(\mathfrak{A}_{\bar{s}}) \equiv \sum_{\bar{s}\in\overline{R}} \left(\sum_{\bar{r}(\mathfrak{B})=\bar{s}} a(\mathfrak{B})\mathbf{N}(\mathfrak{B}) \right) \\
&\equiv \mathrm{Norm}(a) \equiv 0 \mod 2p
\end{aligned}$$

and

$$\begin{aligned}
g_p^{12}(b;\mathcal{O}_K) &= \prod_{\bar{s}\in\overline{R}} g_p^{12}(\mathfrak{A}_{\bar{s}};\mathcal{O}_K)^{b(\bar{s})} = \prod_{\bar{s}\in\overline{R}} g_p^{12}(\mathfrak{A}_{\bar{s}};\mathcal{O}_K)^{\sum_{\bar{r}(\mathfrak{B})=\bar{s}} a(\mathfrak{B})} \\
&= \zeta_p \cdot \prod_{\bar{s}\in\overline{R}} \left(\prod_{\bar{r}(\mathfrak{B})=\bar{s}} g_p^{12}(\mathfrak{B};\mathcal{O}_K)^{a(\mathfrak{B})} \right) = \zeta_p \cdot g_p^{12}(a;\mathcal{O}_K)
\end{aligned}$$

for some pth root of unity ζ_p. Hence $u = g_p^{12}(a;\mathcal{O}_K) = \zeta_p^{-1} \cdot g_p^{12}(b;\mathcal{O}_K)$.

For the converse, let $v = g_p^{12}(b;\mathcal{O}_K)$, with $b \in I_{\overline{R}}$ such that $\deg(b) = 0,\ N(b) \equiv 0 \mod 2p$. Thus b is of the form:

$$b = \sum_{\bar{r}} b(\bar{r})\mathfrak{A}_{\bar{r}}, \quad \sum_{\bar{r}} b(\bar{r}) = 0, \quad \sum_{\bar{r}} b(\bar{r})\mathbf{N}(\mathfrak{A}_{\bar{r}}) \equiv 0 \mod 2p.$$

Then, by definition:

$$v = g_p^{12}(b;\mathcal{O}_K) = \prod_{\bar{r}} g_p^{12}(\mathfrak{A}_{\bar{r}};\mathcal{O}_K)^{b(\bar{r})}$$

Let $\bar{r}_1$ denote the class of $(0,1)$ in $R/\{\pm 1\}$, fix $\mathfrak{A}_{\bar{r}_1} = \mathcal{O}_K$, and write

$$\{\bar{r}_1, \bar{r}_2, \ldots, \bar{r}_k\} = R/\{\pm 1\}$$

with $k = \frac{p^2-1}{2}$. The element v can be rewritten as follows:

$$v = g_p^{12}(b;\mathcal{O}_K) = \prod_{i=1}^{k} g_p^{12}(\mathfrak{A}_{\bar{r}_i};\mathcal{O}_K)^{b(\bar{r}_i)} = \prod_{i=2}^{k} \left(\frac{g_p^{12}(\mathfrak{A}_{\bar{r}_i};\mathcal{O}_K)}{g_p^{12}(\mathfrak{A}_{\bar{r}_1};\mathcal{O}_K)} \right)^{b(\bar{r}_i)}$$

The last equality is inferred from the fact that $\deg(b) = 0$. Next write v as:

$$\begin{aligned} v &= \prod_{i=2}^{k} \left(\frac{g_p^{12}(\mathfrak{A}_{\bar{r}_i};\mathcal{O}_K)}{g_p^{12}(\mathfrak{A}_{\bar{r}_1};\mathcal{O}_K)} \right)^{b(\bar{r}_i)} \\ &= \prod_{i=2}^{k} \left(\frac{g_p^{12}(\mathfrak{A}_{\bar{r}_i};\mathcal{O}_K)}{g_p^{12}(\mathfrak{A}_{\bar{r}_1};\mathcal{O}_K)^{\mathbf{N}(\mathfrak{A}_{\bar{r}_i})}} \right)^{b(\bar{r}_i)} \cdot \prod_{i=2}^{k} \left(\frac{g_p^{12}(\mathfrak{A}_{\bar{r}_1};\mathcal{O}_K)^{\mathbf{N}(\mathfrak{A}_{\bar{r}_i})}}{g_p^{12}(\mathfrak{A}_{\bar{r}_1};\mathcal{O}_K)} \right)^{b(\bar{r}_i)} \end{aligned}$$

Note that the second product on the right hand side is just

$$g_p^{12}(\mathfrak{A}_{\bar{r}_1};\mathcal{O}_K)^{\sum_{i=2}^{k} b(\bar{r}_i)(\mathbf{N}\mathfrak{A}_{\bar{r}_i}-1)}$$

Also, notice that

$$\begin{aligned} \sum_{i=2}^{k} b(\bar{r}_i)(\mathbf{N}\mathfrak{A}_{\bar{r}_i} - 1) &= \sum_{i=2}^{k} b(\bar{r}_i)\mathbf{N}\mathfrak{A}_{\bar{r}_i} - \sum_{i=2}^{k} b(\bar{r}_i) \\ &= \sum_{i=2}^{k} b(\bar{r}_i)\mathbf{N}\mathfrak{A}_{\bar{r}_i} + b(\bar{r}_1) = \sum_{i=1}^{k} b(\bar{r}_i)\mathbf{N}\mathfrak{A}_{\bar{r}_i} \equiv 0 \mod 2p \end{aligned}$$

Let $Cl(p)$ be the ray class group of conductor $p\mathcal{O}_K$. By Lemma 4.2, in p. 216 of [6], there exist ideals $\mathfrak{C}_1, \ldots, \mathfrak{C}_s \in C_0 \in Cl(p)$, prime to $6p$, and integers $n_1, \ldots, n_s$ such that

$$\sum_{i=2}^{k} b(\bar{r}_i)(\mathbf{N}\mathfrak{A}_{\bar{r}_i} - 1) = \sum_{j=1}^{s} n_j(\mathbf{N}\mathfrak{C}_j - 1) \tag{6}$$

Thus:

$$v=\prod_{i=2}^{k}\left(\frac{g_p^{12}(\mathfrak{A}_{\bar r_i};\mathcal{O}_K)}{g_p^{12}(\mathfrak{A}_{\bar r_1};\mathcal{O}_K)^{\mathbf{N}(\mathfrak{A}_{\bar r_i})}}\right)^{b(\bar r_i)}\cdot\prod_{j=1}^{s}\left(\frac{g_p^{12}(\mathfrak{A}_{\bar r_1};\mathcal{O}_K)^{\mathbf{N}(\mathfrak{C}_j)}}{g_p^{12}(\mathfrak{A}_{\bar r_1};\mathcal{O}_K)}\right)^{n_j}$$

The fact that $\mathfrak{C}_{\mathrm{j}}\in C_0$ for all j (and $h_K=1$) implies that the ideals $\mathfrak{C}_{\mathrm{j}}$ are principal and generated by elements which are congruent to 1 modulo p, and so is $\mathfrak{A}_{\bar r_1}(=\mathcal{O}_K)$. Thus:

$$g_p^{12}(\mathfrak{A}_{\bar r_1};\mathcal{O}_K)=\zeta_{p,j}\cdot g_p^{12}(\mathfrak{C}_j;\mathcal{O}_K)$$

for some pth root of unity $\zeta_{p,j}$ (which depends on j). Hence, there is a pth root of unity ζ_p such that:

$$\begin{aligned}v&=\zeta_p\cdot\prod_{i=2}^{k}\left(\frac{g_p^{12}(\mathfrak{A}_{\bar r_i};\mathcal{O}_K)}{g_p^{12}(\mathfrak{A}_{\bar r_1};\mathcal{O}_K)^{\mathbf{N}(\mathfrak{A}_{\bar r_i})}}\right)^{b(\bar r_i)}\cdot\prod_{j=1}^{s}\left(\frac{g_p^{12}(\mathfrak{A}_{\bar r_1};\mathcal{O}_K)^{\mathbf{N}(\mathfrak{C}_j)}}{g_p^{12}(\mathfrak{C}_j;\mathcal{O}_K)}\right)^{n_j}\\&=\zeta_p\cdot\prod_{i=2}^{k}g_p^{12}(\mathfrak{A}_{\bar r_i};\mathcal{O}_K)^{b(\bar r_i)}\cdot\prod_{j=1}^{s}g_p^{12}(\mathfrak{C}_j;\mathcal{O}_K)^{-n_j}\\&\quad\cdot g_p^{12}(\mathfrak{A}_{\bar r_1};\mathcal{O}_K)^{-\sum b(\bar r_i)\mathbf{N}\mathfrak{A}_{\bar r_i}+\sum n_j\mathbf{N}\mathfrak{C}_j}\end{aligned}$$

If one defines $a\in I$ by:

$$a=\sum_{i=2}^{k}b(\bar r_i)\mathfrak{A}_{\bar r_i}-\sum_{j=1}^{s}n_j\mathfrak{C}_j+(-\sum b(\bar r_i)\mathbf{N}\mathfrak{A}_{\bar r_i}+\sum n_j\mathbf{N}\mathfrak{C}_j)\cdot\mathcal{O}_K$$

then $\deg(a)=0$ (by Eq. (6)), and $\mathbf{N}(a)=0$. Hence $g_p^{12}(a;\mathcal{O}_K)\in\mathfrak{R}_p^*$. Moreover $v=\zeta_p\cdot g_p^{12}(a;\mathcal{O}_K)$. Since $\mu_p\subset\mathfrak{R}_p^*$ (Lemma 4.3), we conclude that $v\in\mathfrak{R}_p^*$. □

Definition 5.2 *For each $a\in I_{\overline{R}}$, with*

$$a=\sum_{\bar r}n(\mathfrak{A}_{\bar r})\mathfrak{A}_{\bar r}$$

define an element $m_a\in M$ by putting $m_a(r)=m_a(-r)=n(\mathfrak{A}_{\bar r})$, for each $r\in R$.

Corollary 5.3 $(R_p^\times)^2=\{f^{m_a}(\tau)$: $a\in I_{\overline{R}}$ *such that* $\deg(a)=0,N(a)\equiv 0$ mod $2p\}$.

PROOF. For any $a\in I_{\overline{R}}$:

$$
\begin{aligned}
f^{m_a}(\tau) &= \prod_{r\in R} f_r(\tau)^{m_a(r)} \\
&= \zeta \cdot \prod_{\bar r\in \overline{R}} g_p^{12}(\mathfrak{A}_{\bar r};\mathcal{O}_K)^{2\cdot m_a(r)} = \zeta\cdot\left(\prod_{\bar r\in\overline{R}} g_p^{12}(\mathfrak{A}_{\bar r};\mathcal{O}_K)^{m_a(r)}\right)^2
\end{aligned}
$$

for some pth root of unity ζ (see Remark 4.1). Therefore, if $\deg(a) = 0$ and $N(a) \equiv 0 \mod 2p$ then Proposition 5.1 implies that f^{m_a} belongs to $(R_p^\times)^2$ and, in fact, every element of the group may be constructed this way. □

Now the connection can be made between the $\mathbb{Z}$-module $M_{0,p}$, as defined in Definition 3.12, and the Robert group $\mathfrak{R}_p^*$ (recall that $R_p^\times$ is simply $\mathfrak{R}_p^*/\mu_p$).

Proposition 5.4 *The map*

$$
\begin{aligned}
\Psi_0\colon M_{0,p}/pM_{0,p} &\longrightarrow R_p^\times/(R_p^\times)^p \\
m + pM_{0,p} &\mapsto f^m(\tau) \mod (R_p^\times)^p
\end{aligned}
$$

is an isomorphism of $\mathbb{F}_p$*-modules.*

PROOF. First let us check that the map Ψ_0 is well defined. Let $m \in M_{0,p}$, so that $\deg(m) = 0$, $\mathrm{Norm}(m) \equiv 0 \mod p$. Also, since $m(r) = m(-r)$:

$$
\mathrm{Norm}(m) = \sum_{r\in R} m(r)\mathbf{N}(\mathfrak{A}_{\bar r}) = \sum_{\bar r\in\overline{R}} 2m(r)\mathbf{N}(\mathfrak{A}_{\bar r}) \equiv 0 \mod 2.
$$

Thus $\mathrm{Norm}(m) \equiv 0 \mod 2p$, and $f^m(\tau) \in R_p^\times$.

Moreover, the map Ψ_0 is surjective. This follows from Corollary 5.3 (notice that m_a belongs to $M_{0,p}$ when a satisfies $\deg(a) = 0$ and $N(a) \equiv 0 \mod 2p$) and the fact that $\left((R_p^\times)^2 \cdot (R_p^\times)^p\right)/(R_p^\times)^p = R_p^\times/(R_p^\times)^p$ since $p \neq 2$.

Finally, both $M_{0,p}/pM_{0,p}$ and $R_p^\times/(R_p^\times)^p$ are $\mathbb{F}_p$-modules of rank $\frac{p^2-3}{2}$. Therefore the map is also injective. □

As we will see next, the isomorphism Ψ_0 and Theorem 4.5 will be the key ingredients in the proof of Theorem 2.2.

5.1 Proof of Theorem 2.2 in the Inert Case

In Section 3.2, the proof was reduced to show that $|\psi(N/pQ)| \geq p^4$. Notice that the natural map $q\colon Q_0/pQ_0 \to Q/pQ$ is an injection, thus, it suffices to show that $|\psi \circ q(N_0/pQ_0)| \geq p^4$. In order to finish the proof of the theorem, we will define a map $\Psi\colon Q_0/pQ_0 \to \ell_1^*/(\ell_1^*)^p$ (essentially Ψ_0) such that $\psi \circ q(N_0/pQ_0) = \Psi(N_0/pQ_0)$ and show that $|\Psi(N_0/pQ_0)| \geq p^4$.

Recall that by Proposition 5.4, the map Ψ_0 gives an isomorphism between $M_{0,p}/pM_{0,p}$ and $R_p^\times/(R_p^\times)^p$. On the other hand, Theorem 4.5 establishes that $[E_p^\times\colon R_p^\times] = \lambda h_p$, with $\lambda = 2^\alpha \cdot 3^\beta$, and by assumption $p \nmid h_p$ and $p \geq 7$. It follows that the natural map:

$$R_p^\times/(R_p^\times)^p \hookrightarrow E_p^\times/(E_p^\times)^p \tag{7}$$

is an injection (in fact an isomorphism). Choose a set of generators $\{\xi_i\}$ of the free part of $\mathcal{E}_p^\times$, so that the classes $[\pm\xi_i]$ generate $E_p^\times$, and define a map

$$E_p^\times/(E_p^\times)^p \hookrightarrow \mathcal{E}_p^\times/(\mathcal{E}_p^\times)^p, \quad [\xi_i] \mod (E_p^\times)^p \quad \mapsto \quad \xi_i \mod (\mathcal{E}_p^\times)^p \tag{8}$$

This map is clearly an injection. Moreover we have maps:

$$\mathcal{E}_p^\times/(\mathcal{E}_p^\times)^p \hookrightarrow K(p)^*/(K(p)^*)^p \longrightarrow \ell_1^*/(\ell_1^*)^p = \widetilde{K(p)}^* / \left(\widetilde{K(p)}^*\right)^p \tag{9}$$

where the first map is injective and the kernel of the second map is exactly $\mu_p(K(p)^*)^p$ modulo $(K(p)^*)^p$ by Kummer theory. Note that by construction the image of (8) is disjoint from $\mu_p(\mathcal{E}_p^\times)^p/(\mathcal{E}_p^\times)^p$, therefore the composition of (7), (8) and (9):

$$R_p^\times/(R_p^\times)^p \hookrightarrow E_p^\times/(E_p^\times)^p \hookrightarrow \mathcal{E}_p^\times/(\mathcal{E}_p^\times)^p \longrightarrow \ell_1^*/(\ell_1^*)^p \tag{10}$$

is injective.

We define a map $\Psi\colon Q_0/pQ_0 \to \ell_1^*/(\ell_1^*)^p$ given by the composition of the map $\gamma\colon Q_0/pQ_0 \to M_{0,p}/pM_{0,p}$ (as defined for Lemma 3.15), the isomorphism Ψ_0 and the resulting map from (10). Lemma 3.15, Proposition 5.4 and the remarks above show that $|\Psi(N_0/pQ_0)| = p^4$, and, from the definitions of the several maps involved, it is clear that $\Psi(m) = \psi \circ q(m)$, for all $m \in N_0/pQ_0$. Thus, Theorem 2.2 is proved in the inert case. □

6 The Split Case

In this section we assume that the rational prime p splits in K. Let $\wp, \wp' = \overline{\wp}$ be the two distinct integral prime ideals of $\mathcal{O}_K$ lying above p, so that $p\mathcal{O}_K = \wp \cdot \wp'$.

Let α be a fixed generator of $\wp$ and let α' be the complex conjugate of α. Recall that in Def. 3.6 we fixed a map $\iota\colon \mathbb{F}_p^2 \to \mathcal{O}_K/(p)$ such that $\iota(r) = \iota(r_1, r_2) = r_1\alpha + r_2\alpha'$.

6.1 The Split Robert Group

As usual, we write $K(\wp)$ (resp. $K(\wp')$) for the ray class field of K of conductor $\wp$ (resp. $\wp'$). Notice that both $K(\wp), K(\wp')$ are subfields of $K(p)$ and since we assume that $h_K = 1$, we also have $K(\wp) \cap K(\wp') = K$. Next we define the Robert groups of units which correspond to these subfields (compare with Definition 4.2).

Let $I_\wp$ be the free abelian group on ideals of K which are prime to $6\wp$. Also, for $a \in I_\wp$, with $a = \sum a(\mathfrak{A})\mathfrak{A}$, we write:

$$g_\wp^{12}(a; \mathcal{O}_K) := \prod_{\mathfrak{A}} g_\wp^{12}(\mathfrak{A}; \mathcal{O}_K)^{a(\mathfrak{A})} = \prod_{\mathfrak{A}} g^{12}(1, \wp \cdot \mathfrak{A}^{-1})^{a(\mathfrak{A})}.$$

Definition 6.1 *The primitive Robert group $\mathfrak{R}_\wp^*$ is the group of all elements:*

$$g_\wp^{12}(a; \mathcal{O}_K), \quad a \in I_\wp \text{ such that } \deg(a) = 0,\ N(a) = 0.$$

We define $\mathfrak{R}_{\wp'}^*$ analogously.

Remark 6.2 *We can rewrite the definition of $\mathfrak{R}_\wp^*$ in terms of the invariants g_p^{12} as follows:*

$$\begin{aligned} g_\wp^{12}(\mathfrak{A}; \mathcal{O}_K) &= g^{12}(1, \wp \cdot \mathfrak{A}^{-1}) = g^{12}(1, \wp \cdot \wp' \cdot (\wp' \cdot \mathfrak{A})^{-1}) \\ &= g^{12}(1, p \cdot (\wp' \cdot \mathfrak{A})^{-1}) = g_p^{12}(\wp' \cdot \mathfrak{A}; \mathcal{O}_K) \end{aligned}$$

and similarly we obtain $g_{\wp'}^{12}(\mathfrak{A}; \mathcal{O}_K) = g_p^{12}(\wp \cdot \mathfrak{A}; \mathcal{O}_K)$.

Definition 6.3 *Let the ideals $\mathfrak{A}_{\bar{r}}$ be defined as in Definition 3.9. We denote by $\overline{R}_\wp$ the set of those $\bar{r} \in \overline{R}$ such that $\wp$ divides $\mathfrak{A}_{\bar{r}}$, and we define $\overline{R}_{\wp'}$ similarly. Last, $\overline{R}^*$ will denote the set of those $\bar{r} \in \overline{R}$ such that $\mathfrak{A}_{\bar{r}}$ is relatively prime to p.*

Remark 6.4

(1) Under the map $\iota^{-1}\colon \mathcal{O}_K/(p) \to \mathbb{F}_p^2$, $\iota^{-1}(r_1\alpha + r_2\alpha') = (r_1, r_2)$ one has bijections:

$$\overline{R}^* = (\mathcal{O}_K/(p))^*/\pm 1 \cong (\mathbb{F}_p^* \times \mathbb{F}_p^*)/\{\pm 1\}$$
$$\overline{R}_\wp = (\wp\mathcal{O}_K/p\mathcal{O}_K)/\{\pm 1\} \cong (\mathbb{F}_p^* \times \{0\})/\{\pm 1\}$$
$$\overline{R}_{\wp'} = (\wp'\mathcal{O}_K/p\mathcal{O}_K)/\{\pm 1\} \cong (\{0\} \times \mathbb{F}_p^*)/\{\pm 1\}$$

(2) *Note that $\overline{R} = \overline{R}^* \cup \overline{R}_\wp \cup \overline{R}_{\wp'}$. Also notice that the sets $\overline{R}_\wp, \overline{R}_{\wp'}$ and $\overline{R}^*$ are pairwise disjoint and independent of the choice of ideals $\mathfrak{A}_{\bar{r}}$. Indeed, let us assume that $\wp \mid \mathfrak{A}_{\bar{r}} = (a)$, and let $\mathfrak{B}_{\bar{r}} = (b)$ be another integral ideal, relatively prime to 6, such that $b \equiv \iota(r) \mod p$. Then $a \equiv b \mod p$, so there exists $\beta \in \mathcal{O}_K$ such that $b = a + p \cdot \beta$. Since we assumed that $\wp \mid \mathfrak{A}_{\bar{r}}$, then we conclude that $\wp \mid \mathfrak{B}_{\bar{r}}$, as we claimed. Similarly, if $\mathfrak{A}_{\bar{r}}$ is relatively prime to p, then any other choice of ideal would be relatively prime to p.*

Let J be the free abelian group on integral ideals of K which are relatively prime to 6 and not divisible by p and let J_S be the free abelian group on the ideals attached to the elements of the set S, where $S \in \{\overline{R}, \overline{R}^*, \overline{R}_\wp, \overline{R}_{\wp'}\}$.

Proposition 6.5 *(Compare with Proposition 5.1) Let $p \geq 7$ be a split prime in K. The groups $\mathfrak{R}_p^*$, $\mu_p \cdot \mathfrak{R}_\wp^*$ (and similarly $\mu_p \cdot \mathfrak{R}_{\wp'}^*$) can be described as follows:*

$$\mu_p \mathfrak{R}_\wp^* = \mu_p \cdot \{g_p^{12}(a;\mathcal{O}_K) : a \in J_{\overline{R}_{\wp'}} \text{ with } \deg(a) = 0,\ N(a) \equiv 0 \mod 2\}$$
$$\mathfrak{R}_p^* = \mu_p \cdot \{g_p^{12}(a;\mathcal{O}_K) : a \in J_{\overline{R}^*} \text{ with } \deg(a) = 0,\ N(a) \equiv 0 \mod 2p\}$$

If we define $\mathfrak{S}_p := \mu_p \cdot \{g_p^{12}(a;\mathcal{O}_K) : a \in J$ with $\deg(a) = 0,\ N(a) = 0\}$ then:

$$\mathfrak{S}_p = \mu_p \cdot \{g_p^{12}(a;\mathcal{O}_K) : a \in J_{\overline{R}} \text{ with } \deg(a) = 0,\ \mathrm{Norm}(a) \equiv 0 \mod 2p\}$$

PROOF. The proof is entirely analogous to that of Proposition 5.1 (also, the proposition is essentially proved in [6], Theorem 4.3, p. 258). Notice that by Remark 6.2, we can rewrite the products in the definition of $\mathfrak{R}_\wp^*$ (resp. $\mathfrak{R}_{\wp'}^*$) in terms of the functions g_p^{12}, evaluated at ideals which are divisible by $\wp'$ (resp. $\wp$). Moreover, notice that if $a \in J_{\overline{R}_\wp}$ (or $J_{\overline{R}_{\wp'}}$), then every ideal that appears in a has norm which is congruent to 0 modulo p. Thus $N(a) \equiv 0 \mod p$. □

Remark 6.6

(1) *The groups of units $\mathfrak{R}_\wp^*, \mathfrak{R}_{\wp'}^*$ are subgroups of the Robert group $\mathfrak{R}_p^*$ (for this see [6], Chapter 11, §6). Proposition 6.5 implies that there are certain relations between the invariants $g_\wp, g_{\wp'}$ and g_p. These are called distribution relations and will be determined below.*

(2) *We would like to define a map Ψ_0 in the split case in a similar way as defined in Proposition 5.4 for the inert case. Proposition 6.5 shows that whenever $a \in J_S$ with $S \in \{\overline{R}_\wp, \overline{R}_{\wp'}, \overline{R}^*\}$, and $\deg(a) = \mathrm{Norm}(a) \equiv 0$*

mod $2p$, then $g_p^{12}(a;\mathcal{O}_K) \in \mathfrak{R}_p^*$. However, as we will see, when $a \in J_{\overline{R}}$, the number $g_p^{12}(a;\mathcal{O}_K)$ belongs to a larger subgroup of $K(p)^*/(K(p)^*)^p$.

In order to construct Ψ_0 in the split case, we start with a simple lemma.

Lemma 6.7 *If $a \in J$ and $\deg(a) = 0 = \mathrm{Norm}(a)$ then $g_p^{12}(a;\mathcal{O}_K) \in K(p)^*$.*

PROOF. Let $\mathfrak{A} \subseteq \mathcal{O}_K$ be an integral ideal not divisible by p. We define the invariant (cf. [6], p. 252, invariant $u_{\mathfrak{A}}(C_0)$):

$$u(\mathfrak{A}) = \frac{g^{12}(1, p\mathcal{O}_K)^{\mathbf{N}(\mathfrak{A})}}{g^{12}(1, p\mathfrak{A}^{-1})}$$

Then $u(\mathfrak{A}) \in K(p)^*$ (by [6], p. 252, Theorem 4.1, and the fact that the Siegel functions are non-vanishing in the upper half plane). Let us assume that $a \in J$, with $\deg(a) = \mathrm{Norm}(a) = 0$. In particular, $\sum a(\mathfrak{A})\mathbf{N}(\mathfrak{A}) = 0$. Thus:

$$\begin{aligned} g_p^{12}(a;\mathcal{O}_K) &= \prod g^{12}(1, p\mathfrak{A}^{-1})^{a(\mathfrak{A})} = \prod \left(\frac{g^{12}(1, p\mathcal{O}_K)^{\mathbf{N}(\mathfrak{A})}}{g^{12}(1, p\mathfrak{A}^{-1})} \right)^{-a(\mathfrak{A})} \\ &= \prod u(\mathfrak{A})^{-a(\mathfrak{A})} \in K(p)^*. \qquad \square \end{aligned}$$

Definition 6.8 *We define a homomorphism of $\mathbb{F}_p$ -vector spaces:*

$$\begin{aligned} \Psi_0 \colon M_{0,p}/pM_{0,p} &\longrightarrow K(p)^*/\left(\mu_p \cdot (K(p)^*)^p\right) \\ m + pM_{0,p} &\mapsto f^m(\tau) = \prod_{r \in R} g^{12}(\mathfrak{A}_{\bar{r}}; \mathcal{O}_K)^{m(r)} \mod \mu_p \cdot (K(p)^*)^p. \end{aligned}$$

We claim that the map Ψ_0 is well defined. Indeed, any $m \in M_{0,p}$ satisfies $\deg(m) = 0$ and $\mathrm{Norm}(m) \equiv 0 \mod 2p$ (see Proposition 5.4). By the last part of Proposition 6.5, we can find $a \in J$ with $\deg(a) = 0$ and $N(a) = 0$ and a pth root of unity ζ such that $f^m(\tau) = \zeta \cdot g_p^{12}(a;\mathcal{O}_K)$. Thus, Lemma 6.7 implies that $f^m(\tau) \in K(p)^*$.

In order to study this map, we define some new submodules of $M_{0,p}$. For $S \subseteq \overline{R}$, we denote by $M_{0,p}^S$ the submodule of those $m \in M_{0,p}$ which are supported on those $r \in R$ such that $\bar{r} \in S$, i.e. if $\bar{r} \notin S$, then $m(r) = m(-r) = 0$.

Lemma 6.9 *If $p \nmid h_p$ then the map Ψ_0 restricted to $\left(M_{0,p}^{\overline{R}^*} + pM_{0,p}\right)/pM_{0,p}$ is injective.*

PROOF. This is a direct consequence of Proposition 6.5. Indeed, a slight modification of the argument used in Corollary 5.3 yields:

$$\mu_p \cdot \{\prod_{r\in R} g^{12}(\mathfrak{A}_{\bar{r}}; \mathcal{O}_K)^{m(r)} : m \in M_{0,p}^{\overline{R}^*}\} = (\mathfrak{R}_p^*)^2.$$

Notice that $\overline{R}^*$ contains $\frac{(p-1)^2}{2}$ elements, therefore $M_0^{\overline{R}^*}$ and $M_{0,p}^{\overline{R}^*}$ are both free modules of rank $\frac{(p-1)^2}{2} - 1$, and $\mathfrak{R}_p^*/\mu_p$ has the same rank, by Theorem 4.5. Since $p \geq 7$:

$$\begin{aligned}\Psi_0(M_{0,p}^{\overline{R}^*} + pM_{0,p}) &= (\mathfrak{R}_p^*)^2 \cdot (K(p)^*)^p / \left(\mu_p \cdot (K(p)^*)^p\right) \\ &= \mathfrak{R}_p^* \cdot (K(p)^*)^p / \left(\mu_p \cdot (K(p)^*)^p\right).\end{aligned}$$

Recall that by Theorem 4.5 we have $[\mathcal{E}_p^\times : \mathfrak{R}_p^*] = 2^\alpha \cdot 3^\beta \cdot h_p$ for some $\alpha, \beta \in \mathbb{Z}$. By hypothesis $p \nmid h_p$ and $p \geq 7$, therefore $\mathfrak{R}_p^* \cdot (\mathcal{E}_p^\times)^p / (\mu_p \cdot (\mathcal{E}_p^\times)^p)$ has dimension $\frac{(p-1)^2}{2} - 1$, the free rank of $\mathcal{E}_p^\times$. Hence, Ψ_0 must be injective on $(M_{0,p}^{\overline{R}^*} + pM_{0,p})/pM_{0,p}$ since its image has the same dimension. □

Next we describe the kernel of Ψ_0, which we will denote by $\mathcal{D} := \mathrm{Ker}(\Psi_0)$. Notice that the previous lemma implies that $\dim \mathcal{D} \leq \frac{p^2-3}{2} - (\frac{(p-1)^2}{2} - 1) = p-1$. We will prove that, in fact, the dimension equals $p-3$. The kernel will turn out to be generated by the distribution relations which can be found in Robert's original article [13] and Kubert-Lang.

6.2 The Distribution Relations.

The following is a restatement of Theorem 1.4 of [6], p. 237.

Theorem 6.10 *Let $C' \in \mathrm{Cl}(\wp')$ be an arbitrary class in the ray class group of conductor $\wp'$, and let $\mathcal{C}' \in C'$ be an integral ideal. Let $u_1, \ldots, u_p$ be a complete system of residue classes of $\mathcal{O}_K$ modulo $\wp$ such that $u_i \equiv 1 \mod \wp'$, $u_1 \equiv 0 \mod \wp$. Analogously, let $\mathcal{C} \in C \in \mathrm{Cl}(\wp)$ and let $v_1, \ldots, v_p$ be a system of residue classes of $\mathcal{O}_K$ mod $\wp'$ with $v_j \equiv 1 \mod \wp$, $v_1 \equiv 0 \mod \wp'$. Also, fix an integral ideal $\mathfrak{P}$ (resp. $\mathfrak{P}'$) which lies in the same class as $\wp^{-1}$ of $\mathrm{Cl}(\wp')$ (resp. in the same class as $(\wp')^{-1}$ of $\mathrm{Cl}(\wp)$). Then there exist pth roots of unity $\xi_k, k = 1, \ldots, 4$ such that:*

(1)

$$\prod_{i=2}^{p} g_p^{12}(u_i \cdot \mathcal{C}'; \mathcal{O}_K) = \xi_1 \cdot \frac{g_p^{12}(\wp \cdot \mathcal{C}'; \mathcal{O}_K)}{g_p^{12}(\wp \cdot \mathfrak{P} \cdot \mathcal{C}'; \mathcal{O}_K)};$$
$$\prod_{i=2}^{p} g_p^{12}(v_i \cdot \mathcal{C}; \mathcal{O}_K) = \xi_2 \cdot \frac{g_p^{12}(\wp' \cdot \mathcal{C}; \mathcal{O}_K)}{g_p^{12}(\wp' \cdot \mathfrak{P}' \cdot \mathcal{C}; \mathcal{O}_K)}.$$

(2)

$$\prod_{\bar{r} \in \overline{R}_{\wp'}} g_p^{12}(\mathfrak{A}_{\bar{r}}; \mathcal{O}_K) = \xi_3 \cdot \frac{\Delta(\mathcal{O}_K)}{\Delta(\wp)}\ ; \quad \prod_{\bar{r} \in \overline{R}_{\wp}} g_p^{12}(\mathfrak{A}_{\bar{r}}; \mathcal{O}_K) = \xi_4 \cdot \frac{\Delta(\mathcal{O}_K)}{\Delta(\wp')}.$$

PROOF. The equalities are obtained by taking pth roots of the equations found in Theorem 1.4 of [6], by taking $\mathfrak{f} = \wp'$ and then also reversing the roles of $\wp$ and $\wp'$. For clarity, all invariants have been expressed using the notation g_p^{12} in preference to the notation $g_\wp(C) := g^{12p}(1, p \cdot \mathcal{C}^{-1})$ defined in [6], p. 234, 235. For part (ii), note that $\{\mathfrak{A}_{\bar{r}} : \bar{r} \in \overline{R}_{\wp'}\} = \{\wp' \cdot \mathfrak{B}_{\bar{r}} : \bar{r} \in \overline{R}\}$ for some integral ideals $\mathfrak{B}_{\bar{r}}$, which are a complete system of representatives of classes of $\mathrm{Cl}(\wp)$. Thus:

$$\prod_{\bar{r} \in \overline{R}_{\wp'}} g_p^{12}(\mathfrak{A}_{\bar{r}}; \mathcal{O}_K) = \prod_{C \in \mathrm{Cl}(\wp)} g_\wp(C) = \xi_3 \cdot \frac{\Delta(\mathcal{O}_K)}{\Delta(\wp)}.$$

Note that in our case $\mathrm{Cl}(1)$ is the class group of K, which is assumed to be trivial. Also note that all the exponents that appear in [6], Theorem 1.4, are identically 1 in our case. □

The distribution relations in Theorem 6.10 will induce elements in $M_{0,p}$ which belong to $\mathcal{D}$, the kernel of the homomorphism Ψ_0. The symbol $\mathbf{1}_{\bar{r}}$ will denote the characteristic function $R \to \mathbb{Z}$ for the elements $\pm r$, i.e. $\mathbf{1}_{\bar{r}}(s) = 1$ if $s = \pm r$ and is 0 otherwise.

Corollary 6.11 *With the notation of Theorem 6.10, for each $C \in \mathrm{Cl}(\wp)$, let $\mathcal{C} \in C$ be an integral ideal relatively prime to $\wp'$. Similarly for $C' \in \mathrm{Cl}(\wp')$, let $\mathcal{C}' \in C'$ with $\wp \nmid \mathcal{C}'$. The relations in 6.10 (1) are represented by the elements of M defined by*

$$m_{\beta,\wp} := \sum_{i=0}^{p-1} \mathbf{1}_{(\beta,i)} - \mathbf{1}_{(\beta c_\wp,0)}, \quad m_{\beta,\wp'} := \sum_{i=0}^{p-1} \mathbf{1}_{(i,\beta)} - \mathbf{1}_{(0,\beta c_\wp)}$$

where β runs through a set of representatives of $\mathbb{F}_p^*/\{\pm 1\}$ and $c_\wp \equiv \alpha + \alpha'$ mod p. *Thus $[f^{m_{\beta,\wp}}(\tau)] = [f^{m_{\beta,\wp'}}(\tau)] = [1] \in \mathfrak{R}_p^*/\mu_p$.*

PROOF. Let $\mathcal{C}'$ be an ideal as in the statement of the lemma and suppose that $\mathcal{C}'$ has a generator which is congruent to $c_1\alpha + c_2\alpha'$ modulo p (thus $c_2 \neq 0 \mod p$). We simply write (c_1, c_2) under the identification given by ι^{-1}. When j runs over a set of representatives of $\mathbb{F}_p^*/\{\pm 1\}$, the elements (c_1, jc_2) run over a set of generators of the ideals $u_i\mathcal{C}'$, $2 \leq i \leq p$. Moreover, the ideal $\wp\mathcal{C}'$ has a generator congruent to

$$\alpha(c_1\alpha + c_2\alpha') \equiv c_1\alpha^2 \equiv c_1(\alpha + \alpha')\alpha \equiv c_1 c_\wp \alpha \mod p$$

which we represent by $(c_1 c_\wp, 0)$. Similarly, the ideal $\wp\mathfrak{P}\mathcal{C}'$ has a generator congruent to $(c_1, 0)$. This shows that the elements $m_{\beta,\wp}$ represent the first $(p-1)/2$ relations in 6.10 (1). $\square$

Lemma 6.12 *Let $\chi\colon \mathbb{F}_p^*/\{\pm 1\} \to \mathbb{Z}_p^*$ and define elements of $\mathcal{M} = M \otimes \mathbb{Z}_p$ by:*

$$m_{\chi,\wp} = \sum_\beta \chi(\beta) m_{\beta,\wp}$$

where the sum is over a set of representatives of $\mathbb{F}_p^*/\{\pm 1\}$. Let $m_{\chi,\wp'}$ be defined analogously. If χ is not trivial then

$$\deg(m_{\chi,\wp}) = \deg(m_{\chi,\wp'}) = 0, \quad \mathrm{Norm}(m_{\chi,\wp}) = \mathrm{Norm}(m_{\chi,\wp'}) \equiv 0 \mod p.$$

In other words, $m_{\chi,\wp}, m_{\chi,\wp'} \in \mathcal{M}_{0,p}$. If χ_0 is the trivial character, then the degree of $m_{\chi_0,\wp}$ is $(p-1)^2$ and $\mathrm{Norm}(m_{\chi_0,\wp'}) \equiv 0 \mod p$.

PROOF. For any β, one easily checks that $\deg(m_{\beta,\wp}) = 2(p-1)$. Thus, if χ is non-trivial:

$$\deg(m_{\chi,\wp}) = \sum_\beta \chi(\beta) \deg(m_{\beta,\wp}) = 2(p-1) \sum_\beta \chi(\beta) = 0.$$

Similarly, if χ_0 is the trivial character, $\deg(m_{\chi,\wp}) = 2(p-1)\sum_\beta 1 = (p-1)^2$. In order to show the claim about the norm, notice that:

$$\mathbf{N}(\mathfrak{A}_{\bar{r}}) \equiv \mathbf{N}(r_1\alpha + r_2\alpha') \equiv r_1 r_2 (\tau - \bar{\tau})^2 \mod p \tag{11}$$

where τ is the previously defined element of the basis $\mathcal{O}_K = \mathbb{Z} \oplus \tau\mathbb{Z}$. Thus $(\tau - \bar{\tau})^2$ is an integer which is non-zero modulo p. As a consequence of Eq. (11), a simple calculation shows that $\mathrm{Norm}(m_{\beta,\wp}) \equiv 0 \mod p$ for any β. Hence, by the linearity of the norm, we obtain $\mathrm{Norm}(m_{\chi,\wp}) \equiv 0 \mod p$ for any χ. $\square$

Remark 6.13 *The elements $m_{\chi,\wp}$ can be easily evaluated on elements of R. If $r_1 \neq 0$ then*

$$m_{\chi,\wp}(r_1, r_2) = \chi(r_1)(1 - \chi(c_\wp^{-1})\delta_{0,r_2})$$

where $\delta_{i,j}$ is the Kronecker δ-function and $m_{\chi,\wp}(r_1, r_2) = 0$ when $r_1 = 0$. Similarly, if $r_2 \neq 0$ then $m_{\chi,\wp'}(r_1, r_2) = \chi(r_2)(1 - \chi(c_\wp^{-1})\delta_{0,r_1})$.

At this point, we introduce another natural group action on M, finer than the action of $\mathrm{PSL}(2,\mathbb{F}_p)$. From now on, we define $G = \mathbb{F}_p^* \times \mathbb{F}_p^* \cong (\mathcal{O}_K/\wp)^* \times (\mathcal{O}_K/\wp')^* \cong (\mathcal{O}_K/(p))^*$ which acts on $\mathcal{O}_K/(p)$ by multiplication. Notice that if $g = (\lambda, \mu) \in G$ then $g \cdot (r_1\alpha + r_2\alpha') = \lambda r_1\alpha + \mu r_2\alpha'$. Under ι^{-1} this induces a group action on R defined by $g \cdot r = (\lambda r_1, \mu r_2)$ and an action on M, defined by:

$$g \cdot m(r) = m(gr)$$

for all $g \in G$. Notice that $M_{0,p}$ is a $\mathbb{Z}[G]$-submodule of M because for any $g \in G$ and $m \in M$ one has $\deg(gm) = \deg(m)$ and $\mathrm{Norm}(gm) \equiv \mathbf{N}(g^{-1})\,\mathrm{Norm}(m) \mod p$. Moreover, by the previous remark, $g \cdot m_{\chi,\wp} = \chi(\lambda)m_{\chi,\wp}$ and $g \cdot m_{\chi,\wp'} = \chi(\mu)m_{\chi,\wp}$ for $g = (\lambda, \mu) \in G$.

Lemma 6.14 *The $p-3$ elements in the set*

$$\{m_{\chi,\wp},\ m_{\chi,\wp'} |\ \chi\colon \mathbb{F}_p^*/\{\pm 1\} \to \mathbb{Z}_p^* \text{ non-trivial }\}$$

are linearly independent modulo $p\mathcal{M}_{0,p}$. Let H be the $\mathbb{Z}_p$-module spanned by them. The image of H in $\mathcal{M}_{0,p}/p\mathcal{M}_{0,p}$, denoted by $\mathcal{H}$, belongs to the kernel of Ψ_0.

PROOF. The $\mathbb{F}_p$-module inside $\mathcal{M}_{0,p}/p\mathcal{M}_{0,p}$ generated by the elements $m_{\chi,\wp}$, $m_{\chi,\wp'}$ is in fact a $\mathbb{F}_p[G]$-submodule and the 1-dimensional spaces generated by $m_{\chi,\wp}$ or $m_{\chi,\wp'}$ are $\mathbb{F}_p[G]$-submodules. Furthermore, the action of G on each 1-dimensional subspace is distinct, thus they are all independent and

$$\mathcal{H} \cong \bigoplus_{\chi \neq \chi_0} m_{\chi,\wp}\mathbb{F}_p \oplus m_{\chi,\wp'}\mathbb{F}_p$$

as $\mathbb{F}_p[G]$-module. By Corollary 6.11, the elements of $\mathcal{H}$ belong to the kernel of Ψ_0. $\square$

Next we construct the remaining 2 dimensional space of $M_{0,p}/pM_{0,p}$:

Lemma 6.15 *Define elements of M by:*

$$m_\wp := 2\sum_{\bar{r}\in\overline{R}_\wp} \mathbf{1}_{\bar{r}}, \quad m_{\wp'} := 2\sum_{\bar{r}\in\overline{R}_{\wp'}} \mathbf{1}_{\bar{r}}.$$

If χ_0 denotes the trivial character, then $\frac{p-1}{2}m_\wp - m_{\chi_0,\wp}$, $\frac{p-1}{2}m_{\wp'} - m_{\chi_0,\wp'}$ belong to $M_{0,p}$. Furthermore, if we let P be the subspace generated by these elements in $M_{0,p}/pM_{0,p}$, then Ψ_0 restricted to P is injective and the image of P via Ψ_0 is the subspace generated multiplicatively by α, α', where $(\alpha) = \wp$, $(\alpha') = \wp'$.

PROOF. Note that all ideals $\mathfrak{A}_{\bar{r}}$ with $\bar{r} \in \overline{R}_{\wp} \cup \overline{R}_{\wp'}$ are divisible by either $\wp$ or $\wp'$, thus $\mathbf{N}(\mathfrak{A}_{\bar{r}}) \equiv 0 \mod p$. Moreover, there are $\frac{p-1}{2}$ elements in $\overline{R}_{\wp}$, so:

$$\deg(m_{\wp}) = \deg(m_{\wp'}) = 2(p-1), \quad \mathrm{Norm}(m_{\wp}) \equiv \mathrm{Norm}(m_{\wp'}) \equiv 0 \mod p.$$

Recall that $\deg(m_{\chi_0,\wp}) = (p-1)^2, \mathrm{Norm}(m_{\chi_0,\wp}) \equiv 0 \mod p$ (see Lemma 6.12), thus both elements $m = \frac{p-1}{2} m_{\wp} - m_{\chi_0,\wp}, m' = \frac{p-1}{2} m_{\wp'} - m_{\chi_0,\wp'}$ belong to $M_{0,p}$.

Let $P = \langle m, m' \rangle \subset M_{0,p}/pM_{0,p}$. By Corollary 6.11, we know that $f^{m_{\chi_0,\wp}}(\tau)$ is a pth root of unity. Now the second part of the lemma follows from the second set of distribution relations of Theorem 6.10. Indeed, for example

$$\prod_{\bar{r} \in \overline{R}_{\wp}} g_p^{12}(\mathfrak{A}_{\bar{r}}; \mathcal{O}_K) = \xi_4 \cdot \frac{\Delta(\mathcal{O}_K)}{\Delta(\wp')}$$

implies that $f^{m_{\wp}}(\tau) = \prod_{\bar{r} \in \overline{R}_{\wp}} g_p^{12}(\mathfrak{A}_{\bar{r}}; \mathcal{O}_K)^{2 \cdot m_{\wp}(\bar{r})} = \prod_{\bar{r} \in \overline{R}_{\wp}} g_p^{12}(\mathfrak{A}_{\bar{r}}; \mathcal{O}_K)^4 = \xi_4^4 \cdot \left(\frac{\Delta(\mathcal{O}_K)}{\Delta(\wp')}\right)^4$, which is, up to a pth root of unity, a generator of $(\wp')^{48}$ (for this, see for example [6], Theorem 3.1, p. 264). Hence, the subspace generated by m maps by Ψ_0 to the space generated by α (because $\gcd(48, p) = 1$). Similarly, the subspace generated by m' maps by Ψ_0 to the space generated by α'.

For the injectivity, we first show that α does not belong to $(\mu_p \cdot (K(p)^*)^p)$. This follows from the fact that $(\alpha) = \wp$ and $[K(p) : K] = \frac{(p-1)^2}{2}$, so $\wp$ is not the pth power of an ideal in $K(p)$ (since $K(p)/K$ is a Galois extension and $p \nmid \frac{(p-1)^2}{2}$). With a similar argument, one can show that α and α' are independent modulo $(\mu_p \cdot (K(p)^*)^p)$. $\square$

Definition 6.16 *We define the Robert group of p-units, S_p, to be the multiplicative group generated by $\mathfrak{R}_p^*$ and all powers of α, α'.*

We summarize our work in the following proposition. Here $\mathcal{H}$ denotes $(\langle H \rangle + pM_{0,p})/pM_{0,p}$.

Proposition 6.17 *The map Ψ_0 can be rewritten as:*

$$\Psi_0 \colon M_{0,p}/pM_{0,p} \longrightarrow S_p/(\mu_p \cdot (S_p)^p) \longrightarrow (K(p)^*)/\left(\mu_p \cdot (K(p)^*)^p\right)$$

Moreover, with the notation of the previous results:

$$M_{0,p}/pM_{0,p} = (M_{0,p}^{\overline{R}^*} + pM_{0,p})/pM_{0,p} \oplus P \oplus \mathcal{H}$$

and the kernel of $\Psi_1 \colon M_{0,p}/pM_{0,p} \longrightarrow S_p/(\mu_p \cdot (S_p)^p)$ equals $\mathcal{H}$.

PROOF. We start by proving the decomposition of $M_{0,p}/pM_{0,p}$. Lemma 6.9 and 6.15 provide descriptions of the image via Ψ_0 of $(M_{0,p}^{\overline{R}^*} + pM_{0,p})/pM_{0,p}$ and

P, respectively (they are, essentially, $\mathfrak{R}_p^*/\mu_p$ and $\alpha^i \cdot \alpha'^j$). Moreover, it is clear that the image subgroups are linearly independent modulo $(\mu_p \cdot (K(p)^*)^p)$. Therefore $(M_{0,p}^{\overline{R}^*} + pM_{0,p})/pM_{0,p}$ and P are also linearly independent.

By Lemma 6.14, $\mathcal{H} \subset \mathrm{Ker}(\Psi_0)$, therefore $\mathcal{H}$ is linearly independent of $(M_{0,p}^{\overline{R}^*} + pM_{0,p})/pM_{0,p} \oplus P$.

Finally note that:

$$\begin{aligned}&\dim\left((M_{0,p}^{\overline{R}^*} + pM_{0,p})/pM_{0,p} \oplus P \oplus \mathcal{H}\right) = \\ &= \left(\frac{(p-1)^2}{2} - 1\right) + 2 + (p-3) = \frac{p^2-3}{2} = \dim M_{0,p}/pM_{0,p}\end{aligned}$$

which concludes the proof of the decomposition into subspaces. Also, since we have analyzed the image of each subspace, we see that Ψ_0 factors through $S_p/(\mu_p \cdot (S_p)^p)$, as claimed. $\square$

6.3 Proof of Theorem 2.2 in the Split Case

By Lemma 3.15, the image of N_0/pQ_0 in $M_{0,p}/pM_{0,p}$ is of dimension 4 (the proof is independent of the splitting of p). We now prove that it intersects the kernel of Ψ_1 trivially, in the split case, and hence, it injects into $S_p/\mu_p \cdot (S_p)^p$. Recall that $N_0/pQ_0 \cong \mathcal{N}_0/p\mathcal{Q}_0 \cong p\mathcal{M}_0/p\mathcal{Q}_0 \oplus \mathcal{W}_2/p\mathcal{M}_{(2)}$, as we saw in the proof of Lemma 3.15.

Lemma 6.18 *The intersection of $pM_0/pM_{0,p}$ and $\mathcal{H}$, the kernel of Ψ_1, is trivial.*

PROOF. If $m \in pM_0$ then $m(r) \equiv 0 \mod p$ for all $r \in R$. Thus, by Lemma 6.14, if such an element m is also in $\mathcal{H}$ then it belongs to $pM_{0,p}$. $\square$

Lemma 6.19 *Under the hypothesis of Theorem 2.2, the intersection of the spaces $\mathcal{W}_2/p\mathcal{M}_{0,p}$ and $\mathcal{H}$ is trivial.*

PROOF. Let $G = \mathbb{F}_p^* \times \mathbb{F}_p^* \cong (\mathcal{O}_K/\wp)^* \times (\mathcal{O}_K/\wp')^*$ be acting on $\mathcal{M}$ as before. Notice that the space $\mathcal{W}_2$ is generated by the elements $m_{1,0}\colon (r_1, r_2) \mapsto r_1^2$, $m_{1,1}\colon (r_1, r_2) \mapsto r_1 r_2$ and $m_{0,1}\colon (r_1, r_2) \mapsto r_2^2$. Moreover, $\mathcal{W}_2$ is an invariant subspace under the action of G and one has a decompositions $\mathcal{W}_2 = m_{1,0}\mathbb{Z}_p \oplus m_{1,1}\mathbb{Z}_p \oplus m_{0,1}\mathbb{Z}_p$ while $H = \bigoplus_\chi m_{\chi,\wp}\mathbb{Z}_p \oplus m_{\chi,\wp'}\mathbb{Z}_p$ as a $\mathbb{Z}_p[G]$-modules. Thus, it suffices to show the linear independence of the pairs $m_{1,0}$, $m_{\omega^2,\wp}$ and $m_{0,1}$,

$m_{\omega^2,\wp'}$ modulo p, where ω is the Teichmüller character, because those are the only two pairs where the action of G coincides. However, the independence is clear by the explicit values given in Remark 6.13. $\square$

Proposition 6.20 *The map Ψ_0 restricted to the 4-dimensional space generated by the image of N_0/pQ_0 in $M_{0,p}/pM_{0,p}$ is injective.*

PROOF. By Proposition 6.17, the map Ψ_0 factors:

$$\Psi_0 \colon M_{0,p}/pM_{0,p} \longrightarrow S_p/\mu_p \cdot (S_p)^p \longrightarrow (K(p)^*)/\left(\mu_p \cdot (K(p)^*)^p\right)$$

and the kernel of $\Psi_1 \colon M_{0,p}/pM_{0,p} \longrightarrow S_p/\mu_p \cdot (S_p)^p$ is the subspace $\mathcal{H}$.

Since $N_0/pQ_0 = pM_0/pQ_0 \oplus W_0/pQ_0$, by Lemmas 6.18 and 6.19, we see that N_0/pQ_0 injects into $S_p/\mu_p \cdot (S_p)^p$, where S_p is the Robert group of p-units.

It remains to show that $S_p/(\mu_p \cdot (S_p)^p)$ injects into $(K(p)^*)/\left(\mu_p \cdot (K(p)^*)^p\right)$. Let $S = \{\wp, \wp'\}$ and let $\mathcal{O}_{K}{}_S^\times$ be the usual ring of p-units, i.e. the group of all products $\xi \cdot \alpha^i \cdot \alpha'^j$ with $i, j \in \mathbb{Z}$ and $\xi \in \mathcal{O}_K^\times$. Then, we claim that the natural map:

$$S_p/\mu_p \cdot (S_p)^p \hookrightarrow \mathcal{O}_{K}{}_S^\times/\mu_p \cdot (\mathcal{O}_{K}{}_S^\times)^p \tag{12}$$

is an injection. Indeed, suppose that there exist:

$$\gamma \cdot \alpha^i \cdot \alpha'^j = \zeta_p \cdot (\xi \cdot \alpha^n \alpha'^m)^p$$

with $i, j, n, m \in \mathbb{Z}$, $\gamma \in \mathfrak{R}_p^*$ and $\zeta_p \in \mu_p$. Since $\mu_p \subset \mathfrak{R}_p^*$, we can assume that $\zeta_p = 1$. We obtain $\gamma \cdot \alpha^i \cdot \alpha'^j = \xi^p \cdot \alpha^{pn} \cdot \alpha'^{pm}$ and thus $\gamma = \xi^p \cdot \alpha^{pn-i} \cdot \alpha'^{pm-j}$. In particular, $\alpha^{pn-i} \cdot \alpha'^{pm-j} = \gamma \cdot \xi^{-p} \in \mathcal{O}_K^\times$ must be an algebraic unit, so we must have $pn = i$ and $pm = j$. Thus, $\gamma = \xi^p$. However, by Theorem 4.5, and the assumption $p \nmid h_p$, the natural map:

$$R_p^\times/(R_p^\times) \longrightarrow \mathcal{O}_K^\times/(\mathcal{O}_K^\times)^p$$

is injective. Therefore $\xi \in \mathfrak{R}_p^*$ and $\gamma \in \mu_p \cdot (S_p)^p$ and the map in Eq. (12) is an injection as claimed.

It is a standard fact that given any set of prime ideals S, of a number field F, the map:

$$\mathcal{O}_{F}{}_S^\times/(\mathcal{O}_{F}{}_S^\times)^p \longrightarrow F^*/(F^*)^p$$

is an injection, where $\mathcal{O}_{F}{}_S^\times$ denotes the ring of S-units. Therefore,

$$S_p/\mu_p \cdot (S_p)^p \hookrightarrow \mathcal{O}_{K}{}_S^\times/\mu_p \cdot (\mathcal{O}_{K}{}_S^\times)^p \hookrightarrow (K(p)^*)/\left(\mu_p \cdot (K(p)^*)^p\right). \qquad \square$$

Finally, as in the inert case, we define a map $\Psi\colon Q_0/pQ_0 \to \ell_1^*/(\ell_1^*)^p$ given by the composition of $Q_0/pQ_0 \to M_{0,p}/pM_{0,p}$, Ψ_0 and the natural map

$$K(p)^*/\,(\mu_p \cdot (K(p)^*)^p) \to \ell_1^\times/(\ell_1^\times)^p$$

which is an injection. The proposition above implies that $|\Psi(N_0/pQ_0)| = p^4$ and, from the definition of Ψ_0, it is clear that ψ and Ψ agree on N_0/pQ_0. Therefore $|\psi(N/pQ)| \geq p^4$ as desired. □

References

[1] G. Böckle, *Deformations and the rigidity method*, preprint.

[2] N. Boston, *Appendix to [10]*, Compos. Math. 59 (1986), 261-264.

[3] J. Coates, A. Wiles, *Kummer's criterion for Hurwitz numbers*, Algebraic Number Theory (Kyoto Internat. Sympos., Res. Inst. Math. Sci., Univ. Kyoto, Kyoto, 1976), p. 9-23, Japan Soc. Promotion Sci., Tokyo (1977).

[4] M. Deuring, *Die Zetafunktion einer algebraischen Kurve vom Geschlechte Eins*, Nachrichten der Akademie der Wissenschaften in Göttingen. Mathematisch-Physikalische Klasse, 85-94 (1953); II, ibid., 13-42 (1955); III, ibid., 37-76 (1956); IV, ibid., 55-80 (1957).

[5] M. Deuring, *Die Klassenkörper der komplexen Multiplikation*, Enzyklopädie der mathematischen Wissenschaften: Mit Einschluss ihrer Anwendungen, Band I-2, Heft 10, Teil II. Stuttgart: Teubner 1958.

[6] D. S. Kubert, S. Lang, *Modular Units*, Grundlehren der Mathematischen Wissenschaften, vol. 244, Springer-Verlag, New York, 1981.

[7] S. Lang, *Elliptic Functions*, 2nd Edition, Springer-Verlag, New York, 1987.

[8] S. Lang, *Algebraic Number Theory*, 2nd Edition Springer-Verlag, New York, 1994.

[9] A. Lozano-Robledo, *On the surjectivity of Galois representations attached to elliptic curves over number fields*, to appear in Acta Arithmetica.

[10] B. Mazur and A. Wiles, *On p-adic analytic families of Galois representations*, Compositio Mathematica 59 (1986), 231-264.

[11] The PARI Group, PARI/GP, Version 2.1.1, 2000, Bordeaux, available from http://www.parigp-home.de/

[12] K. Ramachandra, *Some Applications of Kronecker's Limit Formulas*, The Annals of Mathematics, Second Series, Volume 80, Issue 1 (Jul. 1964), 104-148.

[13] G. Robert, *Unites Elliptiques*, Bulletin de la Societe Mathematique de France, Memoire 36, Dec 1973.

[14] G. Robert, *Nombres de Hurwitz et Unités Elliptiques*, Ann. scient. Éc. Norm. Sup., 4^e série, t. 11, p. 297-389, (1978).

[15] D. E. Rohrlich, *Universal deformation rings and universal elliptic curves*, unpublished note (available at his website).

[16] D. E. Rohrlich, *False division towers of elliptic curves*. Journal of Algebra 229, 249-279 (2000).

[17] D. E. Rohrlich, *A deformation of the Tate module*. Journal of Algebra 229, 280-313 (2000).

[18] D. E. Rohrlich, *Modular units and the surjectivity of a Galois representation.* Journal of Number Theory 107, (2004) 8-24.

[19] H. Saito, *Elliptic Units and a Kummer's Criterion for Imaginary Quadratic Fields*, Journal of Number Theory 25, (1987), 53-71.

[20] J.-P. Serre, *Abelian l-adic Representations and Elliptic Curves*, W. A. Benjamin, Inc., New York, 1968.

[21] J.-P. Serre, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, Inventiones Mathematicae 15 (1972), 259-331.

[22] J.-P. Serre, J. Tate, *Good reduction of abelian varieties*, Annals of Mathematics 88, (1968) 492-517.

[23] R. I. Yager, *A Kummer criterion for imaginary quadratic fields*, Compositio Math. 47, no. 1, 31-42 (1982).