The Index of Elliptic Units

by

Paul Denis Smith

of

Trinity College

A dissertation submitted for the Degree of Doctor of Philosophy at the University of Cambridge.

July, 1980

Summary of dissertation submitted for the Degree of Doctor of Philosophy at the University of Cambridge by Paul Denis Smith.

Title: The Index of Elliptic Units.

The elliptic units are a naturally arising subgroup of units of any given abelian extension of an imaginary quadratic field K; their definition is motivated by the desire to find units which play the same role as cyclotomic units in abelian extensions of the rationals. The definition outlined in the thesis uses division values of elliptic functions, and provides a simpler starting point of the theory than Robert's original exposition. The properties of these units are established using the theory of good reduction of elliptic curves rather than the classical basis of Robert's proofs.

The index of the elliptic units is calculated for various abelian extensions of K, particularly for ray class fields modulo an ideal h of K, and fields of division points on an elliptic curve defined over K. Here it is assumed that K has class number one and that h is prime to 6- the relaxation of these assumptions introduces inessential technical complications into the result. There is a further restriction on h, which seems essential for the method of proof: h is not divisible by any rational prime which splits in K. Thus these results include the earlier results of Robert for prime power conductors h. These ray class field results are subsequently used to calculate the p-adic value of the index for a field $K(E_g)$ of g-division points on an elliptic curve E (over K) which has good reduction at all primes dividing g. Here p is any rational prime not in the finite set of primes dividing 6 or the degree of ray class field modulo the conductor of E, and E itself has complex multiplication by the ring of integers of K. A similar p-adic result for the elliptic units of an arbitrary finite abelian extension of K is proved.

The special case with g a prime power is important for current work on the arithmetic of elliptic curves. The p-adic result above is used to prove a new result relating the rank of the group of points on E over the field $K(E_p)$ (p a split prime of K) to the invariants of the Iwasawa module attached to the p-adic L-functions.

Preface

I declare that this dissertation entitled "The Index of Elliptic Units" is not substantially the same as any that I have submitted for a degree or diploma or other qualification at any other university. I further state that no part of my dissertation has already been or is being concurrently submitted for any such degree, diploma or other qualification. The dissertation is the result of my own work and includes nothing which is the outcome of work done in collaboration. The material contained in it is, to the best of my belief, original, except where mention is made to the contrary.

I wish to express my thanks to my research supervisor, Professor J. Coates, for his invaluable advice and encouragement: this thesis owes much to his inspiration.

I also wish to thank Trinity College for their generous support, and the Australian National University for their support during the period spent in Canberra.

Finally, I am indebted to Mrs. J. Scutt for the typing of this manuscript.

Paul Smith.
28th July 1980.

Contents

Introduction.

The elliptic units are a natural subgroup of units of any given abelian extension H of an imaginary field K. Their definition is motivated by the desire to find units which play the same role as cyclotomic units in abelian extensions of the rational field. In particular, the index of such a subgroup (in the global units of H) should be essentially the class number of H, and should provide analogues of Kummer's criteria.

The first successful such definition was provided by Robert [18], who crucially improved earlier work of Ramachandra and Siegel; the units arise from special values of certain modular functions. The definition we outline provides a simpler starting point of the theory - it uses division values of elliptic functions, and is closely related to Robert's original definition. The properties of these units are established rather differently, for we use the theory of good reduction of elliptic curves in an intrinsic way, whereas Robert relies upon earlier classical results about the discriminant function and theta functions.

The index of the elliptic units is calculated for various abelian extensions of K, particularly for ray class fields (chapter 2) and fields of division points on an elliptic curve defined over K (chapter 3). The index for other abelian extensions is also described in chapter 3. For technical simplicity, we assume that K has class number one, but it is apparent that our methods extend to fields K of arbitrary class number. Robert computed the index only for extensions H/K of prime power conductor, which is included in our result. Our method was

inspired by the work of Sinnott [25] on the index of circular units in cyclotomic extensions of arbitrary conductor.

The elliptic units in fields of division points on an elliptic curve defined over K are very important in current research on elliptic curves, as evidenced by the work of Coates and Wiles [7], [8]. This underlines the importance of the result of chapter three and in chapter four we use it to prove a new result about the arithmetic of elliptic curves.

A more precise description of the contents of each chapter is given in the introduction to each.

Notation

Let $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ denote respectively the rational integers, the real field, and the complex field. The letter p will be reserved for rational primes, $\mathbb{Z}_p$ and $\mathbb{Q}_p$ will denote the p-adic integers and the p-adic field.

Throughout, K will denote an imaginary quadratic field, with ring of integers o, the letters $a,b,\ldots,\mathfrak{f},g,h\ldots$ will denote ideals of o; p and q will be reserved for prime ideals of K. In chapter one, the notation o_c will be used for an order in K with conductor c; the letters $a,b,\ldots,\mathfrak{f},g,\ldots$ will also be used to denote ideals of o_c.

Throughout $p(z)$ will denote the Weierstrass p-function; since the variable z will usually be included, no confusion should arise with the prime ideal p.

The group of roots of unity in a field F will be denoted μ_F, and its order, if finite, by e_F. If $\mathfrak{P}$ is a prime of F, let $F_{\mathfrak{P}}$ be the completion of F at $\mathfrak{P}$; in this case $\mathfrak{P}$ will also be used for the maximal ideal lying in the ring of integers of $F_{\mathfrak{P}}$. In particular, K_p denotes the completion of K at p; its ring of integers will be denoted o_p.

Let H be a (finite or infinite) Galois extension of F; its Galois group will be denoted G(H/F). If it is finite, the degree of the extension will be denoted by [H:F] and the norm map by $N_{H/K}$. For any finite abelian extension H/K of conductor $\mathfrak{f}$, and any ideal a of K prime to $\mathfrak{f}$, let $[a,H/K]$ be the element of G(H/K) corresponding to a under the Artin reciprocity map: when the extension H/K is unambiguous, this will be more briefly denoted σ_a, and if a is principal with generator a, also by σ_a. If H is

Notation

Let $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ denote respectively the rational integers, the real field, and the complex field. The letter p will be reserved for rational primes, $\mathbb{Z}_p$ and $\mathbb{Q}_p$ will denote the p-adic integers and the p-adic field.

Throughout, K will denote an imaginary quadratic field, with ring of integers o, the letters $a,b,\ldots,\mathfrak{f},g,h\ldots$ will denote ideals of o; p and q will be reserved for prime ideals of K. In chapter one, the notation o_c will be used for an order in K with conductor c; the letters $a,b,\ldots,\mathfrak{f},g,\ldots$ will also be used to denote ideals of o_c.

Throughout $p(z)$ will denote the Weierstrass p-function; since the variable z will usually be included, no confusion should arise with the prime ideal p.

The group of roots of unity in a field F will be denoted μ_F, and its order, if finite, by e_F. If $\mathfrak{P}$ is a prime of F, let $F_{\mathfrak{P}}$ be the completion of F at $\mathfrak{P}$; in this case $\mathfrak{P}$ will also be used for the maximal ideal lying in the ring of integers of $F_{\mathfrak{P}}$. In particular, K_p denotes the completion of K at p; its ring of integers will be denoted o_p.

Let H be a (finite or infinite) Galois extension of F; its Galois group will be denoted G(H/F). If it is finite, the degree of the extension will be denoted by [H:F] and the norm map by $N_{H/K}$. For any finite abelian extension H/K of conductor $\mathfrak{f}$, and any ideal a of K prime to $\mathfrak{f}$, let $[a,H/K]$ be the element of G(H/K) corresponding to a under the Artin reciprocity map: when the extension H/K is unambiguous, this will be more briefly denoted σ_a, and if a is principal with generator a, also by σ_a. If H is

the maximal abelian extension of K, and x is an idèle of K, let [x,K] denote the element of G(H/K) associated to x by global class field theory.

The letter E will always denote an elliptic curve; if it is defined over a field F, let E(F) be the F-rational points on E.

The units of a commutative ring R with identity will be denoted $R^\times$, and in particular, $F^\times$ for the nonzero elements of the field F, $o_c^\times$ for the units of the order o_c, and $(o_c/a)^\times$ for the units of the quotient ring of o_c by an o_c-ideal a. For any o-ideal a, let $\phi(a)$ be the order of $(o/a)^\times$. The order of any finite group G will be denoted $|G|$.

Chapter 1. Elliptic Units.

This chapter presents the definition of the elliptic units for arbitrary abelian extensions of an imaginary quadratic ground field K. The first two sections review the concept of an order o of a lattice L and explain how to construct the abelian extensions of the imaginary quadratic field K in which o lies i.e. global class field theory for K is made explicit. In §3, the function, Θ, from which the elliptic units arise, is defined; its values at division points of L are shown to be in appropriate abelian extensions of K. The prime factorization of these values is obtained in §4. The method is quite different from Robert's [18] which relies upon earlier work of Ramachandra [17] and Siegel [24] using classical results about the discriminant function and theta functions associated to L. Here we use intrinsic properties of the elliptic curve E attached to L. We choose an elliptic curve isomorphic to E having certain good reduction properties; by considering an appropriate prime $\mathfrak{P}$ and the kernel of the reduction map mod $\mathfrak{P}$ (which is a formal group), we obtain the $\mathfrak{P}$-adic values of the Θ-function values. This allows us to define, in §5, the elliptic units for an arbitrary abelian extension of K with respect to the order o.

Two groups of elliptic units are defined (the larger being called the full group of elliptic units); their relationship to Robert's elliptic units - which are defined only for the maximal order of K - is discussed. The larger group's definition is motivated by Sinnott's definition of the circular units of cyclotomic fields ([25]); his method of computing their index, when modified suitably, applies to this last group.

The values of the θ-function at division points play an analogous role to that of the numbers $1-\exp(2\pi in/m)$ $(n = 1,\ldots,m-1)$ in the field of m^{th} roots of unity. Their prime factorization is similar (see lemma 1.12), and they provide generators for the ramified primes of the appropriate abelian extension (see lemmas 1.12 and 1.15).

§1. Elliptic curves with complex multiplication.

Let L be a lattice in the complex plane $\mathbb{C}$, that is, a subgroup of $\mathbb{C}$ which is free of rank 2 over the rational integers $\mathbb{Z}$, and which generates $\mathbb{C}$ over the real numbers. Let $p(z,L)$ be the associated Weierstrass p-function: it satisfies the differential equation

$$p'(z)^2 = 4p(z)^3 - g_2 p(z) - g_3,$$

where $g_2 = g_2(L) = \sum_{\omega \neq o} \omega^{-4}$ and $g_3 = g_3(L) = \sum_{\omega \neq o} \omega^{-6}$, the sums being taken over all nonzero points ω of L. It is well known that the discriminant of L, $\Delta(L)$, which is equal to $g_2^3 - 27g_3^2$, is nonzero, so that the equation

$$y^2 = 4x^3 - g_2 x - g_3$$

defines a nonsingular curve E (over $\mathbb{Q}(g_2,g_3)$) with points (x,y): E is an elliptic curve.

The group $E(\mathbb{C})$ of $\mathbb{C}$-rational points on E is isomorphic to the quotient group $\mathbb{C}/L$ under the correspondence

$$z \bmod L \longmapsto \xi(z) = (p(z),p'(z)).$$

Every endomorphism of E corresponds to a complex analytic homomorphism of $\mathbb{C}/L$ into itself, and vice versa. Any such homomorphism is induced by the linear map of $\mathbb{C}$

$$z \longmapsto az$$

with a complex number a which maps L into itself: $aL \subset L$. The endomorphism corresponding to such an element a is the mapping

which sends $\xi(z)$ to $\xi(az)$:

$$\xi(z) \longmapsto \xi(az).$$

The set $A = \{a \in \mathbb{C} \mid aL \subset L\}$ is called the order associated with L. Clearly A contains $\mathbb{Z}$; we say that E has complex multiplication if A is strictly larger than $\mathbb{Z}$. Throughout this thesis we will deal exclusively with elliptic curves E which have complex multiplication.

Assuming this, let $[\omega_1,\omega_2]$ be a basis for L: $L = \mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2$. Then it is easy to show (see [23] section 4.4) that $K = \mathbb{Q}(\omega_1/\omega_2)$ is an imaginary quadratic field (independent of choice of basis) and that the order of L is an order in K, that is, a subring of K which contains $\mathbb{Z}$, and is a free $\mathbb{Z}$ -module of rank 2. Further, for any such order A, there exists a unique positive rational integer c such that $A = \mathbb{Z} + c\mathcal{O}$, where $\mathcal{O}$ is the ring of integers of K. This integer is called the conductor of A, and henceforth A will be denoted by $\mathcal{O}_c$. Note that $\mathcal{O}_1 = \mathcal{O}$ is the maximal order of K.

By a proper fractional ideal of $\mathcal{O}_c$, we shall mean a free $\mathbb{Z}$ -submodule $\mathfrak{a}$ in K of rank 2, with order $\mathcal{O}_c$ ($\mathfrak{a}$ is a lattice in $\mathbb{C}$); in the case that $\mathfrak{a}$ is contained in $\mathcal{O}_c$, we shall refer to $\mathfrak{a}$ more simply as a proper $\mathcal{O}_c$-ideal. The properties of orders and proper fractional ideals are outlined in [23] section 4.4 and [14] chapter 8: the following facts are pertinent to this chapter.

First, the product of two proper fractional ideals $\mathfrak{a}$ and $\mathfrak{b}$ is defined to be the $\mathbb{Z}$ -module generated by the elements xy with $x \in \mathfrak{a}$ and $y \in \mathfrak{b}$. With this multiplication, the set of all proper

fractional $\mathcal{O}_c$-ideals forms a group: the inverse of a member a of this group will be denoted a^{-1}.

Secondly, an ideal a of $\mathcal{O}_c$ prime to c is a proper $\mathcal{O}_c$-ideal. (a is prime to c precisely if the ideal of $\mathcal{O}_c$ generated by a and c is equal to $\mathcal{O}_c$). In this case, a is equal to the intersection with $\mathcal{O}_c$ of an ideal in $\mathcal{O}_1 (= \mathcal{O})$ which is prime to c. In particular, if p is a prime ideal of K, not dividing c, then $p \cap \mathcal{O}_c$ is a prime ideal of $\mathcal{O}_c$.

Lastly, there exists a nonzero complex number Ω such that $\Omega^{-1}L = d$ is a proper $\mathcal{O}_c$-ideal. (For $\omega_2^{-1} L$ is a proper fractional $\mathcal{O}_c$-ideal).

For any $\mathcal{O}_c$-ideal g, let E_g be the group of g- division points on E, that is, $E_g = \{\xi(u) \mid au \in L \text{ for all } a \in g\}$. An element $\xi(u)$ of E_g is primitive if u is a primitive g-division point of L, in which case the set $\{a \in K \mid au \in L\}$ is precisely equal to g.

§2. Class Field Theory.

This section outlines the class field theory for the imaginary quadratic field K introduced in the last section: recall that the endomorphism ring of the elliptic curve E attached to the lattice L is an order $\mathcal{O}_c$ in K. Of course given such a field K and an order

A in K, such a curve exists - it suffices to take for a lattice the order itself, and construct the curve E as in section 1. The precise field of definition for E, $\mathbb{Q}(g_2(L), g_3(L))$, is of some interest - more will be said later about this.

To begin, it is necessary to define the multiplication by an idèle of K of two objects: a proper fractional o_c-ideal, and a division point of L. Let $\mathbb{Q}_A$ and K_A denote the adèle group of $\mathbb{Q}$ and K respectively, and $\mathbb{Q}_A^\times$, $K_A^\times$ denote the corresponding (multiplicative) idèle groups. Then $K_A = K \otimes_{\mathbb{Q}} \mathbb{Q}_A$ as a tensor product. For each rational prime p, let $K_p = K \otimes_{\mathbb{Q}} \mathbb{Q}_p$; given an adèle s of K, there corresponds the p-component s_p lying in K_p. Identifying K_p with its image under the canonical injection of K_p into K_A, K_A itself is a subgroup of the (unrestricted) direct product $K_\infty \prod_p K_p$, where K_∞ is the subgroup of K_A corresponding to the archimedean valuation of K. (In fact K_∞ is isomorphic to $\mathbb{C}$).

Now suppose a is a proper fractional ideal of o_c, and s belongs to $K_A^\times$. For each rational prime p, let $a_p = a \otimes_{\mathbb{Z}} \mathbb{Z}_p$. Then a_p is a $\mathbb{Z}_p$-lattice in K_p, that is, a free $\mathbb{Z}_p$-module in K_p of rank 2. Also there is a $\mathbb{Z}$-lattice b in K such that $b_p = b \otimes_{\mathbb{Z}} \mathbb{Z}_p = s_p a_p$ for every p. This $\mathbb{Z}$-lattice b is a proper fractional σ_c-ideal and is defined to be the product of s and a. This multiplication induces an isomorphism between K/a and $K/s.a$, as follows. K/a is canonically isomorphic to the direct sum of the groups K_p/a_p over all p. Multiplication by s_p induces an isomorphism between K_p/a_p and $K_p/s_p a_p$, and combining these isomorphisms for each p gives the required isomorphism. The situation is summarized by the following commutative diagram

$$\begin{array}{ccc} K_p/a_p & \xrightarrow{s_p} & K_p/s_p a_p \\ \downarrow & & \downarrow \\ K/a & \longrightarrow & K/sa \end{array}$$

(the vertical maps are canonical injections).

Consider now a division point u of a, that is, an element of K/a. The product of s and u (denoted s.u) is defined to be the division point v of s.a such that

$$v \equiv s_p u \text{ modulo } s_p a_p$$

for every rational prime p.

When the order of L is the full ring of integers of K, the foregoing definitions simplify. K/a is canonically isomorphic to the direct sum of the modules K_p/a_p for all primes p of K, where K_p denotes the completion of K at p, and a_p the ideal generated by a in the ring of integers o_p of K_p. Corresponding to each prime p of K, there is a component s_p of the idèle s, and there is a fractional ideal b of K such that $b_p = s_p o_p$ for all p. Then s.a = b.a and the isomorphism $K/a \to K/s.a$ may be defined by the commutative diagram

$$\begin{array}{ccc} K_p/a_p & \longrightarrow & K_p/s_p a_p \\ \downarrow & & \downarrow \\ K/a & \longrightarrow & K/s.a. \end{array}$$

The following lemma, which establishes explicitly the connection between abelian extensions of K and subgroups of the idèle group $K_A^\times$, is proved on p122 of [23]. Recall that $L = \Omega d$, and d is a proper o_c-ideal; let j(L) and $\tau(z,L)$ respectively denote the usual modular invariant and the Weber function of L.

Lemma 1.1 Let u be a division point of d and $W = \{s \in K_A^\times | s.d = d, s.u = u\}$. Then $K^\times W$ is a subgroup of $K_A^\times$ containing $K^\times K_\infty^\times$, and it corresponds via the Artin reciprocity map to the abelian extension $K(j(L), \tau(\Omega u, L))$ of K.

($K_\infty^\times$ is the idèle subgroup whose elements have component 1 at all finite places).

If u is a primitive g-division point of d (g a proper σ_c-ideal), let $W(g)$ denote the idèle subgroup

$$\{s \in K_A^\times | s.d = d, s.u = u\}.$$

Clearly $W(g)$ depends merely on g and not on a particular choice of u. We explicitly calculate $W(g)$ in the next lemma. For each rational prime p, let $U_p(g)$ denote the invertible elements of $o_{c,p} = o_c \otimes_{\mathbb{Z}} \mathbb{Z}_p$ when p and g are coprime; when p and g are not coprime, let $U_p(g)$ denote the invertible elements of $(1+g) \otimes_{\mathbb{Z}} \mathbb{Z}_p$. Here $1+g$ denotes the multiplicative subset of elements of o_c congruent to 1 modulo g. $U_p(g)$ canonically injects into $K_A^\times$.

Lemma 1.2 $$W(g) = K_\infty^\times \prod_p U_p(g),$$

the product being taken over all rational primes p.

Proof. Fix a rational prime p, and let $S = \{\lambda \in K_p | \lambda d_p = d_p\}$. Since d is a proper o_c-ideal, there exists an idèle s such that $d = s.o_c$ (see p122 of [23]). Hence $S = \{\lambda \in K_p | \lambda o_{c,p} = o_{c,p}\}$. Since 1 belongs to $o_{c,p}$ ($\mathbb{Z}_p$ injects into $o_{c,p}$), it follows that $S = o_{c,p}^\times$. Also let

$$T = \{\lambda \in K_p | \lambda u \in g_p\},$$

where u is a primitive g-division point of d, regarded now as

an element of $K_p | d_p$. Clearly

$$T \supseteq \mathfrak{g} \otimes_{\mathbb{Z}} \mathbb{Z}_p = \mathfrak{g}_p .$$

On the other hand, given $\lambda \in T$, there exists an element μ of K such that

$$(\mu \otimes 1) - \lambda \in \mathfrak{g}_p$$

and $$\mu \otimes 1 \in \mathfrak{g} \otimes_{\mathbb{Z}} \mathbb{Z}_q$$

for all rational primes $q \neq p$. (For $K^\times$ is dense in the finite part of $K_A^\times$ via the diagonal embedding.)

Hence $(\mu \otimes 1)u \in d_q$ for all rational primes q, including p; consequently $\mu \in \mathfrak{g}$ and $\lambda \in \mathfrak{g}_p$, so that $T = \mathfrak{g}_p$. Thus the set

$$\{\lambda \in K_p | \lambda d_p = d_p \text{ and } \lambda u = u \bmod \mathfrak{g}_p\}$$

is equal to $U_p(\mathfrak{g})$.

The lemma is now completely proved.

Henceforth the unique abelian extension associated with the subgroup $K_\infty^\times W(\mathfrak{g})$ of $K_A^\times$ will be denoted by $R(\mathfrak{g})$.

Remark. If the rational prime p does not divide c, $o_{c,p} = o_{1,p}$. Hence if p is an arbitrary prime of K, prime to c and to $\mathfrak{g}o$ (the ideal generated by $\mathfrak{g}$ in o_1), then p is unramified in $R(\mathfrak{g})$: for in this case, supposing that p lies above the rational prime p, $U_p(\mathfrak{g})$ contains the p-adic units of the completion of K at p. In particular, $R(o_c)$ is unramified at all primes of K not dividing c.

Shimura's treatment of complex multiplication enables us to determine the action of the idèle group on the j-invariant and on

division points of E. For any idèle s of K, let s.L denote the lattice $\Omega(s.d)$; if ρ is a division point of L, so that $\Omega^{-1}\rho$ is a division point of d, let $s.\rho$ denote the division point $\Omega(s.\Omega^{-1}\rho)$ of L.

Lemma 1.3. Let $[s,K]$ denote the element of the Galois group for the maximal abelian extension of K over K, which corresponds to the idèle s under the Artin map.

(1) $j(L) \in R(o_c)$, and $j(L)^{[s,K]} = j(s^{-1}L)$.

(2) Let g be an o_c-ideal, and ρ a g-division point of L. Then $\tau(\rho,L) \in R(g)$. Moreover, $s^{-1}\rho$ is a g-division point of $s^{-1}L$, and

$$\tau(\rho,L)^{[s,K]} = \tau(s^{-1}\rho,\ s^{-1}L).$$

Proof. The first part is proved in [23] p122. As for the second part, lemma 1.1 shows that $\tau(\rho,L) \in R(g)$. Let σ be an automorphism of the complex numbers whose restriction to the maximal abelian extension of K equals $[s,K]$. There is an isomorphism

$$\eta : \mathbb{C}/d \longrightarrow E(\mathbb{C})$$

given by $\eta(z \bmod d) = \xi(\Omega z, L)$.

Let E^σ denote the elliptic curve with invariants g_2^σ, g_3^σ. By theorem 5.4 of [23] there is an isomorphism $\eta^* : \mathbb{C}/s^{-1}d \longrightarrow E^\sigma(\mathbb{C})$ with $\eta(z)^\sigma = \eta^*(s^{-1}z)$ for all $z \in K|d$. In particular, the period lattice of E^σ is of the form $\mu s^{-1} d$ for some nonzero complex μ, and thus

$$g_2^\sigma(L) = g_2(\varepsilon s^{-1}L),$$

$$g_3^\sigma(L) = g_3^\sigma(\varepsilon s^{-1}L)$$

where $\varepsilon = \mu/\Omega$. Now there exists an isomorphism

$$\phi : \mathbb{C}/s^{-1}d \longrightarrow E^{\sigma}(\mathbb{C})$$

given by $\phi(z \bmod s^{-1}d) = \xi(\mu z, \mu s^{-1}d)$. Thus $\eta^* \circ \phi^{-1}$ is an automorphism of E^{σ}, and so there is a root of unity ζ in o_c such that

$$\eta^*(z) = \xi(\zeta\mu z, \mu s^{-1}b).$$

Now let $z = s^{-1}\rho/\Omega$. Then

$$\eta^*(z) = \eta(\rho/\Omega)^{\sigma} = \xi(\rho,L)^{\sigma} = \xi(\zeta\varepsilon s^{-1}\rho, \varepsilon s^{-1}L).$$

Hence $\tau(\rho,L)^{\sigma} = \tau(\zeta\varepsilon s^{-1}\rho, \varepsilon s^{-1}L)$

$$= \tau(\zeta s^{-1}\rho, s^{-1}L)$$

$$= \tau(s^{-1}\rho, s^{-1}L),$$

upon noting that $\tau(\alpha\rho,\alpha L) = \tau(\rho,L)$ for any nonzero complex α. This concludes the proof of the lemma.

Lemma 1.2 can now be used to find canonical sets of representatives for the Galois groups of the extensions $R(\mathfrak{g})$.

Lemma 1.4 (1) $G(R(o_c)/K)$ is isomorphic to the group of the classes of proper o_c-ideals modulo principal o_c-ideals.

(2) Let $\mathfrak{g}$ be a proper o_c-ideal. Let W denote the image of $o_c^{\times}$ in $(o_c/\mathfrak{g})^{\times}$ under the natural map of reduction modulo $\mathfrak{g}$. (In most cases, W is isomorphic to $o_c^{\times}$: for example, if $\mathfrak{g}$ is prime to 6). Then $G(R(\mathfrak{g})/R(o_c))$ is isomorphic to $(o_c/\mathfrak{g})^{\times}/W$.

(3) Let $B_{\mathfrak{g}}$ be a complete set of representatives in o_c for the cosets of $(o_c/\mathfrak{g})^{\times}/W$, and let ρ be a primitive $\mathfrak{g}$-division point of L. The conjugates of $\tau(\rho,L)$ over $R(o_c)$ are the (distinct) elements $\tau(a\rho,L)$, for all a belonging to $B_{\mathfrak{g}}$.

Proof. The first is proved in [23], p123. As for the second part, lemma 1.2 shows

$$G(R(\mathfrak{g})/R(\mathfrak{o}_c)) \xrightarrow{\sim} K^\times W(\mathfrak{o}_c)/K^\times W(\mathfrak{g}).$$

There is an isomorphism between $W(\mathfrak{o}_c)/W(\mathfrak{g})$ and $(\mathfrak{o}_c/\mathfrak{g})^\times$ as follows. Let u be a primitive $\mathfrak{g}$-division point of L. For each $s \in W(\mathfrak{o}_c)$, s.u is also a primitive $\mathfrak{g}$-division point, because sL = L. Hence there exists an element a_s of $\mathfrak{o}_c$ such that $s.u = a_s.u$. This number a_s is well defined modulo $\mathfrak{g}$, and since u is primitive, it is a unit modulo $\mathfrak{g}$. The map $W(\mathfrak{o}_c) \longrightarrow (\mathfrak{o}_c/\mathfrak{g})^\times$ is a surjective homomorphism with kernel $W(\mathfrak{g})$. Further if $s \in W(\mathfrak{o}_c)$, then $s \in K^\times W(\mathfrak{g})$ precisely if $s = \zeta s_1$ for some root of unity $\zeta \in \mathfrak{o}_c^\times$ and some $s_1 \in W(\mathfrak{g})$. Thus $K^\times W(\mathfrak{o}_c)/K^\times W(\mathfrak{g}) \simeq (\mathfrak{o}_c/\mathfrak{g})^\times/W$, and the second part of the lemma is proved. The third part follows immediately from the preceding lemma.

In later work, we will assume for simplicity that $\mathfrak{g}$ is coprime to 6, so that $\mathfrak{o}_c^\times$ may be identified with W. In this case, let $B_{\mathfrak{g}}$ be a complete set of representatives in $\mathfrak{o}_c$ for the cosets of $(\mathfrak{o}_c/\mathfrak{g})^\times/W$; let u be a primitive $\mathfrak{g}$-division point. Define the polynomial

$$T(x, \mathfrak{g}, L) = \prod_{a \in B_{\mathfrak{g}}} (x - \tau(au, L))$$

if $\mathfrak{g} \neq \mathfrak{o}_c$, and to be the constant 1 if $\mathfrak{g} = \mathfrak{o}_c$. By lemmas 3 and 4, if $\mathfrak{g} \neq \mathfrak{o}_c$,

$$T(x, \mathfrak{g}, L) = \prod_{\sigma} (x - \tau(u, L)^\sigma)$$

where the product is taken over all elements σ of $G(R(\mathfrak{g})/R(\mathfrak{o}_c))$. Hence $T(x, \mathfrak{g}, L)$ is independent of the choice of u, and a polynomial with coefficients in $R(\mathfrak{o}_c)$.

§3. The Θ-function.

In this section we define the function $\Theta(z,\mathfrak{a},L)$: it depends upon a complex variable z and an o_c-ideal $\mathfrak{a}$. It is an elliptic function on L, and its values at $\mathfrak{f}$-division points of L lie inside $R(\mathfrak{f})$, provided $\mathfrak{a}$ is prime to $6\mathfrak{f}c$. These values will be calculated in the next section, and used in the following section to define the elliptic units for $R(\mathfrak{f})$.

Let $\sigma(z,L) = z \prod_{\substack{\omega\in L\\ \omega\neq o}} (1-z/\omega)\exp(z/\omega+z^2/2\omega^2)$ be the Weirstrass σ-function of L. The function

$$\sum_{\substack{\omega\in L\\ \omega\neq o}} \frac{1}{\omega^2|\omega|^{2s}}$$

is holomorphic at s = 0 (see [13]); let $s_2(L)$ be its value at s = 0. Define the functions

$$\psi(z,L) = \exp(-s_2(L)z^2/2)\sigma(z,L)$$

and $$\theta(z,L) = \Delta(L)\psi(z,L)^{12} .$$

Let $\mathfrak{a}$ be a o_c-ideal prime to 6c. Then $\mathfrak{a}$ is proper: there exists an o-ideal, which will be denoted $\mathfrak{a}_K$, such that $\mathfrak{a}_K \cap o_c = \mathfrak{a}$. Define $N\mathfrak{a}$ to be the number of elements of $o_c/\mathfrak{a}$. Since $o_c/\mathfrak{a} \simeq o_c/\mathfrak{a}_K \cap o_c \simeq (o_c+\mathfrak{a}_K)/\mathfrak{a}_K$ as abelian groups, and because $o_c+\mathfrak{a}_K$ contain the o-module $co+\mathfrak{a}_K = o$, we conclude that $o_c/\mathfrak{a} \simeq o/\mathfrak{a}_K$. Thus $N\mathfrak{a}$ equals the usual norm of the o-ideal $\mathfrak{a}_K$. For such an o_c-ideal $\mathfrak{a}$, define the functions

$$\Psi(z,\mathfrak{a},L) = \psi(z,L)^{N\mathfrak{a}}/\psi(z,\mathfrak{a}^{-1}L)$$

and $$\Theta(z,\mathfrak{a},L) = \theta(z,L)^{N\mathfrak{a}}/\theta(z,\mathfrak{a}^{-1}L) = \frac{\Delta(L)^{N\mathfrak{a}}}{\Delta(\mathfrak{a}^{-1}L)}\Psi(z,\mathfrak{a},L)^{12}.$$

Here $\mathfrak{a}^{-1}L$ denotes the lattice $\Omega(\mathfrak{a}^{-1}\mathfrak{d})$. Explicit expressions for the functions in terms of the elliptic functions $p(z,L)$ and $\tau(z,L)$ are given in the next lemma.

Lemma 1.5. $\Theta(z,\mathfrak{a},L)$ and $\Psi(z,\mathfrak{a},L)$ are elliptic functions for the lattice L, for which the following formulae hold.

(1) Let S be a complete set of inequivalent representatives of $\mathfrak{a}^{-1}L$ modulo L, excluding that of L, and let S' be a subset of $\frac{1}{2}(N\mathfrak{a}-1)$ elements of S such that

$$\{\ell, -\ell;\ \ell\in S'\}$$

is a complete set of inequivalent representatives of $\mathfrak{a}^{-1}L$ modulo L, excluding that of L.

Then $$\Psi(z,\mathfrak{a},L) = \prod_{\ell\in S'} (p(z)-p(\ell))^{-1}$$

and $$\Theta(z,\mathfrak{a},L) = \frac{\Delta(L)^{N\mathfrak{a}}}{\Delta(\mathfrak{a}^{-1}L)} \prod_{\ell\in S} (p(z)-p(\ell))^{-6} .$$

(2) Define P(x) to be the polynomial $x^2(x-1728)^3/2^{30}3^{24}$ if o_c^* has two elements, otherwise to be the constants 1 or -27 according as o_c^* has four or six elements.

Then $$\Theta(z,\mathfrak{a},\ L) = \frac{\Delta(L)}{\Delta(\mathfrak{a}^{-1}L)} \cdot P(j(L))^{N\mathfrak{a}-1} \cdot \prod_{g\supseteq\mathfrak{a}} T(\tau(z,L),g,L)^{-12}$$

where the product is taken over all o_c-ideals g containing $\mathfrak{a}$. (The polynomial $T(x,g,L)$ was defined in the previous section).

Proof. Let ω be a period of L, and let $\varepsilon = 1$, or -1, according as $\omega/2$ does, or does not, lie in L. Then

$$\sigma(z+\omega,L) = \varepsilon\sigma(z,L)\ \exp(\eta(\omega)(z+\omega/2)),$$

where $\eta(\omega)$ is the Weirstrass η-function (see [14] p241).

Thus $\psi(z+\omega,L)/\psi(z,L) = \varepsilon.\exp((z+\omega/2)(\eta(\omega)-\omega s_2(L)))$.

Let a(L) denote the area of the fundamental parallelogram of L. Then (see [13] appendix),

$$\eta(\omega) - \omega s_2(L) = \pi\bar{\omega}/a(L).$$

Upon noting that $a(\alpha^{-1}L) = a(L)/N\alpha$, and that $N\alpha-1$ is even, we see

$$\Psi(z+\omega,\alpha,L) = \varepsilon^{N\alpha-1}\Psi(z,\alpha,L) = \Psi(z,\alpha,L);$$

hence Ψ is periodic on L, and so is Θ.

To prove the first formula for Ψ, we first note that the right and left hand sides are elliptic functions for L. We show they have the same zeros and poles.

The poles of $\Psi(z,\alpha,L)$ are simple and occur at the elements of $\alpha^{-1}L$ which do not lie in L. The zeros of $\Psi(z,\alpha,L)$ occur, with multiplicity $(N\alpha-1)$, at the elements of L. On the other hand, the zeros of $p(z)-p(\ell)$ occur at the points $z \equiv \ell$ and $z \equiv -\ell$ modulo L, (where $\ell \in S$) and are simple. ($\ell \not\equiv -\ell$ modulo L because α is prime to 6). The poles of $p(z)-p(\ell)$ are double poles and occur at the points of L. Since the functions

$$\Psi(z,\alpha,L) \text{ and } \prod_{\ell \in S'} (p(z)-p(\ell))^{-1}$$

have the same zeros and poles, their ratio is a constant C, which may be evaluated by letting $z \longrightarrow 0$. Since

$$\Psi(z,\alpha,L)/z^{N\alpha-1} \longrightarrow 1$$

and $z^2 p(z) \longrightarrow 1$ as $z \longrightarrow 0$, we obtain C = 1. This proves the first formula for Ψ. The first formula for Θ immediately follows

upon noting that for any $\ell \in S'$, $p(-\ell) = p(\ell)$.

The second formula for Θ is easily derived from the first. First note that if ζ is a root of unity in o_c, then $p(\zeta z) = \zeta^{-2} p(z)$, so given $\ell \in S$,

$$\prod_{\zeta \in o_c}{}_{*} (p(z)-p(\zeta\ell)) = (p^t(z)-p^t(\ell))^2$$

where $2t$ is the number of roots of unity in o_c. Let g be any o_c-ideal containing a (so that g is prime to $6c$, and is proper), and let ℓ vary over all elements of S which are primitive g-division points of L; let $\mu(g)$ be the number of these primitive division points. Then by the definition of $T(x,g,L)$,

$$\prod_{\ell} (p(z)-p(\ell))^{-6} = C_1^{\mu(g)} T(\tau(z,L),g,L)^{-12}$$

where $C_1 = (\Delta(L)/g_2(L)g_3(L))^6$, or $(\Delta(L)/g_2^2(L))^3$, or $(\Delta(L)/g_3(L))^2$ according as $t = 1$, 2 or 3.

Thus $$\Theta(z,a,L) = C_1^{(Na-1)} \prod_{g \supseteq a} T(\tau(z,L),g,L)^{-12} \cdot \left(\frac{\Delta(L)^{Na}}{\Delta(a^{-1}L)}\right)$$

since $$\sum_{g \supseteq a} \mu(g) = Na-1.$$

Since $j(L) = \dfrac{1728\, g_2^3}{\Delta}$, and $\Delta = g_2^3 - 27g_3^2$ (with $g_3 = 0$ if $t = 2$, $g_2 = 0$ if $t = 3$), we obtain

$$C_1 = P(j(L))\Delta(L)^{-1},$$

and the second formula immediately follows.

The formulae derived above immediately imply the following results.

Lemma 1.6. Let ρ be a $\mathfrak{f}$-division point of L. Then for all $\mathcal{O}_c$-ideals $\mathfrak{a}$ which are prime to $6c\mathfrak{f}$, $\Theta(\rho,\mathfrak{a},L)$ belongs to $R(\mathfrak{f})$. Further, if s is an idele of K,

$$\Theta(\rho,\mathfrak{a},L)^{[s,K]} = \Theta(s^{-1}\rho,\mathfrak{a},s^{-1}L).$$

Proof. By the classical theory of complex multiplication, both $j(L)$ and $\frac{\Delta(L)}{\Delta(\mathfrak{a}^{-1}L)}$ belong to $R(\mathcal{O}_c) = R(j(\mathcal{O}_c))$. The second formula for Θ in the previous lemma makes it obvious that $\Theta(\rho,\mathfrak{a},L)\in R(\mathfrak{f})$. Since

$$\left(\frac{\Delta(L)}{\Delta(\mathfrak{a}^{-1}L)}\right)^{[s,K]} = \frac{\Delta(s^{-1}L)}{\Delta(\mathfrak{a}^{-1}s^{-1}L)},$$

(see [14], p159), we conclude, using lemma 1.3 that,

$$\Theta(\rho,\mathfrak{a},L)^{[s,K]} = \Theta(s^{-1}\rho,\mathfrak{a},s^{-1}L).$$

Corollary. Let ρ vary over a complete set S of inequivalent primitive $\mathfrak{f}$-division points of L, which are distinct up to a factor of a root of unity in $\mathcal{O}_c$ (i.e. if ρ is in S, the $\zeta\rho$ is not in S for every root of unity ζ in $\mathcal{O}_c$, other than 1). Then $\{\Theta(\rho,\mathfrak{a},L);\ \rho\in S\}$ is a complete set of conjugates over $R(\mathcal{O}_c)$.

The following result - under the restriction that $(\mathfrak{f},6c) = 1$ - will be used in §5 to compute norms of the values $\Theta(\rho,\mathfrak{a},L)$.

Lemma 1.7. Let $\mathfrak{f}$ and $\mathfrak{a}$ be $\mathcal{O}_c$-ideals, prime to 6c and to each other. Then for all $z\in C$,

$$\prod_{\rho} \Theta(z+\rho,\mathfrak{a},L) = \Theta(z,\mathfrak{a},\mathfrak{f}^{-1}L)$$

where the product is taken over a complete set of inequivalent representatives of $\mathfrak{f}^{-1}L$ modulo L. In particular,

$$\prod_{\rho\neq o} \Theta(\rho,\alpha,L) = \left(\frac{\Delta(\beta^{-1}L)}{\Delta(L)}\right)^{N\alpha} \cdot \left(\frac{\Delta(\alpha^{-1}L)}{\Delta(\alpha^{-1}\beta^{-1}L)}\right) .$$

Proof. We begin by proving a similar result for $\Psi(z,\alpha,L)$ and derive the lemma from this. The function

$$f(z) = \prod_{\rho} \Psi(z+\rho,\alpha,L)$$

is an elliptic function for the lattice L, whose poles and zeros (counting multiplicities) are identical to those for the function $\Psi(z,\alpha,\beta^{-1}L)$. Thus, there is a constant $C = C(\beta,\alpha,L)$ (depending on β, α, and L) such that $f(z) = C.\Psi(z,\alpha,\beta^{-1}L)$. The constant may be evaluated by considering limits as $z \longrightarrow 0$.

Since $$\lim_{z\to o} \frac{\Psi(z,\alpha,L)}{\Psi(z,\alpha,\beta^{-1}L)} = 1$$

$$C = \prod_{\rho\neq o} \Psi(\rho,\alpha,L) .$$

This constant will be computed by considering the value of $C(2\beta,\alpha,L)$ in two different ways. On the one hand,

$$C(2\beta,\alpha,L) = \prod_{\zeta,\eta}{}' \Psi(\eta+\zeta,\alpha,L)$$

where η and ζ vary over a complete set of representatives for the cosets of $\beta^{-1}L$ modulo L and $(2\beta)^{-1}L$ modulo $\beta^{-1}L$ respectively, subject to the condition that not both ζ and η lie in the zero cosets. Thus

$$C(2\beta,\alpha,L) = \prod_{\eta\neq o} \Psi(\eta,\alpha,L) \prod_{\zeta\neq o} C(\beta,\alpha,L)\Psi(\zeta,\alpha,\beta^{-1}L)$$

$$= C(\beta,\alpha,L)^4 \, C(2,\alpha,\beta^{-1}L) .$$

On the other hand

$$C(2\mathfrak{f},a,L) = \prod_{\zeta',\eta}{}' \Psi(\zeta'+\eta',a,L)$$

where η' and ζ' vary over a complete set of representatives for the cosets of $(2\mathfrak{f})^{-1}L$ modulo $2^{-1}L$, and $2^{-1}L$ modulo L, subject to the condition that not both η' and ζ lie in the zero cosets. Then

$$C(2\mathfrak{f},a,L) = \prod_{\zeta'\neq o}{}' \Psi(\zeta',a,L) \prod_{\eta'\neq o} C(2,a,L)\Psi(\eta',a,2^{-1}L)$$

$$= C(2,a,L)^{N\mathfrak{f}}\, C(\mathfrak{f},a,2^{-1}L).$$

Thus $$\frac{C(\mathfrak{f},a,L)^4}{C(\mathfrak{f},a,2^{-1}L)} = \frac{C(2,a,L)^{N\mathfrak{f}}}{C(2,a,\mathfrak{f}^{-1}L)}.$$

Now $$C(\mathfrak{f},a,2^{-1}L) = 2^{-(Na-1)(N\mathfrak{f}-1)}\, C(\mathfrak{f},a,L)$$

(because $p(z,2^{-1}L) = 4p(2z,L)$, and $a,\mathfrak{f}$ are prime to 6). We now compute $C(2,a,L)$. First suppose that L is normalized with basis of form $[\tau,1]$ with $\mathrm{Im}\,\tau > 0$. Following Lang [14] p250 and 251, we have

$$\Delta(L) = 2^4 \exp\{\eta(1)+(\tau+1)\eta(\tau)\}/\sigma^4(\tfrac{1}{2})\sigma^4(\tfrac{\tau}{2})\sigma^4(\tfrac{1+\tau}{2})$$

where σ and η denote the Weirstrass σ-and η-functions attached to L. Thus

$$\psi^4(\tfrac{1}{2},L)\psi^4(\tfrac{\tau}{2},L)\psi^4(\tfrac{1+\tau}{2},L) = \frac{2^4\exp\{\eta(1)+(\tau+1)\eta(\tau)-(1+\tau+\tau^2).s_2(L)\}}{\Delta(L)}$$

The identities $\eta(1)-s_2(L) = \pi/a(L)$

$$\eta(\tau)-\tau s_2(L) = \pi\bar{\tau}/a(L)$$

proved in [13] (see also Lemma 5) give

$$\psi^4(\tfrac{1}{2},L)\psi^4(\tfrac{\tau}{2},L)\psi^4(\tfrac{1+\tau}{2},L) = 2^4\exp\left(\frac{\pi}{a(L)}(1+\bar{\tau}+\tau\bar{\tau})\right)/\Delta(L).$$

A similar computation for the lattice $a^{-1}L$ shows that

$$\psi^4(\tfrac{1}{2},a^{-1}L)\psi^4(\tfrac{\tau}{2},a^{-1}L)\psi^4(\tfrac{1+\tau}{2},a^{-1}L) = 2^4\exp\left(\frac{\pi}{a(a^{-1}L)}(1+\bar{\tau}+\tau\bar{\tau})\right)/\Delta(a^{-1}L).$$

Notice that $\frac{1}{2}$, $\frac{\tau}{2}$, $\frac{1+\tau}{2}$ are 2-division points for $a^{-1}L$ but not necessarily located in the usual fundamental parallelogram for $a^{-1}L$. The derivation of p250 of [14] is still valid.

Thus for the normalized lattice L and hence for any lattice L

$$C(2,a,L)^4 = 2^{4(Na-1)}\cdot\left(\frac{\Delta(L)^{Na}}{\Delta(a^{-1}L)}\right)^{-1}$$

The same is true for $\beta^{-1}L$: hence, because

$$C(\beta,a,L)^3\cdot 2^{(Na-1)(N\beta-1)} = \frac{C(2,a,L)^{N\beta}}{C(2,a,\beta^{-1}L)},$$

we obtain

$$C(\beta,a,L)^{12} = \left(\frac{\Delta(L)^{Na}}{\Delta(a^{-1}L)}\right)^{-N\beta}\cdot\left(\frac{\Delta(\beta^{-1}L)^{Na}}{\Delta(\beta^{-1}a^{-1}L)}\right).$$

Recalling that

$$\Theta(z,a,L) = \left(\frac{\Delta(L)^{Na}}{\Delta(a^{-1}L)}\right)\cdot\Psi(z,a,L)^{12}$$

we deduce that

$$\prod_{\rho}\Theta(z+\rho,a,L) = \Theta(z,a,\beta^{-1}L).$$

§4. Factorization of values of Θ-functions.

The prime factorization of the numbers $\Theta(\rho,a,L)$ is now considered. The technique depends upon expressing these values in terms of the discriminant and division points of an elliptic curve E', which is isomorphic to E and which has certain good reduction properties described below. The existence of such a curve E' is guaranteed for all but the following "special type" of order - the orders of $\mathbb{Q}(\sqrt{-1})$ and of $\mathbb{Q}(\sqrt{-3})$ whose conductor is a power of a single prime. Henceforth, the order o_c will be assumed to be not of "special type"; in particular, o_c may be the full ring of integers of K.

Throughout, let a and $\mathfrak{b}$ denote o_c-ideals prime to c: they are proper, so let a_K and $\mathfrak{b}_K$ denote the o-ideals such that $a = a_K \cap o_c$ and $\mathfrak{b} = \mathfrak{b}_K \cap o_c$. Furthermore a will be supposed prime to $6\mathfrak{b}$; ρ will denote a fixed $\mathfrak{b}$-division point of L, and for brevity H will denote the field $K(j_E)$.

The principal result of this section (Lemma 1.12) is that $\Theta(\rho,a,L)$ is an integer of $R(\mathfrak{b})$; it is a unit if $\mathfrak{b}_K$ is not a prime power; if $\mathfrak{b}_K$ is a power of a prime p, it is a unit at all places of $R(\mathfrak{b})$ except those above p, and here its value is described.

As mentioned earlier the method of establishing this result is different from Robert's; the main steps in the argument are the following. First, it is noted that E can be taken as defined over $H = K(j_E)$. Next, a prime p of K is fixed, and a curve E', which is isomorphic to E, is defined over H, and has good reduction at all primes of H dividing $\mathfrak{b}_K a_K p$, is found; the exclusion of the special type of order is needed for this step. $\Theta(\rho,a,L)$ is then expressed in terms of the discriminant, the $\mathfrak{b}$-division and the

a-division points on E'. Let $\mathfrak{P}$ be a prime above p in the field of definition of such division points; E' has good reduction at $\mathfrak{P}$, and the $\mathfrak{P}$-adic value of these division points is found by considering the formal group which is the kernel of the reduction map modulo $\mathfrak{P}$. From this the $\mathfrak{P}$-adic value of $\Theta(\rho,a,L)$ quickly follows.

So we begin by considering the field of definition of E, namely $\mathbb{Q}(g_2(L),g_3(L))$. It is not necessarily algebraic (over $\mathbb{Q}$), but since the j-invariant of E, j_E, generates over K the finite algebraic extension $R(\sigma_c)$, there is an elliptic curve E' which is defined over $H = K(j_E)$ and is isomorphic to E over the complex field. It has a Weierstrass model $y^2 = 4x^3-g_2'x-g_3'$ with g_2',g_3' in H (see Shimura [23], p97-98); the isomorphism connecting points (x,y) of E to points (x',y') of E' is given by

$$x' = u^2x,\ y' = u^3y,\ g_2' = u^4g_2,\ g_3' = u^6g_3,$$

for some $u\in\mathbb{C}^*$. The lattice associated to E' is $u^{-1}L$; hence $\tau(u^{-1}z,L') = \tau(z,L)$ and $\Delta(L')/\Delta(a^{-1}L') = \Delta(L)/\Delta(a^{-1}L)$. Thus in considering the value of $\Theta(\rho,a,L)$, we may suppose that E is defined over H, that is, g_2,g_3 and Δ lie in H. We shall use E_1 to denote the model $Y^2 = X^3-G_2X-G_3$ which is related to E by the equations

$$X = x,\ 2Y = y,\ 4G_2 = g_2,\ 4G_3 = g_3.$$

E_1 has discriminant equal to $\Delta(L)$.

Now suppose E' is another curve, which is defined over H and is isomorphic to E_1. Let $f: E' \longrightarrow E_1$ denote the isomorphism carrying the origin of E' to that of E_1; we denote the coordinates

of a point P of E' by (x'(P),y'(P)) and those of the image point f(P) on E_1 by (X(f(P)),Y(f(P))) or more simply (X(P),Y(P)). This isomorphism must be defined over a field extension M/H of degree dividing e_K; there exist constants r,s,u,w in M with $u \neq 0$ such that

$$\begin{aligned} X(P) &= u^2x'(P)+r \\ Y(P) &= u^3y'(P)+su^2x'(P)+w, \end{aligned} \qquad (*)$$

and the discriminant Δ' of E' satisfies $\Delta' = u^{-12}\Delta(L)$ (see [28], p37).

We may write $\Theta(\rho,a,L)$ in terms of the a-division and $\mathfrak{l}$-division points on E'. Let $P_1 = (p(\rho),\frac{1}{2}p'(\rho))$ and $P = f^{-1}(P_1)$ be corresponding $\mathfrak{l}$-division points on E_1 and E'; let $E_{1,a}$ and E'_a denote the corresponding a-division points on these curves ($E'_a = f^{-1}(E_{1,a})$). Then Lemma 1.5 shows that

$$\begin{aligned} \Theta(\rho,a,L) &= \frac{\Delta(L)^{N\mathfrak{a}}}{\Delta(a^{-1}L)} \prod_{Q_1 \in E_{1,a}} (X(P_1)-X(Q_1))^{-6} \\ &= \frac{\Delta(L)}{\Delta(a^{-1}L)} (\Delta')^{N\mathfrak{a}-1} \prod_{Q \in E'_a} (x'(P)-x'(Q))^{-6} \end{aligned} \qquad (1)$$

We emphasize this expression is valid for any such model E', including those for which E' has certain good reduction properties.

For the remainder of this section, let p be a fixed prime of K. Since the special type of order has been excluded, the work of Serre and Tate ([22], theorem 9 and corollary) shows that there exists an H-form for E_1 which has good reduction at all primes of H dividing $a_K\mathfrak{l}_K p$. We will denote this form by E': it is defined over H, it has the same j-invariant as E_1, it is isomorphic to E_1 as described, it has a defining equation

$$y^2+a_1xy+a_3y = x^3+a_2x^2+a_4x+a_6$$

with coefficients a_i which belong to H and are integral at each prime of H dividing $a_K\mathfrak{d}_K p$, and, finally, its discriminant Δ' is a unit at each such prime.

Let $N = K(j_E, E'_{\mathfrak{d}}, E'_a)$ be the extension of H obtained by adjoining the coordinates of the $\mathfrak{d}$-division and a-division points on E'. Fix a prime $\mathfrak{P}_1$ of N lying above p; let $\mathfrak{P} = \mathfrak{P}_1 \cap H$ and $(p) = p \cap \mathbb{Q}$ be the primes of H and $\mathbb{Q}$ above which it lies. To compute the $\mathfrak{P}_1$-adic value of $\Theta(\rho, a, L)$, we consider the one parameter formal group $\hat{E}$ which is the kernel of the reduction map modulo $\mathfrak{P}$ on the curve E' (see [28] p42). Let $t(P) = -x(P)/y(P)$ for each point P on E': t is a local parameter for the point at infinity on the curve; as shown in [28], there are expansions

$$x(t) = t^{-2}a(t), \quad y(t) = -t^{-3}a(t)$$

where a(t) is a power series in t, leading coefficient 1, and the remaining coefficients lie in the ring R of integers of the completion $H_{\mathfrak{P}}$ of H at $\mathfrak{P}$.

Let A be the ring of integers of a finite extension B of H, and m its maximal ideal. We write $\hat{E}(m)$ for the set m endowed with the group law given by $\hat{E}$. The map

$$t \longmapsto (x(t), y(t))$$

defines an isomorphism from $\hat{E}(m)$ onto the kernel of reduction modulo m of the points on E' with coordinates in B. If v denotes the valuation on B (for which the value of a generator of m is +1), the subgroup m^n corresponds to the subgroup $E'_n(B)$ of points (x,y) on E' with

$$v(x) \leq -2n, \quad v(y) \leq -3n$$

(and including the zero of E').

Let $o_{c,p}$ be the completion of o_c in K_p: we show that $\hat{E}$ is an $o_{c,p}$-module, as follows. Let P lie in $E_1'(B)$ and α in $o_{c,p}$. Define the map $[\alpha]$ of $\hat{E}(m)$ by

$$[\alpha]t(P) = t(\alpha P).$$

We claim this is a power series in t with coefficients in R, i.e. integral coefficients, and so is an endomorphism of $\hat{E}$. By m-adic continuity, it suffices to prove this for any dense subset of $o_{c,p}$, in particular for any α in o_c.

If p is an unramified prime of degree 1, it even suffices to prove this when α is a rational integer; this is well known (see [14] p305). The result in general can be derived from a much deeper result of Tate [28]. Since multiplication by p in $\hat{E}$ is an isogeny of degree p^2, $\hat{E}$ is a divisible formal group (see [28] p162). Let

$$T_p(\hat{E}) = \varprojlim E'_{p^n}$$

be the Tate-module, where the inverse limit is taken with respect to the maps $p: E'_{p^{n+1}} \longrightarrow E'_{p^n}$ of multiplication by p. Now the map $[\alpha]$ is an endomorphism of $T_p(E')$ which commutes with the action of $G(\bar{H}_{\mathfrak{P}}/H_{\mathfrak{P}})$ (- here $\bar{H}_{\mathfrak{P}}$ denotes the algebraic closure of $H_{\mathfrak{P}}$ -); for if (P_n) is a sequence in $T_p(E')$, we have $pP_{n+1} = P_n$ and $pP_1 = O$, and (αP_n) is a similar such sequence. Now every endomorphism of $\hat{E}$ clearly gives rise to a $G(\bar{H}_{\mathfrak{P}}/H_{\mathfrak{P}})$ endomorphism of $T_p(E')$; Tate's deep result asserts that every $G(\bar{H}_{\mathfrak{P}}/H_{\mathfrak{P}})$ endomorphism of $T_p(E')$ is induced by an endomorphism of $\hat{E}$ (see corollary 1 of theorem 4.1 in [28]; c.f the examples on p161, and

p170). In particular, $[\alpha]$ is an endomorphism of $\hat{E}$. This proves our claim.

The following lemma is an easy consequence of the preceding discussion. Recall that P is a primitive $\mathfrak{f}$-division point (on E').

Lemma 1.8. Suppose that p does not divide $\mathfrak{f}_K$. Then P is integral at $\mathfrak{P}_1$, and so $|x'(P)|_{\mathfrak{P}_1} \leq 1$.

Proof. Suppose P were not integral at $\mathfrak{P}_1$: then it lies in $E'_{\mathfrak{f}} \cap \hat{E}(\mathfrak{P}_1)$. Choose an element α in $\mathfrak{f}$, but not in p. Since α is invertible in $o_{c,p}$, we have

$$P = [\alpha^{-1}]\,([\alpha]P) = O,$$

a contradiction. Thus P is integral at $\mathfrak{P}_1$, q.e.d.

We now compute the $\mathfrak{P}_1$-adic value of x'(P) when $\mathfrak{f}_K$ is a power of the fixed prime p: say $\mathfrak{f}_K = p^{n+1}$. Note that in this case p does not divide c because $\mathfrak{f}$ is prime to c.

Choose an o_c-ideal d, and an analytic parametrization $\xi'\colon \mathbb{C}/d \longrightarrow E'$. (Indeed, ξ' may be taken to be the composition of the Weierstrass parametrization of §1, and the transformation laws (*) giving good reduction on E'). Let ψ be the Grossen character of the curve E': ψ maps the idèles of H to elements of K* (see [23], p212.).

Because E' has good reduction at $\mathfrak{P}_1$, ψ is unramified at $\mathfrak{P}$. We define $\psi(\mathfrak{P})$ to be the value of ψ at an idèle whose local components except at $\mathfrak{P}$, equal one; the $\mathfrak{P}$-component is taken to be any local parameter for $\mathfrak{P}$ (see [23], theorem 7.42). Further, the reduction of the endomorphism $[\psi(\mathfrak{P})]$ modulo $\mathfrak{P}$ is the Frobenus endomorphism of the reduction of E' modulo $\mathfrak{P}$. If f is the degree

of the residue field of $H_{\mathfrak{P}}$ over the residue field of K_p, p^f is principal, and is generated by $\psi(\mathfrak{P})$. Setting $q = (N_{K/\mathbb{Q}}p)^f$, this means that

$$[\psi(\mathfrak{P})](t) = t^q \bmod \mathfrak{P}.$$

(Note that because p does not divide c, $\psi(\mathfrak{P})$ lies in $o_{c,p} = o_p$).

Let π be a local parameter for p; since p is unramified in H/K, π is a local parameter for $\mathfrak{P}$. There exists a unit u in o_p such that

$$\psi(\mathfrak{P}) = u\pi^f.$$

We claim that $[\pi]$ has the following properties.

(i) $[\pi](t) \equiv \pi t$ mod degree 2.

(ii) $[\pi](t) = t^{Np}U(t) + \pi V(t)$

where U(t) is a unit power series, and V(t) is a power series. (Both, of course, have coefficients in the ring R of integers of $H_{\mathfrak{P}}$).

To prove the first property, consider an element α of o_c. Since $[\alpha](p(z),p'(z)) = (p(\alpha z),p'(\alpha z))$, for all z, the t-ordinate for the model E_1, $T = X/Y$ satisfies $[\alpha]T \equiv \alpha T$ mod degree 2. Under the transformation relating E_1 and E', t transforms $t = uT(1+\sum_{k=1}^{\infty} \ell_k T^k)$ with coefficients ℓ_k lying in M. Thus $[\alpha]t \equiv \alpha t$ mod degree 2. By continuity, the same is true for all α in $o_{c,p} = o_p$; in particular, this holds for π.

To prove the second property, suppose $[\pi](t)$ has the form $\sum_{n=1}^{\infty} a_n t^n$ with coefficients in R. Suppose a_r is the first coefficient not lying in $\mathfrak{P}$, so that it is a unit. Then the first coefficient of $[\pi]^f(t)$ not lying in $\mathfrak{P}$ is the coefficient of t^{r^f}; thus the

first coefficient of $[\psi(\mathfrak{P})](t) = [u][\pi]^f(t)$ not lying in $\mathfrak{P}$ is the coefficient of t^{r^f} (because $[u](t) \equiv ut$ mod degree 2). Hence $r = Np$, and our assertions (i),(ii) are proven. We conclude:

Lemma 1.9. Suppose that $\mathfrak{d}_K = p^{n+1}$. Then

$$|x'(P)|_{\mathfrak{P}_1} = |\pi|_{\mathfrak{P}}^{-2/\phi(p^{n+1})}.$$

Proof. We first observe that P belongs to $\hat{E}(\mathfrak{P}_1)$. For otherwise, $t = t(P)$ is not in $\mathfrak{P}_1$, nor are the conjugates over H. But $[\psi(\mathfrak{P})](t)$ is congruent mod $\mathfrak{P}$ to one such conjugate, and since this is zero, we have a contradiction.

Suppose $n = 0$. Then t satisfies $[\pi](t) = 0$. The assertions (i) and (ii) above show that

$$|t|_{\mathfrak{P}}^{Np-1} = |\pi|_{\mathfrak{P}}.$$

Since $x'(t) = t^{-2}a(t)$, the result follows. Now suppose the result is true for some integer $n \geq 0$, and consider a primitive p^{n+2}-division point P. Then $[\pi]P$ is a primitive p^{n+1}-division point, and

$$|[\pi]t|_{\mathfrak{P}} = |\pi|_{\mathfrak{P}}^{1/\phi(p^{n+1})}.$$

The assertions (i),(ii) again show that

$$|t|_{\mathfrak{P}}^{Np} = |[\pi]t|_{\mathfrak{P}},$$

so that

$$|x'(t)|_{\mathfrak{P}} = |\pi|_{\mathfrak{P}}^{-2/\phi(p^{n+1})}.$$

The lemma follows by induction.

Finally, we calculate the $\mathfrak{P}_1$-adic value of x'(P) in the cases not considered in the previous two lemmas, namely that $\mathfrak{f}_K$ is divisible by p and also by another prime of K.

Lemma 1.10. Suppose $\mathfrak{f}_K$ is divisible by at least two primes of K, including p. Then P is integral at $\mathfrak{P}_1$, and so $|x'(P)|_{\mathfrak{P}} \leq 1$.

Proof. Suppose $\mathfrak{f}_K = p^{n+1}g$ for some non-trivial o-ideal g, and let $\mathfrak{f}_1 = g \cap o_c$ be the corresponding proper o_c-ideal. Since P is a primitive $\mathfrak{f}$-division point, there exist a primitive p^{n+1}-division point Q_1 and a primitive $\mathfrak{f}_1$-division point Q_2 such that $P = Q_1+Q_2$. Now suppose that P were not integral at $\mathfrak{P}_1$, so that $P \in E'_{\mathfrak{f}} \cap \hat{E}(\mathfrak{P}_1)$. Now $Q_1 \in \hat{E}(\mathfrak{P}_1)$ (see previous lemma), so that $Q_2 = P-Q_1$ must lie in $\hat{E}(\mathfrak{P}_1)$. This contradicts lemma 1.8; thus P is integral at $\mathfrak{P}_1$, q.e.d.

Lemma 1.11. Let P and Q be primitive $\mathfrak{f}$-division and a-division points of E'. Suppose neither $\mathfrak{f}_K$ nor a_K are powers of the prime p. Then

$$|x'(P)-x'(Q)|_{\mathfrak{P}} = 1.$$

Proof. The preceding lemmas show that $|x'(P)-x'(Q)|_{\mathfrak{P}} \leq 1$. Suppose that strict inequality holds; thus denoting reduction mod $\mathfrak{P}_1$ by a tilde, this means that $x'(\tilde{P}) = x'(\tilde{Q})$, and therefore $\tilde{P} = \pm\tilde{Q}$. Since $(\mathfrak{f},a) = 1$, we conclude that $\tilde{P} = \tilde{Q} = \tilde{O}$ (the point at infinity under reduction). Thus both P and Q lie in $\hat{E}(\mathfrak{P}_1)$, contradicting lemmas 1.8 and 1.10. This proves the lemma.

We may now evaluate $\Theta(\rho,a,L)$ $\mathfrak{P}_1$-adically.

Lemma 1.12. Suppose that $\mathfrak{f}_K$ is a power of the prime p: $\mathfrak{f}_K = p^{n+1}$. Then $|\theta(\rho,a,L)|_{\mathfrak{P}} = |\pi|_{\mathfrak{P}}^{12(Na-1)/\phi(p^{n+1})}$. Otherwise, if $\mathfrak{f}_K$ is not a power of the prime p, $\theta(\rho,a,L)$ is a unit at $\mathfrak{P}_1$.

Proof. We use the expression (1) to calculate the $\mathfrak{P}_1$-adic values. First, note that because E' has good reduction at $\mathfrak{P}_1$, Δ' is a unit at $\mathfrak{P}_1$. Second, if p^r is the exact power of p dividing a,

$$|\Delta(L)/\Delta(a^{-1}L)|_{\mathfrak{P}} = |\pi|_{\mathfrak{P}}^{-12r}$$

[This follows from [14], p165, where it is shown that if q is an unramified prime of degree 1, prime to c, and $q_c = g \cap o_c$ then $\Delta(q_c^{-1}L)/\Delta(L)$ generates the ideal q^{12} in the ring of integers of H. From this a similar result for ramified primes holds (see proof of corollary); the result is trivial for unramified primes of degree 2, for they are principal].

Considering first the case when $\mathfrak{f}_K = p^{n+1}$, we note that p does not divide a_K, and so in the earlier notation

$$|\theta(\rho,a,L)|_{\mathfrak{P}} = \prod_{Q \in E'_a} |x'(P)-x'(Q)|_{\mathfrak{P}}^{-6} .$$

Lemmas 1.8, 1.9 show that $|x'(P)-x'(Q)|_{\mathfrak{P}} = |x'(P)|_{\mathfrak{P}} = |\pi|_{\mathfrak{P}}^{-2/\phi(p^{n+1})}$ and so prove the result.

Now suppose that $\mathfrak{f}_K$ is not a power of p. If p divides $\mathfrak{f}$, p does not divide a_K, and so

$$|\theta(\rho,a,L)|_{\mathfrak{P}} = \prod_{Q \in E'_a} |x'(P)-x'(Q)|_{\mathfrak{P}}^{-6} .$$

Lemma 1.11 then shows that the right hand side equals 1, so that $\theta(\rho,a,L)$ is a unit at $\mathfrak{P}_1$. On the other hand, if p divides a,

let p^r be the exact power of p dividing a; we have

$$|\theta(\rho,a,L)|_{\mathfrak{P}} = |\pi|_{\mathfrak{P}}^{-12r} \prod_{Q\in E'_a} |x'(P)-x'(Q)|_{\mathfrak{P}}^{-6} .$$

Lemma 1.11 shows that $|x'(P)-x'(Q)|_{\mathfrak{P}} = 1$ unless Q is a primitive p^S-division point (for some $1\le S\le r$), in which case

$$|x'(P)-x'(Q)|_{\mathfrak{P}} = |x'(Q)|_{\mathfrak{P}} = |\pi|_{\mathfrak{P}}^{-2/\phi(p^S)}.$$

The number of primitive p^S-division points is $\phi(p^S)$, so $\theta(\rho,a,L)$ is a unit at $\mathfrak{P}$. Finally, if p does not divide $\mathfrak{d}_K$ or a_K,

$$|\theta(\rho,a,L)|_{\mathfrak{P}} = \prod_{Q\in E'_a} |x'(P)-x'(Q)|_{\mathfrak{P}}^{-6} = 1$$

by lemma 1.11. This completes the proof of lemma 1.12.

The following corollary is immediate:

Corollary. Suppose that $\mathfrak{d}_K = p^{n+1}$. Let $a_1,\dots,a_r$ be o_c-ideals prime to 6c, let $\rho_1,\dots,\rho_r$ be primitive $\mathfrak{d}$-division points of L, and $n_1,\dots,n_r$ be rational integers. The product

$$\prod_{i=1}^{r} \theta(\rho_i,a_i,L)^{n_i}$$

is a unit (in $R(\mathfrak{d})$) precisely if $\sum_{i=1}^{r} n_i(Na_i-1) = 0$.

§5. Definition of the Elliptic Units.

We can now define the elliptic units with respect to the order o_c for arbitrary finite abelian extensions of K. As in the last section, the special orders in $\mathbb{Q}(\sqrt{-1})$ and $\mathbb{Q}(\sqrt{-3})$ are excluded.

Consider first the field $R(o_c)$. Let $\mathfrak{b}_1,\ldots,\mathfrak{b}_r$ be o_c-ideals prime to c, and $n_1,\ldots,n_r$ integers such that $\mathfrak{b}_1^{n_1}\ldots\mathfrak{b}_r^{n_r}$ is a principal fractional o_c-ideal with generator α in K*. Then (see lemma 1.12),

$$\alpha^{-12}\left(\frac{\Delta(L)}{\Delta(\mathfrak{b}_1^{-1}L)}\right)^{n_1}\cdots\left(\frac{\Delta(L)}{\Delta(\mathfrak{b}_r^{-1}L)}\right)^{n_r}$$

is a unit in $R(o_c)$. We define the elliptic units of $R(o_c)$ (with respect to the order o_c) to be the group $D(o_c)$ of values generated by these units and the roots $\mu_{R(o_c)}$ of unity in $R(o_c)$. [Note this definition is applicable for any order of K, including the special ones].

Lemma 1.13. $D(o_c)$ is stable under the action of $G(R(o_c)/K)$; it is independent of the choice of lattice L of definition, and depends solely upon o_c.

Proof. Let $a,\mathfrak{b}$ be proper o_c-ideals prime to c. Since

$$\left(\frac{\Delta(L)}{\Delta(\mathfrak{b}^{-1}L)}\right)^{[a_K,R(o_c)/K]} = \frac{\Delta(a^{-1}L)}{\Delta(a^{-1}\mathfrak{b}^{-1}L)} = \left(\frac{\Delta(L)}{\Delta(a^{-1}\mathfrak{b}^{-1}L)}\right)\cdot\left(\frac{\Delta(L)}{\Delta(a^{-1}L)}\right)^{-1},$$

it follows that $D(o_c)$ is stable under $G(R(o_c)/K)$. If L' is another lattice with order o_c, there is an idèle s of K such that $L' = s^{-1}L$ (see [23] p122.).

Now $\dfrac{\Delta(L')}{\Delta(\mathfrak{f}^{-1}L')} = \dfrac{\Delta(s^{-1}L)}{\Delta(\mathfrak{f}^{-1}s^{-1}L)} = \left(\dfrac{\Delta(L)}{\Delta(\mathfrak{f}^{-1}L)}\right)^{[s,K]}$; hence

$D(o_c)$ is independent of the choice of defining lattice, q.e.d.

When the conductor c equals 1, it is possible to define a larger group of units in $H = R(o)$. For in this case, every element of the form described above is, apart from a factor of a root of unity in $R(o_c)$, an e_K-th power. It is sufficient to prove this assertion for the numbers $\Delta(L)/\Delta(p^{-1}L)$, where p is a prime of K. Consider for a primitive p-division point ρ of L and a nontrivial principal ideal $a = (a)$ prime to $6p$, the number

$$N_{R(p)/R(o)}\ \Theta(\rho,a,L).$$

By lemma 1.7, it equals $(\Delta(L)/\Delta(p^{-1}L))^{\frac{(1-N\alpha)}{e_K}}$; but by lemma 1.5 it also equals

$$(*)\quad a^{12(Np-1)/e_K}\, P(j(L))^{(Np-1)(Na-1)/e_K}\, N_{R(p)/R(o)}\left(\prod_{\ell}(\tau(\rho,L)-\tau(\ell,L))^{-12}\right)$$

(the notation is as explained there). The numbers $Na-1$, as a varies over all such principal ideals, generate the ideal $e_H\mathbb{Z}$; choose integers $n_1,\ldots,n_r$ and principal ideals $a_1,\ldots,a_r$ such that $\sum_{i=1}^{r} n_i(Na_i-1) = e_H$.

Then $N_{R(p)/R(o)}\left(\prod_{i=1}^{r}\Theta(\rho,a_i,L)^{n_i}\right) = \left(\dfrac{\Delta(L)}{\Delta(p^{-1}L)}\right)^{-e_H/e_K}$.

Since e_H divides 12 (see [18] lemma 7), numbers of the form (*) are e_H-th powers; thus $\Delta(L)/\Delta(p^{-1}L)$ is, apart from a factor in μ_H, an e_K-th power in H.

We define C_H, <u>the full group of elliptic units in H</u>, to be the largest subgroup of the units in H such that $\mu_H C_H^{e_K} = \mu_H D(o)$.

It is obvious that C_H is stable under $G(H/K)$; its definition is independent of the defining lattice L - it depends solely on o. This group is defined by Robert ([18], section 3; see theorem 5 for the equivalence); he calculates its index in the units of H. Henceforth, let $C(o_c)$ denote the group $D(o_c)$, if $c \neq 1$, or the group C_H, if $c = 1$.

Let us now consider the field $R(\mathfrak{f})$, where $\mathfrak{f}$ is an o_c-ideal prime to c. For every divisor $b \neq (1)$ of $\mathfrak{f}$, let $P(b)$ denote the group generated by the values $\Theta(\rho,a,L)$, where ρ varies over all primitive b-division points of L, and a varies over all o_c-ideals prime to $6bc$; let $W(b)$ denote the subgroup of products $\prod_i \Theta(\rho_i,a_i,L)^{n_i}$ in $P(b)$ satisfying $\sum_i n_i(Na_i-1) = 0$. Lemma 1.12 shows that $W(b)$ lies inside the units of $R(\mathfrak{f})$. We define the <u>group of elliptic units of $R(\mathfrak{f})$</u> (<u>with respect to o_c</u>) to be the group generated by these groups $W(b)$, by $\mu_{R(\mathfrak{f})}$ and $C(o_c)$, that is, the group $\mu_{R(\mathfrak{f})} \cdot \prod_{b|\mathfrak{f},b\neq(1)} W(b) \cdot C(o_c)$; we define the <u>full group of elliptic units of $R(\mathfrak{f})$ (with respect to o_c)</u> to be the units (of $R(\mathfrak{f})$) contained in the group

$$\mu_{R(\mathfrak{f})} \cdot \prod_{b|\mathfrak{f},b\neq(1)} P(b) \cdot C(o_c).$$

More generally, given a finite abelian extension F of K with o_c-conductor $\mathfrak{f}$, prime to c, (i.e. $\mathfrak{f}$ is the largest o_c-ideal g such that $F \subseteq R(g)$), we define the <u>group of elliptic units of F (with respect to o_c)</u> to be the group generated by μ_H and the norm groups $N_{R(b)/R(b)\cap F}(W(b))$ (for b dividing $\mathfrak{f}$, $b \neq (1)$) and $N_{R(o_c)/R(o_c)\cap F}(C(o_c))$. Similarly, we define the <u>full</u>

group of elliptic units of F (with respect to o_c) to be the units (in F) in the group generated by μ_H, and the norm groups $N_{R(b)/R(b)\cap F}(P(b))$ and $N_{R(o_c)/R(o_c)\cap F}(C(o_c))$.

Note that if $\mathfrak{f}_K$ is a power of a single prime, the group of elliptic units of F equals the full group.

Lemma 1.14. Both the group and the full group of elliptic units of F are stable under the action of G(F/K). The groups are independent of the choice of L, and depend solely upon o_c and F.

Proof. It suffices to show that the groups $W(b)$ and $P(b)$ are stable under the action of a idèle s of K. Let ρ be a primitive b-division point of L, and a an ideal of K prime to $6cb$. Then

$$\Theta(\rho,a,L)^{[s,K]} = \Theta(s^{-1}\rho,a,s^{-1}L)$$

Now $s^{-1}L$ is a lattice with order o_c, so there is an o_c-ideal g prime to $6bc$ and a complex number λ such that $s^{-1}L = \lambda g^{-1}L$; hence

$$\Theta(\rho,a,L)^{[s,K]} = \Theta(\lambda^{-1}s^{-1}\rho,a,g^{-1}L).$$

But $\lambda^{-1}s^{-1}\rho$ is a primitive b-division point of $g^{-1}L$, and

$$\Theta(\tau,a,g^{-1}L) = \Theta(\tau,ag,L)/\Theta(\tau,g,L)^{Na}.$$

It is therefore clear that $P(b)$ is stable under [s,K]. The action of s on a product

$$\prod_i \Theta(\rho_i,a_i,L)^{n_i}$$

of $P(b)$ satisfying $\sum_i n_i(Na_i-1) = 0$ gives an element

$$\prod_i \Theta(\tau_i,a_ig,L)^{n_i}/\Theta(\tau_i,g,L)^{n_iNa_i}$$

with $\tau_i = \lambda^{-1}s^{-1}\rho_i$; this lies in $W(b)$ because the sum

$$\sum_i n_i(N\mathfrak{a}_i g-1)-n_i N\mathfrak{a}_i(Ng-1) = \sum_i n_i(N\mathfrak{a}_i-1)$$

is zero, so that $W(\mathfrak{b})$ is stable under $[s,K]$.

Also, if L' is another lattice with order $\mathfrak{o}_c$, then $L' = s^{-1}L$ for some idèle s of K. If ρ' is an $\mathfrak{b}$-division point of L', $s\rho'$ is a $\mathfrak{b}$-division of L, and therefore $\theta(\rho',\mathfrak{a},L') = \theta(s\rho',\mathfrak{a},L)^{[s,K]}$ lies in $P(\mathfrak{b})$. Thus $P(\mathfrak{b})$, and similarly $W(\mathfrak{b})$, is independent of the choice of L: that is, the group of elliptic units and the full group of elliptic units of F depend solely upon $\mathfrak{o}_c$ (and F).

Remark. The group $\prod_{\mathfrak{b}\mid\mathfrak{f},\mathfrak{b}\neq(1)} P(\mathfrak{b})$ defined above is, modulo roots of unity, generated by the values $\theta(\rho,\mathfrak{a},L)$ where ρ varies over all primitive or imprimitive division points of L, and $\mathfrak{a}$ varies over all $\mathfrak{o}_c$-ideals prime to $6\mathfrak{f}c$. For, if ρ is primitive $\mathfrak{b}$-division, and $\mathfrak{a}$ is not prime to $\mathfrak{f}$, choose an $\mathfrak{o}_c$-ideal $\mathfrak{g}$ prime to $\mathfrak{f}$ and lying in the same class mod*$\mathfrak{b}$. Then using the function $\phi(z,L)$ (see chap.2, p.46)
$\theta(\rho,\mathfrak{a},L) = \phi(\rho,L)^{N\mathfrak{a}}/\phi(\rho,\mathfrak{a}^{-1}L) = \theta(\rho,\mathfrak{g},L)\phi(\rho,L)^{N\mathfrak{a}-N\mathfrak{g}}\phi(\rho,\mathfrak{g}^{-1}L)/\phi(\rho,\mathfrak{a}^{-1}L)$
Choose integers $\alpha,\beta \equiv 1 \bmod \mathfrak{b}$ such that $\alpha\mathfrak{a} = \beta\mathfrak{g} = \mathfrak{c}$. Then
$\phi(\rho,\mathfrak{g}^{-1}L)/\phi(\rho,\mathfrak{a}^{-1}L) = \phi(\beta^{-1}\rho,\mathfrak{c}^{-1}L)/\phi(\alpha^{-1}\rho,\mathfrak{c}^{-1}L)$. Now $\alpha^{-1}\rho$ and $\beta^{-1}\rho$ are $\mathfrak{b}$-division points for $\mathfrak{c}^{-1}L$ and $\alpha^{-1}\rho \equiv \rho \equiv \beta^{-1}\rho \bmod \mathfrak{c}^{-1}L$. Lemma 2.6 shows this ratio is a root of unity. Since $N\mathfrak{a}-N\mathfrak{g}$ is divisible by $e_{R(\mathfrak{b})}$, we may choose $\mathfrak{o}_c$-ideals $\mathfrak{g}_1,\ldots,\mathfrak{g}_r$ prime to $6\mathfrak{f}c$ in the principal class mod*$\mathfrak{b}$ such that $n = \sum_1^r n_i(N\mathfrak{g}_i-1) = N\mathfrak{a}-N\mathfrak{g}$; hence $\phi(\rho,L)^n = \prod_1^r \theta(\rho,\mathfrak{g}_i,L)^{n_i}$ and our assertion follows.

Robert [18] defines the group of elliptic units for arbitrary abelian extensions F of K with respect to the order which is the full ring of integers of K (c = 1). When the conductor $\mathfrak{f}$ is prime to e_K, the group of elliptic units (not the full group) is precisely that defined in [18] (§4.4, §4.5 and §5; see theorem 7

for the equivalence). In the case that $(\mathfrak{f}, e_K) \neq 1$, Robert obtains a slightly larger group by extracting a square root (and third or fourth roots in $\mathbb{Q}(\sqrt{-3})$ or $\mathbb{Q}(\sqrt{-1})$) in some of the subgroups $W(b)$ as follows. For each divisor b, let e_b be the number of elements in μ_K congruent to 1 modulo b; then each element of $W(b)$ is an e_b-th power, and set $W'(b)$ to be the largest subgroup of units such that $(W'(b))^{e_b} \subseteq W(b)$ [This is non-trivial only if b divides 2 ($K \neq \mathbb{Q}(\sqrt{-3})$) or b divides $2\sqrt{-3}$ ($K = \mathbb{Q}(\sqrt{-3})$)]. Robert takes the elliptic units to be as defined above with $W(b)$ replaced by $W'(b)$; in §6 of [18], he calculates the index of this group for those extensions F with the conductor $\mathfrak{f}$ a power of a single prime p of K (in this case the full group equals the group of elliptic units).

We will calculate the index of the <u>full</u> group of units for a much wider class of conductors $\mathfrak{f}$ which includes all prime powers. For simplicity the conductor $\mathfrak{f}$ will be taken to be prime to 6, and the class number of K will be assumed to be 1. These assumptions seem inessential to the method used, and we hope to publish the refinements soon.

The following result will be used in chapters 2 and 3.

<u>Lemma 1.15</u>. Suppose K has class number one.

(1) Let $\mathfrak{f}$ be an integral ideal of K prime to 6 and p a prime divisor of $\mathfrak{f}$. Then for all positive integers n,

$$\mathbf{N}_{R(\mathfrak{f}p^n)/R(\mathfrak{f})} P(\mathfrak{f}p^n) = P(\mathfrak{f})$$

(2) Let p be a prime of K, not dividing 6, and $\mathfrak{P}$ be the unique prime of $R(p^n)$ above p. Then $\mathfrak{P}^{12}$ is principal, and is generated by an element of $P(p^n)$.

Proof. It suffices to prove the first assertion for n = 1. Let ρ be a primitive $\mathfrak{f}p$-division point. The conjugates of $\theta(\rho,a,L)$ over $R(\mathfrak{f})$ are

$$\theta(\rho+\eta,a,L),$$

where η runs over all p-division points of L.

Lemma 1.5 shows that

$$\prod_{\eta} \theta(\rho+\eta,a,L) = \theta(\rho,a,p^{-1}L);$$

the result follows upon noting that ρ is a primitive $\mathfrak{f}$-division point of $p^{-1}L$.

As for the second, choose ideals $a_1,\ldots,a_r$ prime to $6p$ and integers $n_1,\ldots,n_r$ such that $\sum_{j=1}^{r} n_j(Na_j-1) = e_K$. Let ρ be a primitive p^n-division point of L. Then lemma 1.12 shows that the element

$$\prod_{j=1}^{r} \theta(\rho,a_j,L)^{n_j}, \text{ which lies in } P(p^n) \text{ generates } \mathfrak{P}^{12}.$$

Also in this case, when K has class number 1, and we consider the order with conductor 1, the following more general version of lemma 1.7 holds.

Lemma 1.16. Lemma 1.7 holds for o-ideals a and $\mathfrak{f}$ such that $(a,6\mathfrak{f}) = 1$ (So $\mathfrak{f}$ is not necessarily prime to 6).

Proof. As shown in the proof of lemma 1.7, there is a constant $C = C(\mathfrak{f},a,L)$ such that

$$\prod_{\rho} \theta(z+\rho,a,L) = C^{12}\theta(z,a,\mathfrak{f}^{-1}L),$$

where ρ runs over all $\mathfrak{f}$-division points of L; the constant C lies in K. Lemma 1.12 shows that C is a unit; hence $C^{12} = 1$. q.e.d.

Chapter 2. The index of elliptic units for ray class fields.

This chapter presents the calculation of the index of the elliptic units in the global units for ray class fields over the quadratic imaginary base field K. The technique is guided by the work of Sinnott [25] on the index of cyclotomic units for fields of roots of unity. Throughout, we assume that K has class number one; this is made for technical convenience only, and we hope to extend these methods to arbitrary fields K. Also the conductor h of the ray class field is assumed prime to 6; but it is apparent that the present method can be refined to remove this restriction. This is related to the need to define a slightly larger subgroup of units than that given in §5 (c.f. remarks there).

Let h be a nontrivial integral ideal of K prime to 6, with a fixed generator h; let $H = R(h)$ denote the ray class field modulo h. The ideal h will remain fixed throughout this chapter, and suppose that $h = p_1^{e_1} \ldots p_r^{e_r}$ is its factorization into primes $p_1, \ldots, p_r$ (with positive integers $e_1, \ldots, e_r$); for each i let π_i denote a fixed generator of p_i. Let P be the group $\prod_{\substack{b \mid h \\ b \neq (1)}} P(b)$ defined in the last chapter (c.f. remark on p34); let S and C denote the global units and the full group of elliptic units of H, so that $C = S \cap \mu_H P$.

We suppose that h satisfies the following condition: if any prime p_i dividing h is unramified and of degree 1, then its conjugate $\overline{p_i}$ does not divide h. This somewhat strange condition is needed to establish a property (lemma 2.15) of the logarithm map defined below; the present method of calculating the index relies on this property.

Chapter 2. The index of elliptic units for ray class fields.

This chapter presents the calculation of the index of the elliptic units in the global units for ray class fields over the quadratic imaginary base field K. The technique is guided by the work of Sinnott [25] on the index of cyclotomic units for fields of roots of unity. Throughout, we assume that K has class number one; this is made for technical convenience only, and we hope to extend these methods to arbitrary fields K. Also the conductor h of the ray class field is assumed prime to 6; but it is apparent that the present method can be refined to remove this restriction. This is related to the need to define a slightly larger subgroup of units than that given in §5 (c.f. remarks there).

Let h be a nontrivial integral ideal of K prime to 6, with a fixed generator h; let $H = R(h)$ denote the ray class field modulo h. The ideal h will remain fixed throughout this chapter, and suppose that $h = p_1^{e_1} \ldots p_r^{e_r}$ is its factorization into primes $p_1, \ldots, p_r$ (with positive integers $e_1, \ldots, e_r$); for each i let π_i denote a fixed generator of p_i. Let P be the group $\prod_{\substack{b \mid h \\ b \neq (1)}} P(b)$ defined in the last chapter (c.f. remark on p34); let S and C denote the global units and the full group of elliptic units of H, so that $C = S \cap \mu_H P$.

We suppose that h satisfies the following condition: if any prime p_i dividing h is unramified and of degree 1, then its conjugate $\overline{p_i}$ does not divide h. This somewhat strange condition is needed to establish a property (lemma 2.15) of the logarithm map defined below; the present method of calculating the index relies on this property.

Chapter 2. The index of elliptic units for ray class fields.

This chapter presents the calculation of the index of the elliptic units in the global units for ray class fields over the quadratic imaginary base field K. The technique is guided by the work of Sinnott [25] on the index of cyclotomic units for fields of roots of unity. Throughout, we assume that K has class number one; this is made for technical convenience only, and we hope to extend these methods to arbitrary fields K. Also the conductor h of the ray class field is assumed prime to 6; but it is apparent that the present method can be refined to remove this restriction. This is related to the need to define a slightly larger subgroup of units than that given in §5 (c.f. remarks there).

Let h be a nontrivial integral ideal of K prime to 6, with a fixed generator h; let $H = R(h)$ denote the ray class field modulo h. The ideal h will remain fixed throughout this chapter, and suppose that $h = p_1^{e_1} \ldots p_r^{e_r}$ is its factorization into primes $p_1, \ldots, p_r$ (with positive integers $e_1, \ldots, e_r$); for each i let π_i denote a fixed generator of p_i. Let P be the group $\prod_{\substack{b \mid h \\ b \neq (1)}} P(b)$ defined in the last chapter (c.f. remark on p34); let S and C denote the global units and the full group of elliptic units of H, so that $C = S \cap \mu_H P$.

We suppose that h satisfies the following condition: if any prime p_i dividing h is unramified and of degree 1, then its conjugate $\overline{p_i}$ does not divide h. This somewhat strange condition is needed to establish a property (lemma 2.15) of the logarithm map defined below; the present method of calculating the index relies on this property.

Let S be the subset of 2^r-1 divisors of h obtained from the products of the ideals $p_1^{e_1},\ldots,p_r^{e_r}$, but omitting (1). Define $w = e_K^{-r} \prod_{b\in S} e_{R(b)}$; note $w = e_H/e_K$ if h is a prime power. Throughout let h_H and R_H denote the class number and regulator of H. Our main result is

Theorem 1. The group C is of finite index in S, equal to $12^{[H:K]-1}h_H$ (if $r = 1$) or $12^{[H:K]-1}h_H e_K^{2^{r-2}-r}.w_1(e_H/e_K)^{-1}$ (if $r \geq 2$), where w_1 divides w.

Robert [18] proved this result for the case of a prime power conductor h (i.e. $r = 1$); by using the cohomological arguments of Sinnott [25], we are able to prove our result for more general conductors h.

The method of proof analyses the classical class number formula relating h_H, R_H, and the values of the L-function for the characters of G(H/K) at $s = 1$: these values can be expressed in terms of elliptic units. The formula is quoted in section 2.

Throughout this chapter, it will be necessary to view H as a subfield of a field of h-division points as an elliptic curve E, which we now specify. As explained in chapter 1, §3, there is an elliptic curve E defined over K (which is equal to its own maximal abelian unramified extension) whose ring of endomorphisms is isomorphic to the integers o of K; by the work of Serre and Tate ([22], theorem 9), it is possible to suppose that E has good reduction at each prime dividing $6h\bar{h}$: that is, E is specified by an equation

$$y^2+a_1xy+a_3y = x^3+a_2x^2+a_4x+a_6$$

where the coefficients a_i are elements of K, integral at all primes

dividing $6h\bar{h}$, and the discriminant Δ is a unit at each such prime. Under the transformation

$$\eta = y + \frac{1}{2}(a_1x+a_3)$$

$$\xi = x + \frac{1}{12}(a_1^2+4a_2)$$

this equation takes the form E': $\eta^2 = \xi^3 - \frac{1}{4}g_2\xi - \frac{1}{4}g_3$ for some constants g_2, g_3 in K. Let $p(z)$ be the associated Weierstrass p-function satisfying

$$p'(z)^2 = 4p^3(z) - g_2p(z) - g_3.$$

Since K has class number one, there is a complex constant Ω such that $L = \Omega o$ is the period lattice of $p(z)$; the discriminant, $\Delta(L)$, of L equals Δ. Combining these maps ($\mathbb{C}/L \longrightarrow E'$ and $E' \longrightarrow E$) we obtain an analytic parametrization $\xi: \mathbb{C}/L \longrightarrow E$; we conclude that $K(E_h)$ is generated over K by the values $\{p(\rho), p'(\rho);\ \rho$ is h-division of L$\}$, and that H, which is generated by the values $\{\tau(\rho,L);\ \rho$ is h-division$\}$, is a subfield of $K(E_h)$. We also note that E has integral j-invariant (see [23], §4.6).

Let ψ be the Grossen character for E and $\mathfrak{f}$ its conductor (see [23], theorems 7.40 and 7.42); $\mathfrak{f}$ is divisible by precisely those primes of K where E has bad reduction; in particular, h is prime to $6\mathfrak{f}\bar{\mathfrak{f}}$.

Throughout this chapter, G will denote the Galois group G(H/K), and $R = \mathbb{Z}[G]$ its group ring; G_1 will denote $G(K(E_h)/K)$, and $R_1 = \mathbb{Z}[G_1]$ its group ring. The letters χ and ξ will be reserved for characters of G and G_1 respectively; ρ_χ and ρ_ξ will denote the ring homomorphisms $\rho_\chi: \mathbb{C}[G] \longrightarrow \mathbb{C}$ and $\rho_\xi: \mathbb{C}[G_1] \longrightarrow \mathbb{C}$ induced by χ and ξ respectively. Given a set of complex numbers a_χ for characters χ of G, there is a unique a in $\mathbb{C}[G]$ such that

$\rho_\chi(a) = a_\chi$ for each χ; explicitly $a = \sum_\chi a_\chi e_\chi$, where $e_\chi = \frac{1}{|G|} \sum_{\sigma \in G} \chi(\sigma)\sigma^{-1}$ is the idempotent associated to $\chi (e_\chi^2 = e_\chi)$; for any two distinct characters χ_1, χ_2 of G, $e_{\chi_1} e_{\chi_2} = 0$. A similar result holds for the homomorphisms ρ_ξ attached to G_1; we will denote the idempotent attached to ξ by ε_ξ $(= \frac{1}{|G_1|} \sum_{\tau \in G_1} \xi(\tau)\tau^{-1})$.

For a character χ of G, denote its conductor by $\mathfrak{f}_\chi$; $\mathfrak{f}_\chi$ is the conductor (in the sense of class field theory) of the extension K_χ/K, where K_χ is the fixed field of the kernel of χ. χ therefore induces a character, denoted always by χ', of $G(R(\mathfrak{f}_\chi)/K)$; χ' is the associated primitive character of χ, and its kernel fixes K_χ. The conductor $\mathfrak{f}_\chi$ divides h, and so is prime to 6; hence $G(R(\mathfrak{f}_\chi)/K)$ is isomorphic, via the Artin map, to $(o/\mathfrak{f}_\chi)^*/\mu_K$. The following diagram is commutative:

$$\begin{array}{ccc} (o/h)^* & \longrightarrow & G(R(h)/K) \\ \downarrow & & \downarrow \\ (o/\mathfrak{f}_\chi)^* & \longrightarrow & G(R(\mathfrak{f}_\chi)/K) \end{array}$$

The vertical map on the left is the natural surjection; that on the right is the restriction map.

We regard χ as a function on the ideals a of K by defining $\chi(a)$ to be $\chi([a,H/K])$ if $(a,h) = 1$, and to be zero otherwise; similarly we define $\chi'(a)$ to be $\chi'([a,R(\mathfrak{f}_\chi)/K])$ if $(a,\mathfrak{f}_\chi) = 1$, and to be zero otherwise. Note that if p is a prime dividing h, but <u>not</u> $\mathfrak{f}_\chi$, then $\chi'(p) \neq 0$. For any integer of K, we set $\chi(t) = \chi(to)$.

A similar notation will be used for characters ξ of G_1; these will be regarded as characters of $G(R(\mathfrak{f}h)/K)$ whose kernels

fix $K(E_h)$. The conductor $\mathfrak{f}_\xi$ is the conductor of the fixed field K_ξ of the kernel of ξ, and ξ induces an associated primitive character ξ' of $G(R(\mathfrak{f}_\xi)/K)$ (whose kernel fixes K_ξ).

For brevity, $B(\mathfrak{g})$ will denote the group $(\mathfrak{o}/\mathfrak{g})^*/\mu_K$ for any ideal $\mathfrak{g}$ prime to 6.

Throughout $\ell = \ell_H$ will denote the logarithmic embedding into $\mathbb{R}[G]$, defined by

$$\ell: H^x \longrightarrow \mathbb{R}[G]$$
$$x \longmapsto \sum_{\sigma\in G} -\log|x^\sigma|\sigma^{-1}.$$

Note that ℓ is an R-module map: $\sigma\ell(x) = \ell(x^\sigma)$ for each $\sigma\in G$. If $x\in H^x$ lies in the kernel of ℓ, $|x^\sigma| = 1$ for each $\sigma\in G$; thus if x is integral, x lies in μ_H. In particular, the kernel of ℓ in S is μ_H, and since $\mu_H \subseteq C$, $S/C \simeq \ell(S)/\ell(C)$.

Finally, for any R-module A, let A_o denote the submodule annihilated by $s(G) = \sum_{\sigma\in G} \sigma$; let A^G denote the submodule fixed by G.

The condition on h implies that if x lies in $P\cap K^\times$, and $\ell(x) = 0$, the x is a root of unity in K. This property of ℓ will be used in lemma 2.15 to show that $\ell(P)_o = \ell(C)$.

§1. Fields of division points.

In this section, we gather together some results about fields of division points on E. Recall that $h \neq (1)$, and is prime to $6\mathfrak{f}\bar{\mathfrak{f}}$.

Lemma 2.1. E has good reduction everywhere over $K(E_h)$.

Proof: Let p be a prime dividing h; we use the criterion of Néron-Ogg-Shafarevich to show that E has good reduction everywhere over $K(E_p) \subseteq K(E_h)$. If p is unramified of degree 1, this is proven in [7] (theorem 2), so suppose that p is inert or ramified and lies above the rational prime p. Let $F_o = K(E_p)$ and q be a prime of F_o not lying above p; let $\bar{F}_o$ be the algebraic closure of F_o. Pick a prime of $\bar{F}_o$ lying above q, and let I_q be the corresponding inertia group. Let $T_p = \varprojlim E_{p^{n+1}}$ be the Tate module formed from the p^{n+1}-division points on E; it is a $G(\bar{F}_o/F_o)$ module, and its automorphism group is o_p^x. The image of $G(\bar{F}_o/F_o)$ is contained in the units congruent to 1 mod p; in particular, the image of I_q in the automorphism group of T_p is either trivial or infinite. Now E has integral j-invariant, and it is known (c.f. [22] p496) that the image of I_q must be finite; thus I_q acts trivially on T_p. Theorem 1 of [22] shows that E has good reduction at q. This is true for all primes q of F_o not above p; by hypothesis the same is true for all primes above p, and the proof of the lemma is complete.

Lemma 2.2. The ray class field mod $\mathfrak{f}$ equals $K(E_{\mathfrak{f}})$;
the ray class field mod $\mathfrak{f}h$ equals $K(E_{\mathfrak{f}h})$.
The conductor of $K(E_h)$ is $\mathfrak{f}h$.

Proof: We use the notation and results of [23] to prove this in a manner similar to that of Coates-Wiles [7].

Let g be an ideal of K divisible by $\mathfrak{f}$. Let $U(g)$ denote the subgroup of the idèle group as defined on p116 of [23], and x be any element of $U(g)$ with $x_\infty = 1$. Since the conductor $\mathfrak{f}$ of ψ divides g, Shimura's reciprocity law shows that the Artin symbol $[x,K]$ fixes E_h (see [7], lemma 3). Thus $K(E_g) \subseteq R(g)$. But the classical theory of complex multiplication shows that $R(g) \subseteq K(E_g)$. Hence $K(E_g) = R(g)$ and the first two statements of the lemma follow.

For the last part, let b denote the conductor of $K(E_h)$ over K. We first show that b divides $\mathfrak{f}h$. Again Shimura's reciprocity law shows that, for any idèle x in $U(\mathfrak{f}h)$ with $x_\infty = 1$, the Artin symbol $[x,K]$ fixes E_h (see [7], Lemma 4). Thus b divides $\mathfrak{f}h$.

On the other hand, because E has good reduction everywhere over $K(E_h)$, the Grossen character Ψ of E over $K(E_h)$ must be 1 (see [23], theorem 7.42). But Ψ is the composition of ψ and the norm map from $K(E_h)$ to K; so the conductor of ψ divides the conductor b of $K(E_h)/K$. Furthermore, because $K(E_h)$ contains $R(h)$, h must divide b. Since $(\mathfrak{f},h) = 1$, $\mathfrak{f}h$ divides g; we conclude that $g = \mathfrak{f}h$, q.e.d.

Lemma 2.3. Suppose h is a power of a prime p, $h = p^{n+1}$.

Then $K(E_h)$ is an extension of K of degree $\phi(p^{n+1})$, which is totally ramified at p.

Proof: This is proved in [7], p228 for the case of an unramified prime of degree 1. More generally, since E has good reduction at p over K, we may consider as in §3, chapter 1, the formal group $\hat{E}$ which is the kernel of reduction modulo p. K has class number one

so $\psi(p) = \pi$ is a generator for p, and the endomorphism $[\psi(p)]$ of the formal group $\hat{E}$ induced by it satisfies

(i) $[\pi](t) \equiv \pi t$ mod degree 2

(ii) $[\pi](t) \equiv t^{Np}$ mod p.

Thus $\hat{E}$ is a Lubin-Tate formal group over o_p. By [16], there is a unique formal group E defined over o_p such that the endomorphism $[\pi]$ of E is given by the power series $[\pi]w = w^{Np}+\pi w$; E is isomorphic to $\hat{E}$ over o_p. We conclude that $K_p(E_{p^{n+1}})$ is a totally ramified extension of K_p of degree $(Np)^n(Np-1)$.

Now the action of $G(K(E_h)/K)$ on E_h defines an injection $G(K(E_h)/K) \hookrightarrow (o/h)^x$, so that $[K(E_h):K]$ is at most $\phi(h) = (Np)^n(Np-1)$; we conclude that $K(E_h)/K$ has degree $\phi(h)$ and is totally ramified at p.

Lemma 2.4. Suppose h_1 and h_2 are coprime ideals of K, prime to $6\mathfrak{f}\bar{\mathfrak{f}}$. Then $K(E_{h_1})\cap K(E_{h_2}) = K$ and the composition $K(E_{h_1})K(E_{h_2}) = K(E_{h_1h_2})$.

Proof: The conductor of the extension $K(E_{h_1})\cap K(E_{h_2})$ divides $\mathfrak{f}h_1$ and $\mathfrak{f}h_2$, and so divides $\mathfrak{f}$. But $R(\mathfrak{f}) = K(E_{\mathfrak{f}})$ is unramified at any primes dividing h_1h_2, so $K(E_{h_1})\cap K(E_{h_2}) = K$. Because $E_{h_1h_2} = E_{h_1}\oplus E_{h_2}$ is the direct sum of E_{h_1} and E_{h_2} on the curve E, $K(E_{h_1h_2})$ is contained in $K(E_{h_1}).K(E_{h_2})$; equality follows upon computing degrees.

Lemma 2.5. The ray class field mod $\mathfrak{f}h$ equals the composition

$$K(E_{\mathfrak{f}}).K(E_h), \text{ and}$$

$$K(E_{\mathfrak{f}})\cap K(E_h) = K.$$

The degree $[K(E_h): R(h)]$ equals e_K.

Proof: Since $K(E_{\mathfrak{f}})$ is unramified at all primes dividing h, $K(E_{\mathfrak{f}}) \cap K(E_h) = K$. Clearly

$$R(\mathfrak{f}h) = K(E_{\mathfrak{f}h}) \supseteq K(E_{\mathfrak{f}}).K(E_h);$$

equality follows by computing degrees. Finally,

$$[K(E_h): R(h)] = [K(E_h):K][R(h):K]^{-1} = e_K.$$

Remark. The results of this section are in fact valid for any conductor $\mathfrak{f}$ and any ideal h prime to $\mathfrak{f}\bar{\mathfrak{f}}$; we do not need the conditions imposed on $\mathfrak{f}$ and h in the introduction.

§2. The Class Number Formula.

The proof of theorem 1 relies upon the classical class number formula, which relates the class number h_H, the regulator R_H, and the values $L(1,\chi)$ of the L-functions attached to the nontrivial characters χ of G. These values $L(1,\chi)$ can be expressed in terms of a function ϕ defined below (see [24],[18]); this function $\phi(z,L)$ takes values at h-division points z of L which are closely related to generators of the elliptic units of H.

We recall that the function $\theta(z,L)$ was defined in the last chapter (§3), and that a(L) denotes the area of the fundamental parallelogram of $L = \Omega o$. Define

$$\phi(z,L) = \theta(z,L)\exp(-6\pi|z|^2/a(L))$$

and $u(z) = \log|\phi(z\Omega,L)|$. Notice that for an ideal a of K,

$$\phi(z,L)^{N\alpha}/\phi(z,a^{-1}L) = \Theta(z,a,L);$$

we will be considering values of $\phi(\rho,L)$ and $u(\rho/\Omega,L)$ at h-division points ρ of L. The following lemma summarises the basic properties of ϕ and u.

Lemma 2.6. Let b be an integral ideal of K.

(1) Suppose that b is the smallest positive rational integer in b; let ρ be a b-division point of L. Then $\phi(\rho,L)^b$ is independent of the choice of ρ modulo L.

(2) Let a be a nonintegral element of K. For any integer α and any root of unity ε in K, $u(a+\alpha) = u(\varepsilon a) = u(a)$.

(3) Let β be a generator of b. Then

$$\sum_{t \bmod b} u(\frac{a+t}{\beta}) = u(a),$$

the sum being taken over a complete set of inequivalent representatives for o mod b.

Proof: For arbitrary $\omega \in L$,

$$\frac{\phi(\rho+\omega,L)}{\phi(\rho,L)} = \frac{\theta(\rho+\omega,L)}{\theta(\rho,L)} \exp\left(\frac{6\pi}{a(L)} (z\bar{z}-(z+\omega)(\bar{z}+\bar{\omega}))\right)$$

But $\frac{\theta(\rho+\omega,L)}{\theta(\rho,L)} = \exp\left(\frac{12\pi\bar{\omega}}{a(L)} (\rho + \frac{1}{2}\omega)\right)$ (see the proof of lemma 1.5), so that

$$\frac{\phi(\rho+\omega,L)}{\phi(\rho,L)} = \exp\left(\frac{6\pi}{a(L)} (\bar{\omega}\rho - \bar{\rho}\omega)\right)$$

Now $(\bar{\omega}\rho - \bar{\rho}\omega)/2i$ in the area of the parallelogram formed by the points ω and ρ in the complex plane, so that this ratio is a b^{th} root of unity. This proves part (1).

Now consider a nonintegral element a of K. The result just proved shows that $u(a+\alpha) = u(a)$ for every integer α. For the rest, suppose that a has denominator g (so that $ag \subseteq o$); choose a nontrivial ideal a prime to $6gb$ and in the principal ray class mod gb. Then $(N\mathfrak{a}-1)u(a,L) = \log|\theta(a\Omega,\mathfrak{a},L)|$; from this, it is clear that $u(\varepsilon a,L) = u(a,L)$ for any ε in μ_K. Also by lemma 1.16,

$$(N\mathfrak{a}-1) \sum_{t \bmod b} u\left(\frac{a+t}{\beta}\right) = \log\left| \prod_{t \bmod b} \theta\left(\frac{a+t}{\beta}\Omega,\mathfrak{a},L\right)\right|$$

$$= \log|\theta(a\Omega,\mathfrak{a},L)| = (N\mathfrak{a}-1)u(a).$$

This completes the proof of parts (2) and (3).

The connection between u and the elliptic units of H may be summarized as follows. Let $V(h)$ be the additive subgroup of $\mathbb{C}[G]$ generated by the elements

$$\eta(a) = \sum_{t \in B(h)} u\left(\frac{at}{h}\right)[t,H/K]^{-1},$$

where a ranges over all integers of K not divisible by h. $V(h)$ is an R-module ($[t,H/K]\eta(a) = \eta(at)$) and is in fact generated as an R-module by the elements $\eta(b)$, where b ranges over all integers

of K which divide h (excluding (b) = h). For given an integer $a \nmid h$, we may choose an integer t, prime to $6h$, such that b = at is a divisor of h; then $\eta(a) = [t,H/K]^{-1}\eta(b)$. Since $\eta(\varepsilon b) = \eta(b)$ for any ε in μ_K, we use the notation $\eta(b)$ for $\eta(b)$, where b is any generator of b.

For any ideal a of K, prime to $6h$,

$$(Na-[a,H/K])\eta(a) = \ell(\Theta(\tfrac{a}{h},a,L)).$$

Thus, denoting by $I(h)$ the R-ideal generated by the elements $Na-[a,H/K]$ as above, we have

$$I(h).V(h) = \ell(P).$$

For brevity, $V(h)$ and $I(h)$ will be denoted by V and I (resp.) in the rest of this chapter.

The function u may be used to form sums depending upon characters χ of G. For such a character, let f_χ be a generator of the conductor $\mathfrak{f}_\chi$ of χ; recall that χ' denotes the associated primitive character of $G(R(\mathfrak{f}_\chi)/K)$.

Define $$u(\chi') = \sum_{t\in B(\mathfrak{f}_\chi)} u(\tfrac{at}{f_\chi})\chi'(\sigma_t),$$

where $\sigma_t = [t,R(\mathfrak{f}_\chi)/K]$. (Note it is independent of choice of generator f_χ). The next lemma shows in particular that

$$\rho_\chi(\eta(1)) = \sum_{t\in B(h)} \bar{\chi}([t,H/K])u(\tfrac{t}{h}) = u(\bar{\chi}').\prod_{p|h}(1-\bar{\chi}'(p)),$$

the product being taken over all primes p dividing h.

Lemma 2.7. Let b = (b) be an integral ideal of K, prime to 6, and divisible by $\mathfrak{f}_\chi$. Then

$$\sum_{t \in B(b)} \chi'(t) u\left(\frac{t}{b}\right) = u(\chi') \prod_{p \mid b} (1-\chi'(p))$$

the product being taken over all primes p dividing b.

Proof: For any such ideal b divisible by $\mathfrak{f}_\chi$, let $u_b(\chi')$ denote the sum on the left hand side. We show that for any prime p (with generator π)

$$u_{bp}(\chi') = u_b(\chi') \text{ if } p \text{ divides } b,$$

and $$u_{bp}(\chi') = (1-\chi'(p))u_b(\chi') \text{ otherwise.}$$

Consider first the case when p divides b; we have

$$u_{bp}(\chi') = e_K^{-1} \sum_{\substack{t \bmod bp \\ (t,bp)=1}} \chi'(t) u\left(\frac{t}{b\pi}\right).$$

In this case, an integer of the form x+yb is prime to b precisely if x is prime to b. Thus

$$u_{bp}(\chi') = e_K^{-1} \sum_{\substack{x \bmod b \\ (x,b)=1}} \sum_{y \bmod p} \chi'(x+yb) u\left(\frac{x+yb}{b\pi}\right).$$

Now $\chi'(x+yb) = \chi'(x)$ because $\mathfrak{f}_\chi$ divides b, and Lemma 2.6 shows that

$$\sum_{y \bmod p} u\left(\frac{x+yb}{b\pi}\right) = u\left(\frac{x}{b}\right).$$

Hence $u_{bp}(\chi') = e_K^{-1} \sum_{\substack{x \bmod b \\ (x,b)=1}} \chi'(x) u\left(\frac{x}{b}\right) = u_b(\chi')$, as desired.

Turning to the case where $p \nmid b$, an integer of the form $x\pi+yb$ is prime to bp precisely if $(x,b) = (y,p) = 1$. Thus

$$u_{bp}(\chi') = e_K^{-1} \sum_{\substack{x \bmod b \\ (x,b)=1}} \sum_{\substack{y \bmod p \\ (y,p)=1}} \chi'(x\pi+yb) u\left(\frac{x\pi+yb}{\pi b}\right)$$

Again $\chi'(x\pi+yb) = \chi'(x\pi)$; also

$$\sum_{\substack{y \bmod p \\ (y,p)=1}} u\left(\frac{x\pi+yb}{\pi b}\right) = u\left(\frac{x\pi}{b}\right) - u\left(\frac{x}{b}\right).$$

Thus $u_{bp}(\chi') = (1-\chi'(\pi))u_b(\chi')$, which proves the second part.

We deduce from the formulae that

$$u_b(\chi') = \prod_{\substack{p \mid b \\ p \nmid \mathfrak{f}}} (1-\chi'(p)) \cdot u_{\mathfrak{f}_\chi}(\chi'),$$

where the product is taken over all primes dividing b, but not $\mathfrak{f}_\chi$. Since χ has conductor $\mathfrak{f}_\chi$, $\chi'(p) = 0$ if $p \mid \mathfrak{f}_\chi$, furthermore, $u_{\mathfrak{f}\chi}(\chi') = u(\chi')$. The lemma is now proven. The class number formula can be stated in terms of the $u(\chi')$:

$$h_H |R_H| = \frac{e_H}{e_K} \prod_{\chi \neq 1} \frac{|u(\chi')|}{6},$$

the product being taken over all nontrivial characters χ of G. [See Robert [18] p20; in his notation, $u(\chi') = S(\chi')/f_\chi$, where f_χ denotes the smallest positive rational integer in $\mathfrak{f}_\chi$, the conductor of χ; the modulus of $\rho(\chi')$ is 1, and $e_{\mathfrak{f}_\chi} = 1$ because $(h,6) = 1$].

The techniques of computing the index uses the general notion of lattice index outlined in Sinnott[25]; we briefly describe it here. If X is a subspace of the group ring $\mathbb{R}[G]$, we say that M is a lattice in X if M is a subgroup of X which is discrete (in the induced topology from $\mathbb{R}$) and which spans X. We note that a subgroup M of $\mathbb{R}[G]$ is discrete if and only if it is free over $\mathbb{Z}$ with a basis of elements linearly independent over $\mathbb{R}$.

Let M_1 and M_2 be lattices in X: then there is a nonsingular linear transformation A: X $\longrightarrow$ X such that $A(M_1) = M_2$. In this case, we define the symbol $(M_1:M_2)$ to be $|\det A|$ (the modulus of

the determinant of the transformation): it does not depend upon the choice of A. The following lemma is stated in Sinnott [25] (lemma 1.1) and is restated here for convenience.

Lemma 2.8. (a) If M_1 and M_2 are discrete subgroups of $\mathbb{R}[G]$ with $M_2 \subseteq M_1$, then $(M_1:M_2)$ is defined if and only if M_2 is of finite index in M_1; in this case $(M_1:M_2) = [M_1:M_2]$, the index.

(b) If M_1, M_2 and M_3 are discrete subgroups of $\mathbb{R}[G]$, then $(M_1:M_3) = (M_1:M_2)(M_2:M_3)$ i.e. whenever two of these symbols are defined, so is the third, and this relation holds.

This terminology and notation is applied to subgroups of $\mathbb{Q}[G]$, simply by viewing $\mathbb{Q}[G]$as a subring of $\mathbb{R}[G]$. A subgroup M of $\mathbb{Q}[G]$ is discrete precisely if M is finitely generated over $\mathbb{Z}$; given two discrete subgroups M_1 and M_2 of $\mathbb{Q}[G]$, the index $(M_1:M_2)$ is defined precisely if M_1 and M_2 generate over $\mathbb{Q}$ the same subspace of $\mathbb{Q}[G]$. The following lemma which is proved in [25] (lemma 6.1) is quite useful.

Lemma 2.9. Let A and B be discrete subgroups of $\mathbb{Q}[G]$, and suppose that (A:B) is defined. Let α be an element of $\mathbb{Q}[G]$.

Let A_α denote the set of elements $a \in A$ such that $\alpha a = 0$, and define B_α similarly. Then $(A_\alpha:B_\alpha)$ and $(\alpha A:\alpha B)$ are both defined, and $(A:B) = (A_\alpha:B_\alpha)(\alpha A:\alpha B)$.

The remainder of this section relates V to an R-module U which is independent of u; we will show that U is a free $\mathbb{Z}$-module of rank [H:K]. The basic step in the proof of theorem 1 is to express the index $[S:C] = [\ell(S):\ell(C)] = (\ell(S):\ell(C))$ in the form

$$(\ell(S):R_o)(R_o:U_o)(U_o:(1-e_1)V)((1-e_1)V:(1-e_1)\ell(P))((1-e_1)\ell(P):\ell(C)).$$

(Here R_o, U_o denote the submodules of R,U respectively annihilated

by $s(G) = \sum_{\sigma \in G} \sigma$). Each of the indices will be shown to be defined, and the value calculated.

We now discuss the module U. For any prime p, let $\bar{\sigma}_p = \sum_{\chi} \bar{\chi}'(p) e_\chi$, the sum being taken over all characters χ of G. Note that $\bar{\sigma}_p$ actually lies in $\mathbb{Q}[G]$. For any divisor b of h, let $H_b = G(R(h)/R(b))$ be the subgroup of G fixing $R(b)$; let $s(H_b) = \sum_{\sigma \in H_b} \sigma$ (an element of $\mathbb{Z}[G]$). Finally, let $\omega = \omega(u) = \sum_{\chi \neq 1} u(\bar{\chi}') e_\chi$, the sum being taken over all nontrivial characters of G. We define $U(h)$ to be the R-module generated by the elements $\alpha_b = s(H_b) \prod_{p \mid b} (1-\bar{\sigma}_p)$, the product being taken over all primes p dividing b , and b varying over all integral divisors of h. For brevity $U(h)$ will be denoted by U in this chapter.

Lemma 2.10. $(1-e_1)V = \omega.U$.

Proof: V is generated as an R-module by the elements $\eta(b)$, where b is an integral divisor of h ($b \neq h$). For such a divisor $b = (b)$, let $a = hb^{-1}$. We claim that

$$(1-e_1)\eta(b) = \omega\alpha_a;$$

it suffices to show that for any nontrivial character χ of G,

$$\rho_\chi(\eta(b)) = \rho_\chi(\omega\alpha_a).$$

We first observe that $\rho_\chi(\eta(b)) = 0$ if the conductor δ_χ of χ does not divide a. For, in this case, there exists an integer t prime to h and congruent to 1 mod a such that $\chi(t) \neq 1$; then $[t,H/K]\eta(b) = \eta(bt) = \eta(b)$ since $bt \equiv b \bmod h$. Applying ρ_χ to this last equation shows that $\rho_\chi(\eta(b)) = 0$.

On the other hand, if δ_χ divides a,

$$\rho_\chi(\eta(b)) = \sum_{t\in B(h)} \bar{\chi}(t)u(\tfrac{t}{a}),$$

where a is a generator of a. The term under summation depends only upon t mod a, and since $a \neq (1)$

$$\rho_\chi(\eta(b)) = \frac{\phi(h)}{\phi(a)} \sum_{t\in B(a)} \bar{\chi}(t)u(t/a)$$

$$= \frac{\phi(h)}{\phi(a)}\, u(\bar{\chi}') \prod_{p|a} (1-\bar{\chi}'(p))$$

by lemma 2.7.

We now compute $\rho_\chi(\omega\alpha_a)$. First, $\rho_\chi(\omega) = u(\bar{\chi}')$ and $\rho_\chi(\bar{\sigma}_p) = \bar{\chi}'(p)$ for all primes p dividing a. Also $\rho_\chi(s(H_a)) = \sum_{\sigma\in H_a} \chi(\sigma)$ equals 0 if χ is nontrivial on H_a (in which case $\delta_\chi \nmid a$), or equals $|G|/|H_a| = \phi(h)/\phi(a)$ if χ is trivial on H_a (in which case $\delta_\chi | a$). It is now clear that

$$\rho_\chi(\eta(b)) = \rho_\chi(\omega\alpha_a)$$

for all nontrivial characters χ of G.

Upon noting that $\omega\alpha_1 = \omega s(G) = 0$, it follows that $(1-e_1)V = \omega.U$, q.e.d.

Lemma 2.11. U is contained in $\mathbb{Q}[G]$, and is isomorphic as an abelian group to $\mathbb{Z}^{|G|}$ (i.e. is free on $|G|$ generators).

Proof: Since $\bar{\sigma}_p$ and $s(H_a)$ (any a dividing h) both lie in $\mathbb{Q}[G]$, so do all the elements of U. Also U is finitely generated over $\mathbb{Z}[G]$, so it is free over $\mathbb{Z}$. It remains to determine its rank as an abelian group.

Let I be the subspace spanned by U; since U is a $\mathbb{Z}[G]$-module, I is an ideal of $\mathbb{Q}[G]$. To prove the lemma, it suffices to show that $I = \mathbb{Q}[G]$. If this were not the case, there would exist a character χ of G such that $\rho_\chi(I) = 0$ (since I is an ideal). Let χ be a character of G, with conductor a. Then, if $a \neq (1)$,

$$\rho_\chi(\alpha_a) = \frac{\phi(h)}{\phi(a)} \prod_{p|a} (1-\bar{\chi}'(p)).$$

But $\bar{\chi}'(p) = 0$ for any prime $p|a$, so $\rho_\chi(\alpha_a) \neq 0$. If, alternatively, $a = (1)$, then $\rho_\chi(\alpha_a) = \frac{\phi(h)}{e_K} \neq 0$. Hence $I = \mathbb{Q}[G]$, and the lemma is proven.

§3. Properties of elliptic units of H.

In this section, we discuss some properties of the elliptic units C of H. This will enable us to compute four of the five indices mentioned in §2; the remaining one $(R_o:U_o)$ will be calculated in the next section.

Lemma 2.12. Let $a\in P$. Then $a^{s(G)}\in\mu_K$ if and only if $a\in C$.

Proof: If $a\in C$, $a^{s(G)}$ is a unit of K, that is, a root of unity in K. On the other hand, suppose $a\notin C$. Since $a^{\sigma-1}\in C$ for each σ belonging to G, $a^{|G|} \equiv a^{s(G)} \bmod C$. Since a is not a unit, neither is $a^{s(G)}$, q.e.d.

Lemma 2.13. Let $a\in P$. Suppose that $a^{\sigma-1}\in\mu_H$ for every $\sigma\in G$. Then $\ell(a)$ lies in the group

$$\sum_{i=1}^{r} 12\log|\pi_i|\mathbb{Z}\, s(G).$$

(Recall that $(\pi_i) = p_i$ is a prime divisor of h).

Proof: If a is a unit, a^{e_H} is fixed by G and so is a unit of K; thus $a\in\mu_H$ and $\ell(a) = 0$. So suppose that a is not a unit. By lemma 1.5, a is of the form

$$\Delta(L)^k\, b^{12}$$

for some b in $K(E_h)$; thus $b^{\sigma-1}$ is a root of unity in $K(E_h)$ for every σ in $G(K(E_h)/K)$. Furthermore b is not a unit, for b^{12} has the same $\mathfrak{P}$-adic value as a for every prime $\mathfrak{P}$ of $K(E_h)$ not dividing $\mathfrak{f}$ (because at such primes $\Delta(L)$ is a unit). Let m be the least positive integer n satisfying $b^n\in K^x$. We claim that because $K(\mu_m,b)$ is abelian over K, and b is not a unit, m must divide e_K. (This will be proved in the following lemma). Thus $b^{\sigma-1}$ lies in μ_K for every $\sigma\in G(K(E_h)/K)$.

Consider a prime p_i (i = 1,...,r) dividing h. Recall that $p_i^{e_i}$ is the exact power of p_i dividing h; let $g_i = hp_i^{-e_i}$. The extension $K(E_h)/K(E_{g_i})$ is totally ramified at all primes $\mathfrak{P}$ of $K(E_{g_i})$ which divide p_i. Thus for any prime $\mathfrak{P}_1$ of $K(E_h)$ above p_i and any $\sigma \in G(K(E_h)/K(E_{g_i}))$, we have

$$b^{\sigma-1} \equiv 1 \bmod \mathfrak{P}_1.$$

Since $(\mathfrak{P}_1, e_K) = 1$, and $b^{\sigma-1} \in \mu_K$, we conclude that $b^{\sigma-1} = 1$ and $b \in K(E_{g_i})$. Thus b lies in $\bigcap_{i=1}^{r} K(E_{g_i}) = K$.

Hence a lies in K. For any prime p_i dividing h, its p_i-adic value is the 12-th power of that of b, and it is a unit at all other primes not dividing h. Thus the fractional ideal (a) factorizes in the form $(\prod_{i=1}^{r} p_i^{n_i})^{12}$ for some integers n_i; hence $\ell(a) \in \sum_{i=1}^{r} 12 \log|\pi_i| \mathbb{Z}\, s(G)$; this completes the proof of lemma 2.13.

We now prove the result quoted in the proof of the preceding lemma.

Lemma 2.14. Let m be the least positive integer n satisfying $\beta^n \in K^x$. If the extension $K(\mu_m, \beta)/K$ is abelian, and if β is not a root of unity, then $\mu_m \subseteq K$.

Proof: Let $\Delta = G(K(\mu_m)/K)$; Δ acts on μ_m and defines an injection $\chi: \Delta \hookrightarrow (\mathbb{Z}/m\mathbb{Z})^x$. On the other hand, Δ acts on $G(K(\mu_m, \beta)/K(\mu_m))$, via inner automorphisms, and it is clear from Kummer theory, and the fact that $\alpha = \beta^m$ lies in K, that Δ acts on $G(K(\mu_m, \beta)/K(\mu_m))$ via the character χ. But as $K(\mu_m, \beta)/K$ is abelian, this action is trivial, so $\chi = 1$ and $\Delta = 1$, q.e.d.

The next lemma establishes the connection between $\ell(P)$ and $\ell(C)$. Its proof uses the condition imposed on h at the beginning of this chapter, namely that h is not divisible by both an unramified split prime p and its conjugate $\bar{p}$. For brevity we denote $\ell(P)$ by T. Recall that for an R-module A, A_o denotes the submodule of A annihilated by s(G), and A^G the submodule fixed by G.

Lemma 2.15. $\ell(C) = T_o$.

Proof: By lemma 2.12, $s(G)\ell(C) = \ell(C^{s(G)}) = 0$, so that $\ell(C) \subseteq T_o$. For the reverse inclusion, consider an a in P with $\ell(a)$ in T_o. Then $\ell(a^{s(G)}) = 0$, and so $|a^{s(G)}| = 1$. Let $b = a^{s(G)}$; it lies in K^x and satisfies $b\bar{b} = 1$. The fractional ideal (b) factorizes as a product of unramified split prime ideals $q_1,\ldots,q_s$ of K and their conjugates $\bar{q}_1,\ldots,\bar{q}_s$ in the form

$$(q_1\bar{q}_1^{-1})^{n_1} \ldots (q_s\bar{q}_s^{-1})^{n_s},$$

for some integers $n_1,\ldots,n_s$. Because a lies in P, for each i, either the ideal q_i and its conjugate $\bar{q}_i$ must divide h, or $n_i = 0$. But since h is not divisible by $p\bar{p}$ for any unramified split prime p of K, we conclude that b lies in μ_K; by lemma 2.12, a must lie in C. This proves the lemma.

The next lemma computes one of the indices (described in §2) to be used in the proof of theorem 1.

Lemma 2.16. $T_o = T \cap (1-e_1)T$. Furthermore, T_o has finite index in $(1-e_1)T$, equal to $\phi(h)/e_K^r$.

Proof: Since $s(G)(1-e_1)T = 0$, T_o contains $T \cap (1-e_1)T$. Conversely, if $x \in T_o$, $(1-e_1)x = x$, so that $T_o \subseteq (1-e_1)T$. Hence $T_o = T \cap (1-e_1)T$.

Now $(1-e_1)T/T_o \simeq (1-e_1)T+T/T$

$\simeq e_1T+T/T \simeq e_1T/T^G$,

since $(1-e_1)T+T = e_1T+T$ and $e_1T\cap T = T^G$. The groups e_1T and T^G may be explicitly computed.

First, $e_1T = \frac{s(G)}{|G|}\,\ell(P) = \frac{e_K}{\phi(h)}\,\ell(P^{s(G)})$.

Lemma 1.12 shows that

$$\ell(P^{s(G)}) = \sum_{i=1}^{r} 12\,\frac{\phi(h)}{\phi(p_i^{e_i})}\log|\pi_i|\,s(G)\mathbb{Z}\ .$$

Now consider T^G. Let $a\in P$: then $\ell(a)\in T^G$ if and only if $(\sigma-1)\ell(a) = \ell(a^{\sigma-1}) = 0$ for every $\sigma\in G$. Fix $\sigma\in G$. Then $a^{\sigma-1}$ is a unit in H (an elliptic unit!), and lies in the kernel of ℓ: hence it is a root of unity. By lemma 2.13, $\ell(a)$ lies in the group $\sum_{i=1}^{r} 12\log|\pi_i|\mathbb{Z}\,s(G)$. We now show that T^G is precisely the group $\sum_i 12\log|\pi_i|\mathbb{Z}\,s(G)$; for each i, we produce an element $a_{p_i}\in P$ such that $\ell(a_{p_i}) = 12\log|\pi_i|s(G)$. Choose ideals $a_1,\ldots,a_s$ of K prime to $6h$ and integers $n_1,\ldots,n_s$ such that $\sum_{j=1}^{s} n_j(Na_j-1) = e_K$. Let

$$b_{p_i} = \prod_{j=1}^{s}\Theta(\tfrac{\Omega}{\pi_i},a_j,L)^{n_j},$$

and $a_{p_i} = N_{K(p_i)/K}b_{p_i}$. Lemma 1.12 shows that a_{p_i} generates the ideal p_i^{12} in K, as required.

It is now clear that $(1-e_1)T/T_o$ is finite, and has order $\prod_{i=1}^{r}\frac{\phi(p_i^{e_i})}{e_K} = \frac{\phi(h)}{e_K^r}$. This concludes the proof of lemma 2.16.

The next lemma computes another index required for the proof of theorem 1, namely $[(1-e_1)V: (1-e_1)T]$. Recall that the set S is the collection of 2^r-1 divisors of h generated by products of

the ideals $p_1^{e_1},\ldots,p_r^{e_r}$, omitting (1); the element w was defined in the introduction to be $e_K^{-r}\prod_{b\in S} e_{R(b)}$. Let $w_1 = [(1-e_1)V:(1-e_1)T]$.

Lemma 2.17. The index w_1 divides w; if h is a prime power,

$$w_1 = w = e_H/e_K.$$

Proof: Let $g \neq (1)$ be a divisor of h with generator g; let $b = (b)$ be the largest divisor of h divisible only by those primes dividing g. Consider a nontrivial ideal a of K, prime to $6h$, in the principal ray class mod h. Then by lemma 1.7 (or lemma 1.15),

$$\eta(hg^{-1}) = (Na-1)^{-1}\ell(\Theta(\tfrac{\Omega}{g},a,L))$$

$$= (Na-1)^{-1}\ell(N_{R(b)/R(g)}\Theta(\tfrac{\Omega}{b},a,L));$$

this last item is equal to the sum of the distinct elements in the set $\{\sigma\eta(hb^{-1});\ \sigma\in G(H/R(g))\}$. Thus V is generated as an R-module by the set $\{\eta(hb^{-1});\ b\in S\}$. Furthermore, if t is an integer prime to $6h$,

$$Nt.\eta(hb^{-1}) - [t,H/K]\eta(hb^{-1})\in T,$$

so that $$V \simeq T + \sum_{b\in S}\eta(hb^{-1})\mathbb{Z}.$$

The group $V' = \sum_{b\in S}\eta(hb^{-1})\mathbb{Z}$ is, in fact, a direct sum. For suppose there are integers a_b such that $\sum_{b\in S} a_b\eta(hb^{-1}) = 0$. We show by induction on the number s of distinct prime factors of hb^{-1}, that each $a_b = 0$. Consider the case $s = 0$. Choose a character χ of G with conductor $\mathfrak{f}_\chi = h$, and apply ρ_χ to the sum $\sum_b a_b\eta(hb^{-1})$. The proof of lemma 2.7 showed that $\rho_\chi(\eta(hb^{-1}))$ equals 0 unless

$b = h$, in which case it equals $u(\bar{\chi}')$ (which is not 0). Thus $a_h = 0$. Now suppose inductively that $a_b = 0$ for all divisors $b \in S$ such that hb^{-1} has at most s distinct prime factors. Consider a divisor $b_1 \in S$ such that hb_1^{-1} has s+1 distinct prime factors. Choose a character χ of G with conductor $\mathfrak{f}_\chi = b_1$. The proof of lemma 2.7 shows that for each $b \in S$, $\rho_\chi(\eta(hb^{-1})) = 0$ if $\mathfrak{f}_\chi$ does not divide b, and otherwise equals $\frac{\phi(h)}{\phi(b)} u(\bar{\chi}') \prod_{p \mid b} (1-\bar{\chi}'(p))$.

Now $\rho_\chi(\eta(hb_1^{-1})) = \frac{\phi(h)}{\phi(b_1)} u(\bar{\chi}')$ because $\chi'(p) = 0$ for each prime p dividing $b_1 = \mathfrak{f}_\chi$; it is not zero (by the class number formula!). The inductive hypothesis implies that

$$\rho_\chi\Big(\sum_{b \in S} a_b \eta(hb^{-1})\Big) = \sum_{\substack{b \in S \\ b_1 \mid b}} a_b \rho_\chi(\eta(hb^{-1}))$$

$$= a_{b_1} \frac{\phi(h)}{\phi(b_1)} u(\bar{\chi}'),$$

because b_1 is the unique divisor b in S which is divisible by b_1 and that hb^{-1} has s+1 distinct prime factors. We deduce that $a_{b_1} = 0$; by induction $a_b = 0$ for all $b \in S$, and we obtain a direct sum

$$V' = \bigoplus_{b \in S} \eta(hb^{-1})\mathbb{Z} .$$

Thus $V/T \simeq V'/V' \cap T$ has order dividing

$$\prod_{b \in S} e_{R(b)} ,$$

since $e_{R(b)}$ is the least integer n_b such that $n_b \eta(hb^{-1})$ lies in T; in that case that h is a prime power, $S = \{h\}$, and V/T has order precisely e_H.

Thus the index $(V:T)$ is defined; lemma 2.9 shows that $((1-e_1)V:(1-e_1)T)$ is defined and equals $(V:T)(V^G:T^G)^{-1}$ (since $e_1V\cap V = V^G$, $e_1T\cap T = T^G$). The preceding lemma showed that $T^G = \bigoplus_{i=1}^{r} 12\log|\pi_i|\mathbb{Z}\, s(G)$; we claim that $T^G = e_KV^G$. If $x\in V^G$, choose ideals a prime to $6h$, and integers n_a such that $\sum_a n_a(Na-1) = e_K$. Then

$$\sum_a n_a(Na-[a,H/K])\ x \text{ lies in } T;$$

since $x = e_1x$, this sum equals $e_Ke_1x = e_Kx$ and lies in e_1T; we conclude that $e_Kx\in T\cap e_1T = T^G$, so that $e_KV^G \subseteq T^G$. Conversely, choosing an ideal a in the principal ray class mod h, we have

$$\sum_{t\in B(p_i)} u\left(\frac{t}{\pi_i}\right) = (Na-1)^{-1}\ell\left(N_{R(p_i)/K}\Theta\left(\frac{\Omega}{\pi_i}, a, L\right)\right)$$

$$= \ell(\pi_i^{12/e_K}) = 12e_K^{-1}\log|\pi_i|s(G);$$ we conclude that $T^G = e_KV^G$.

Thus $(V^G:T^G) = e_K^r$, and the lemma follows immediately.

We have calculated most of the indices to be used in the proof of theorem 1; we gather together these results now.

Theorem 1. C has finite index in S, equal to

$$12^{[H:K]-1}h_Hw_1(R_o:U_o)\phi(h)/e_K^r\cdot e_K/e_H$$

where w_1 is the divisor of w defined above.

Proof: As noted earlier, $S/C \simeq \ell(S)/\ell(C)$. Both $\ell(S)$ and $\ell(C)$ lie in the subspace $X = (1-e_1)\mathbb{R}[G]$ (For if $a\in S$, $e_1\ell(a) = |G|^{-1}\ell(a^{s(G)}) = 0$). Thus formally at least,

$$(\ell(S):\ell(C)) = (\ell(S):R_o)(R_o:U_o)(U_o:(1-e_1)V)((1-e_1)V:(1-e_1)T)((1-e_1)T:T_o)$$

where we recall that $T_o = \ell(C)$. In fact, each of the groups appearing is a lattice in X; in the course of the proof this will be demonstrated for each index separately. The last two indices have already been calculated in the preceding two lemmas; also lemma 2.11 shows that $(R_o:U_o)$ is defined, for the span of each of R_o and U_o is X, they are discrete, lie inside $\mathbb{Q}[G]$, and are finitely generated over $\mathbb{Z}$. It remains to consider the first and third indices.

Let $m = [H:K]-1$. The dimension of X over $\mathbb{R}$ is equal to m; the $\mathbb{Z}$-rank of $\ell(S) \simeq S/\mu_H$ is also equal to m (for H is an extension of an imaginary quadratic field, of degree m+1). The elements $-(\sigma^{-1}-1)$, where σ varies over the nontrivial elements of G, form a basis for R_o over $\mathbb{Z}$ (if $x = \sum_\sigma a_\sigma \sigma^{-1}$ lies in R_o, then $\sum_\sigma a_\sigma = 0$, so that $x = \sum_\sigma a_\sigma(\sigma^{-1}-1)$); hence they form a basis for X over $\mathbb{R}$.

Let $\eta_1,\ldots,\eta_m$ be a system of fundamental units of H. Then for each i,

$$\ell(\eta_i) = \sum_\sigma - \log|\eta_i^\sigma|\sigma^{-1} = \sum_{\sigma\neq 1} - \log|\eta_i^\sigma|(\sigma^{-1}-1)$$

in terms of the specified basis of X. Label the nontrivial elements of G as $\sigma_1,\ldots,\sigma_m$. Now the absolute value of the determinant of the m×m matrix, whose entry in the i^{th} row and j^{th} column is

$$\log|\eta_j^{\sigma_i}|,$$

is 2^{-m} times the absolute value of the regulator R_H of H. Since $R_H \neq 0$, $\ell(S)$ is a lattice in X and

$$(R_o:\ell(S)) = 2^{-m}|R_H|$$

so that $$(\ell(S):R_o) = 2^m|R_H^{-1}|.$$

We now turn to the third index $(U_o:(1-e_1)V)$. Clearly $(1-e_1)V \subseteq X$, and it has been shown in lemma 2.10 that $(1-e_1)V = \omega.U$. We first prove that $(1-e_1)U = U_o$. Let a be any divisor of h, and let

$$\alpha_a = s(H_a) \prod_{p|a} (1-\bar{\sigma}_p)$$

be a typical generator of U. For any character χ of G, $e_\chi \bar{\sigma}_p = \bar{\chi}'(p) e_\chi$; in particular, $e_1 \bar{\sigma}_p = e_1$. Hence $e_1 \alpha_a = 0$ if $a \neq (1)$; also $e_1 \alpha_1 = s(G)$. Let

$$\alpha = \sum_{a|h} g_a \alpha_a$$

be a typical element of U ($g_a \in R$). Then α lies in U_o precisely if $s(G) g_1 \alpha_1 = 0$, or equivalently if $g_1 \alpha_1 = 0$. Furthermore, $g_1 s(G) \in \mathbb{Z}\, s(G)$. Then U_o is the R-module generated by the elements α_a with $a \neq (1)$, and $U = U_o + s(G)\mathbb{Z}$. Hence $(1-e_1)U = U_o$, as was to be shown. Let A be the linear transformation on X induced by multiplication with ω:

$$Ax = \omega x \text{ for each } x \in X.$$

Then, by lemma 2.10, $A(U_o) = (1-e_1)V$. Let $A_{\mathbb{C}}$ be the $\mathbb{C}$-linear extension of A to $(1-e_1)\mathbb{C}[G]$. Since the idempotents e_χ, for nontrivial characters χ of G, form a basis for $(1-e_1)\mathbb{C}[G]$, and

$$A_{\mathbb{C}}(e_\chi) = \omega e_\chi = u(\bar{\chi}')e_\chi,$$

we conclude that $\det A = \det A_{\mathbb{C}} = \prod_{\chi \neq 1} u(\bar{\chi}')$. By the class number formula, $\det A \neq 0$. Hence $(1-e_1)V$ is a lattice in X, and $(U_o:(1-e_1)V) = \left| \prod_{\chi \neq 1} u(\bar{\chi}') \right|$.

Combining these calculations gives

$$[S:C] = 2^{[H:K]-1}|R_H|^{-1}.(R_o:U_o).\prod_{\chi\neq 1}|u(\bar{\chi}')| \quad w_1.\phi(h)/e_K^r$$

$$= 12^{[H:K]-1}h_H.w_1 \ (R_o:U_o).\phi(h)/e_K^r.\ e_K/e_H$$

by the class number formula. This completes the present calculations. The calculation of $(R_o:U_o)$ will be performed in the next section.

Remark. If the restriction $(h,6) = 1$ is removed, extra factors divisible by 2 or 3 enter the formula, but these come entirely from the index $(U_o:(1-e_1)V)$ and can be compensated for by using the slightly larger group of elliptic units mentioned on page 35, and modifying the definition of V. In particular, the calculation of the next section is unaffected by the removal of this restriction.

§4. The calculation of $(R_o:U_o)$.

In this section we calculate the index $(R_o:U_o)$ by computing various indices in subspaces of $\mathbb{C}[G_1]$, where we recall that $G_1 = G(K(E_h)/K)$. Throughout, let J denote the subgroup of G_1 fixing H ($J = G(K(E_h)/H)$); it is cyclic of order e_K, and let j be a generator of J. Let s(J) denote the group norm $\sum_{\sigma \in J} \sigma$ in R_1, and $e_J = s(J)/e_K$; the natural surjection $G_1 \longrightarrow G$ induces two isomorphisms $e_J R_1 \simeq R$ and $e_J \mathbb{C}[G_1] \simeq \mathbb{C}[G]$. Let ξ be a character of G_1, and consider the idempotent ε_ξ in $\mathbb{C}[G_1]$ associated to ξ. We note that $e_J \varepsilon_\xi = 0$ if ξ is nontrivial on J; otherwise ξ induces a character χ of G, and $e_J \varepsilon_\xi = e_\chi$ is the idempotent in $\mathbb{C}[G]$ attached to χ.

For any divisor a of h, let $L_a = G(K(E_h)/K(E_a))$ and let $s(L_a) = \sum_{\sigma \in L_a} \sigma$ be its group norm in R_1. For any prime p dividing h, let

$$\bar{\Sigma}_p = \sum_{\xi} \bar{\xi}'(p)\varepsilon_\xi,$$

the sum being taken over all characters ξ of G_1. Let W be the R_1-module generated by the elements

$$\beta_a = s(L_a) \prod_{p \mid a} (1-\bar{\Sigma}_p)$$

where p varies over all prime divisors of a, and a varies over all divisors of h. It is easily seen that $e_J W \simeq U$; the index $(R_o:U_o)$ will be evaluated by considering the index $(R_1:W)$.

For a given R_1-module A, denote by A_o (resp. A_J) the submodule of A annihilated by $s(G_1)$ (resp. s(J)); denote by A^{G_1} (resp. A^J) the submodule of A fixed by G_1 (resp. J). We will see that

$$(R_{1,o}:W_o) = (e_J R_{1,o}:e_J W_o)((R_{1,o})_J:(W_o)_J)$$

and $(e_J R_{1,o}:e_J W_o) = (R_o:U_o)$. (Here $R_{1,o}$ denotes $(R_1)_o$).

The following lemma shows that the index $(R_1:W)$ is defined.

Lemma 2.18. W is contained in $\mathbb{Q}[G_1]$ and is isomorphic, as an abelian group, to $\mathbb{Z}^{|G_1|}$.

Proof: It is easy to check that $\bar{\Sigma}_p$ lies in $\mathbb{Q}[G_1]$ (any prime p); hence so does W. Also W is finitely generated over R_1, and so is free over $\mathbb{Z}$. It remains to determine its rank as an abelian group. To prove the lemma it suffices to show that the subspace I of $\mathbb{Q}[G_1]$ spanned by W is, in fact, $\mathbb{Q}[G_1]$ itself. If this were not the case, since I is an ideal, there would exist a character ξ of G_1 such that $\rho_\xi(I) = 0$. Let a be the greatest common divisor of its conductor $\mathfrak{f}_\xi$ (which divides $\mathfrak{f}h$) and h. Then $\rho_\xi(\beta_a) = |L_a| \prod_{p|a} (1-\bar{\xi}'(p))$; since $\bar{\xi}'(p) = 0$ for any prime p dividing a, $\rho_\xi(\beta_a) \neq 0$. Thus $I = \mathbb{Q}[G_1]$, q.e.d.

For any prime p which divides h, let T_p be the inertia group of p in G_1: so for $i = 1,\ldots,r$, T_{p_i} fixes $K(E_{hp_i}-e_i)$. Further let $W_p = R_1 s(T_p)+R_1(1-\bar{\Sigma}_p)$, and let W' be the R_1-module generated by products $\prod_{i=1}^{r} w_{p_i}$ where $w_{p_i} \in W_{p_i}$. We claim that $W = W'$.

Proof: G_1 is the internal direct product of its inertia groups T_p, where p varies over all prime divisors of h. W' is generated by the elements

$$\beta_S = \prod_{p\in S} s(T_p) \prod_{\substack{p|h \\ p\notin S}} (1-\bar{\Sigma}_p),$$

as S varies over all subsets of the set of primes p dividing h. Given such a subset S, let g be the largest divisor of h not divisible by any prime of S. $K(E_g)$ is the largest subfield of $K(E_h)$ unramified at the prime of S, so that it is the fixed field of the subgroup $\prod_{p\in S} T_p$ of G_1. Hence

$$L_g = \prod_{p\in S} T_p,$$

so that $$s(L_g) = \prod_{p\in S} s(T_p) \text{ in } R_1.$$

Therefore $\beta_S = s(L_g) \prod_{p|g} (1-\bar{\Sigma}_p)$, and hence $W' \subseteq W$.

On the other hand, let g be a divisor of h, and we now show that

$$\beta_g = s(L_g) \prod_{p|g} (1-\bar{\Sigma}_p) \in W'.$$

Let S be the set of primes dividing h but not g. Since $K(E_g)$ is unramified at each $p\in S$, $\prod_{p\in S} T_p \subseteq L_g$. Hence

$s(L_g) = \beta . s(\prod_{p\in S} T_p) = \beta \prod_{p\in S} s(T_p)$ for some $\beta\in R_1$. Thus

$$\beta_g = \beta . \prod_{p\in S} s(T_p) \prod_{\substack{p|h \\ p\notin S}} (1-\bar{\Sigma}_p) = \beta . \beta_S$$

lies in U'. This concludes the proof of the claim.

We can describe the element $\bar{\Sigma}_p$ more explicitly. For any $i = 1,\ldots,r$, let $e_{p_i} = s(T_{p_i})/|T_{p_i}|$; then e_{p_i} is idempotent in $\mathbb{Q}[G_1]$. Choose an integer t prime to ℓh such that

$$t \equiv 1 \bmod p_i^{e_i}$$

$$t \equiv \pi_i \bmod \ell h p_i^{-e_i};$$

let λ_{p_i} be the restriction of $[t,R(\mathfrak{f}h)/K]$ to $K(E_h)$. We claim that $\bar{\Sigma}_{p_i} = \lambda_{p_i}^{-1} e_{p_i}$. To see this, consider a character ξ of G_1. If ξ is nontrivial on T_{p_i} (equivalently if p_i divides $\mathfrak{f}_\xi$), $\rho_\xi(e_{p_i}) = 0$; otherwise, p_i does not divide $\mathfrak{f}_\xi$, $\mathfrak{f}_\xi$ divides $\mathfrak{f}hp_i^{-e_i}$ and $\rho_\xi(e_{p_i}) = 1$, so that $\rho_\xi(\lambda_{p_i}^{-1} e_{p_i}) = \bar{\xi}(t) = \bar{\xi}'(\pi_i)$. Since $\rho_\xi(\bar{\Sigma}_{p_i}) = \bar{\xi}'(p_i)$, in either case we obtain $\rho_\xi(\lambda_{p_i}^{-1} e_{p_i}) = \rho_\xi(\bar{\Sigma}_{p_i})$, and so prove the claim.

We introduce some notational conventions which will remain in force throughout this section. Let h_1 be the product of the primes dividing h. The symbols g and g' will be reserved for divisors of h_1; such divisors correspond in an obvious way to subsets of the set of primes dividing h. The symbol p will always denote a divisor of h.

For any g, let W_g denote the R_1-module generated by the products $\prod_{p|g} x_p$ where each x_p lies in W_p; let T_g denote the product $\prod_{p|g} T_p$; we have $T_{h_1} = G_1$ and, by convention $W_1 = R_1$, $T_1 = \{1\}$. It is clear that each W_g is contained in $\mathbb{Q}[G_1]$, and furthermore is free, of rank $|G_1|$ over $\mathbb{Z}$. [For it suffices to show, as in lemma 2.18, that for each character ξ of G_1, $\rho_\xi(W_g) \neq 0$. Let $a = (\mathfrak{f}_\xi, g)$. The element $x = \prod_{\substack{p|g \\ p+a}} s(T_p) \prod_{p|a} (1-\bar{\Sigma}_p)$ lies in W_g and $\rho_\xi(x) = \prod_{\substack{p|g \\ p\nmid a}} |T_p| \neq 0$, so that $\rho_\xi(W_g) \neq 0$].

We view W as being formed from $W_1 = R_1$ by multiplying successively with the modules W_p for each p: most of what we prove arises by comparing the module W_g and W_{pg}, where $p\nmid g$.

W_{pg} is generated by the products $x_p x_g$ where $x_p \in W_p$, $x_g \in W_g$. The main tool for comparison is a pair of exact sequences defined as follows.

Since e_p is idempotent, $e_p(1-e_p) = 0$. Thus $(1-e_p)s(T_p) = 0$ and $(1-e_p)(1-\bar{\Sigma}_p) = (1-e_p)$, since $\bar{\Sigma}_p = \lambda_p^{-1} e_p$. Hence $(1-e_p)W_p = (1-e_p)R_1$, so that $(1-e_p)W_{gp} = (1-e_p)W_g$, if $p \nmid g$. If A is any R_1-submodule of $\mathbb{Q}[G_1]$, we denote by A^{T_p}, the set of elements of A left fixed by T_p: an element $a \in A$ is fixed by T_p if and only if $(1-e_p)a = 0$. Therefore we have a pair of exact sequences of R_1-modules:

$$(1) \qquad 0 \longrightarrow W_g^{T_p} \longrightarrow W_g \longrightarrow Y \longrightarrow 0$$

$$(2) \qquad 0 \longrightarrow W_{gp}^{T_p} \longrightarrow W_{gp} \longrightarrow Y \longrightarrow 0,$$

where $Y = (1-e_p)W_g = (1-e_p)W_{gp}$, and the surjections in (1) and (2) are induced by mult. with $(1-e_p)$. We begin with two simple lemmas.

Lemma 2.19. Let H be a subgroup of G_1 such that

$$H \cap T_p = \langle 1 \rangle.$$

Let A be a HT_p submodule of $\mathbb{Q}[G_1]$, and suppose A is free over HT_p. Then A^{T_p} and $(1-e_p)A$ are both free over H.

This lemma is proved in a similar manner to that of Sinnott ([25], lemma 5.1).

Lemma 2.20. Let A be an R_1-module of $\mathbb{Q}[G_1]$. Then

$(AW_p)^{T_p} = s(T_p)A + (1-\lambda_p^{-1})A^{T_p}$. Hence if A is free over T_p,

$(AW_p)^{T_p} = A^{T_p} = s(T_p)A$.

[AW_p denotes the R_1-module generated by products au where $a \in A$, $u \in W_p$].

Proof: The second statement is immediate from the first. To prove the first, let a be any element of AW_p. Since $W_p = s(T_p)R_1+(1-\bar{\Sigma}_p)R_1$, we may write $a = s(T_p)b+(1-\bar{\Sigma}_p)c$ with $b,c\in A$. Now $(1-e_p)a = (1-e_p)c$; so a lies in $(AW_p)^{T_p}$ if and only if $(1-e_p)c = 0$, i.e. $c\in A^{T_p}$. Since $(1-\bar{\Sigma}_p)c = (1-\lambda_p^{-1})c$ if $c\in A^{T_p}$, the lemma follows.

Lemma 2.21. If g and g' are relatively prime, then W_g is a free $T_{g'}$-module; if in addition, $gg' \neq h_1$, then W_g is a free $JT_{g'}$ module.

Proof: The proof proceeds by induction on g. If $g = 1$, $W_g = R_1$ is free over any subgroup of G_1. Now let g be a divisor of h_1, not equal to h_1, and suppose the proposition is true for g. Let p be prime to g and let g' be prime to gp. We show that W_{gp} is free over $T_{g''}$, and is free over $JT_{g'}$, if $gpg' \neq h_1$.

Since pg' is prime to g, W_g is free over $T_{pg'}$; since $p\nmid g'$, $T_p\cap T_{g'} = \langle 1\rangle$. Hence by lemma 2.19, $(1-e_p)W_g$ is free over $T_{g'}$. The sequences (1) and (2) split over $T_{g''}$, and

$$W_g \simeq W_g^{T_p} \oplus (1-e_p)W_g$$

$$W_{gp} \simeq W_{gp}^{T_p} \oplus (1-e_p)W_g$$

as $T_{g'}$-modules. Since $p\nmid g$, W_g is free over T_p. By lemma 2.20, $W_{gp}^{T_p} = W_g^{T_p}$, and thus $W_g \simeq W_{gp}$ as $T_{g'}$-modules. Hence W_{gp} is free over $T_{g''}$, as desired.

Suppose $gpg' \neq h_1$; then $J\cap T_{gpg'} = \langle 1\rangle$. Now W_g is free over $JT_{pg'}$ (by our inductive hypothesis) i.e. over $T_p.JT_{g'}$, and , $T_p\cap JT_{g'} = \langle 1\rangle$, and lemma 2.19 implies that $(1-e_p)W_g$ is free over $JT_{g'}$. The sequences (1) and (2) split over $JT_{g''}$, and $W_g \simeq W_{gp}$

as JT_g,-modules, because $W_g^{T^p} = W_{gp}^{T^p}$. Hence W_{gp} is free over JT_g,, q.e.d.

This lemma will be used to compute cohomology groups arising from the modules W_g; these cohomology groups will be used in the last part to determine the index $(R_o:U_o)$. A general reference is [21] ch.8.

Let A be a G_1-module, and G_2 a subgroup of G_1. For any $\sigma \in G_1$, the endomorphism of A induced by multiplication with σ is a G_2-endomorphism, since G_1 is abelian. Thus σ induces an endomorphism σ^* of the cohomology group $H^q(G_2,A)$ for any $q \geq 0$. We thus obtain an action of G_1 on $H^q(G_2,A)$ which makes $H^q(G_2,A)$ into a G_1-module. The following properties of this G_1-module structure are immediately verified:

(1) If $f: A \longrightarrow B$ is a G_1-map, so is the induced map $f^*: H^q(G_2,A) \longrightarrow H^q(G_2,B)$.

(2) If $0 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 0$ is an exact sequence of G_1-modules, the connecting homomorphism

$$\delta: H^q(G_2,C) \longrightarrow H^q(G_2,A)$$

is a G_1-map.

(3) If $G_2 \subseteq G_3$ are subgroups of G_1, then

$$\text{Res}: H^q(G_3,A) \longrightarrow H^q(G_2,A)$$

is a G_1-map. Moreover if we make

$$H^q(G_3/G_2, A^{G_2})$$

into a G_1-module in the same way as above, via the G_1-module structure on A^{G_2}, then $\text{Inf}: H^q(G_3/G_2,A^{G_2}) \longrightarrow H^q(G_3,A)$ is also a G_1-map.

Lemma 2.22. Let g,g' be relatively prime, and suppose neither g nor g' equals h_1. Then for all $q > 0$,

$$H^q(T_g,,W_g^J) \simeq H^q(JT_g,,W_g) \simeq H^q(J,W_g^{T_{g'}}).$$

These are G_1-module isomorphisms. Moreover, the groups are trivial unless $gg' = h_1$.

Proof: The final statement is immediate from lemma 2.21, for if $gg' \neq h_1$, W_g is free over $JT_g,$, and thus

$$H^q(JT_g,,W_g) = 0.$$

We prove the first isomorphism. Since $g \neq h_1$, W_g is free over J by lemma 2.21 and so $H^q(J,W_g) = 0$ for all $q > 0$. Hence inflation gives an isomorphism of G_1-modules

$$H^q(JT_g,/J,W_g^J) \simeq H^q(JT_g,,W_g)$$

for all $q > 0$. Since $g' \neq h_1$, $J \cap T_g, = \langle 1 \rangle$ and we may identify $JT_g,/J \simeq T_g,$.

The second isomorphism is similar. By lemma 2.21 again, W_g is free over $T_g,$, so that $H^q(T_g,,U_g) = 0$ for any $q > 0$. Hence inflation gives an isomorphism of G_1-modules

$$H^q(JT_g,/T_g,,W_g^{T_{g'}}) \simeq H^q(JT_g,,W_g)$$

for all $q > 0$. Since $g' \neq h_1$, we may identify $J \simeq JT_g,/T_g,$. This completes the proof.

For any $q > 0$, and any g, let $g' = h_1 g^{-1}$ and write, for brevity,

$$A_g^q = H^q(J,W_g^{T_{g'}}).$$

Since $gg' = h_1$, these groups might not be trivial: we shall determine the structure of these G_1-modules.

Lemma 2.23. A_g^q has exponent dividing e_K, and G_1 acts trivially on A_g^q.

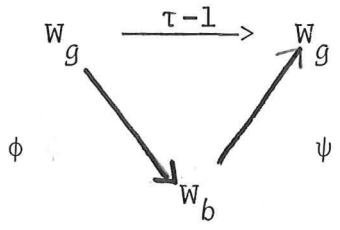
Proof: Since J has order e_K, we certainly have $e_K.A_g^q = 0$. To see that G_1 acts trivially on A_g^q, it suffices to show that T_p acts trivially, for each p.

If p does not divide g, p must divide $g' = h_1 g^{-1}$. Then T_p acts trivially on $W_g^{T_{g'}}$, and therefore acts trivially on A_g^q for all $q > 0$.

If p divides g, let $g = pb$ for some divisor b of h_1. Now W_g is the R_1-module generated by products $x_p x_b$ where $x_p \in W_p$, $x_b \in W_b$. Thus

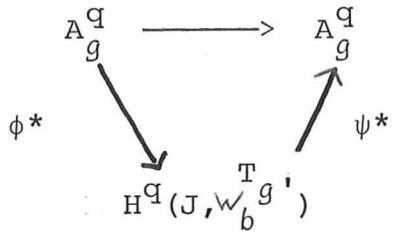
$$W_g = s(T_p)W_b + (1-\bar{\Sigma}_p)W_b.$$

Let τ belong to T_p. Then $(\tau-1)W_g \subseteq W_b$, because $(\tau-1)\,s(T_p) = 0$ and $(\tau-1)(1-\bar{\Sigma}_p) = (\tau-1)$. We obtain a commutative diagram of G_1-modules:



Here ϕ is the map induced by multiplication by $\tau-1$, and ψ is the map induced by multiplication by $1-\bar{\Sigma}_p$. Since $(\tau-1)(1-\bar{\Sigma}_p) = (\tau-1)$, $\psi \circ \phi$ is simply the endomorphism of W_g induced by multiplication with $\tau-1$. All of these maps are G_1-maps. Let $g' = h_1 g^{-1}$. Taking $T_{g'}$-invariants, and applying the functor $H^q(J, \ )$ we obtain a

second commutative diagram



(ϕ^*, ψ^* denote the maps induced by ϕ and ψ). However, by lemma 2.22, $H^q(J, W_b^{T_{g'}}) = 0$, since $g'b = p^{-1}h_1 \neq h_1$. Hence $\psi^* \circ \phi^* = 0$ i.e. $(\tau-1)A_g^q = 0$. Thus T_p acts trivially on A_g^q; the proof is concluded.

The next lemma enables us to determine the order of the group A_g^q.

Lemma 2.24. Suppose that p does not divide g. For any integer $q > 0$, there is an exact sequence

$$0 \longrightarrow A_g^q \longrightarrow A_{gp}^q \longrightarrow A_{gp}^{q+1} \longrightarrow 0.$$

Proof: We use the basic exact sequences (1) and (2). Since $(1-\bar{\Sigma}_p)W_g \subseteq W_{gp}$, there is a G_1-map $\beta: W_g \longrightarrow W_{gp}$ induced by multiplication by $1-\bar{\Sigma}_p$. From this, and the sequences (1) and (2), we obtain the following commutative diagram, with exact rows:

$$(3) \qquad \begin{array}{ccccccccc} 0 & \longrightarrow & W_g^{T_p} & \longrightarrow & W_g & \longrightarrow & Y & \longrightarrow & 0 \\ & & \downarrow \alpha & & \downarrow \beta & & \downarrow \gamma & & \\ 0 & \longrightarrow & W_{gp}^{T_p} & \longrightarrow & W_{gp} & \longrightarrow & Y & \longrightarrow & 0 \end{array}$$

Here $Y = (1-e_p)W_g$, and α and γ are the maps induced by β. Since $p \nmid g$, W_g is free over T_p (by lemma 2.21); hence $W_{gp}^{T_p} = W_g^{T_p}$ (lemma 2.20). Since $1-\bar{\Sigma}_p = 1-\lambda_p^{-1}e_p$, α is the map induced by multiplication with $1-\lambda_p^{-1}$, and γ is the identity map on Y.

Let $g' = h_1 g^{-1} p^{-1}$. By lemma 2.21, both W_g and W_{gp} are free over $T_{g'}$; by lemma 2.19, $W_g^{T_p}$ and Y are also free over $T_{g'}$. Taking $T_{g'}$ invariants in (3) leaves rows exact: we therefore obtain a second commutative diagram of G_1-module with exact rows:

$$
\begin{array}{ccccccccc}
0 & \longrightarrow & W_g^{T_{pg'}} & \longrightarrow & W_g^{T_{g'}} & \longrightarrow & Y^{T_{g'}} & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle 1-\lambda_p^{-1}} & & \downarrow{\scriptstyle \beta} & & \downarrow{\scriptstyle 1} & & \\
0 & \longrightarrow & W_{gp}^{T_{pg'}} & \longrightarrow & W_{gp}^{T_{g'}} & \longrightarrow & Y^{T_{g'}} & \longrightarrow & P
\end{array}
\tag{4}
$$

(here "1" denotes indentity map).

Now $H^q(J, W_g^{T_{g'}}) = 0$ for any $q > 0$, since $gg' = h_1 p^{-1} \neq h_1$, (lemma 2.22). Applying the functor $H^q(J, \ )$ to (4), we obtain from the long exact cohomology sequence the following commutative diagram of G_1-modules, with exact rows:

$$
\begin{array}{ccccccccccc}
\cdots & \longrightarrow & H^{q-1}(J, Y^{T_{g'}}) & \longrightarrow & A_g^q & \longrightarrow & 0 & \longrightarrow & H^q(J, Y^{T_{g'}}) & \longrightarrow & A_g^{q+1} \longrightarrow \cdots \\
 & & \downarrow{\scriptstyle 1} & & \downarrow{\scriptstyle 1-\lambda_p^{-1}} & & \downarrow & & \downarrow{\scriptstyle 1} & & \downarrow{\scriptstyle 1-\lambda_p^{-1}} \\
\cdots & \longrightarrow & H^{q-1}(J, Y^{T_{g'}}) & \xrightarrow{\alpha_1} & A_g^q & \xrightarrow{\alpha_2} & A_{gp}^q & \xrightarrow{\alpha_3} & H^q(J, Y^{T_{g'}}) & \longrightarrow & A_g^{q+1} \longrightarrow \cdots
\end{array}
$$

(here q is a positive integer). Let $\alpha_1, \alpha_2, \alpha_3$ denote the maps as shown in the second row of the diagram.

Using the commutativity of the square on the far left, we see that the image of α_1 is $(1-\lambda_p^{-1})A_g^q$, which is 0 by lemma 2.23 (because λ_p^{-1} acts trivially). Hence the map α_2 is injective. The same argument applied to the square on the far right shows that α_3 is surjective. Finally, the top row gives an isomorphism

$$H^q(J, Y^{T_{g'}}) \simeq A_g^{q+1}.$$

The lemma is proved.

The last two lemmas enable us to determine the order $|A_g^q|$ of A_g^q for any positive integer q.

Lemma 2.25. Let n be the number of primes dividing g.

If $n = 0$, $|A_1^q| = 1$ if q is odd

$|A_1^q| = e_K$ if q is even.

If $n > 0$, $|A_g^q| = e_K^{2^{n-1}}$.

Proof: Let $n = 0$, so that $g = 1$. Since $W_1 = R_1$ and $T_{h_1} = G_1$,

$$A_1' = H^1(J, R_1^{G_1}) \simeq (R_1^{G_1})_J/(1-j)R_1^{G_1} = 0$$

where $(R_1^{G_1})_J$ denotes the kernel of the map $s(J)$ in $R_1^{G_1}$.

Also $$A_1^2 = H^2(J, R_1^{G_1}) = (R_1^{G_1})^J/s(J)R_1^{G_1}$$

$$\simeq R_1^{G_1}/s(J)R_1^{G_1} \simeq \mathbb{Z}/|J|\mathbb{Z}.$$

Since J is cyclic, $A_1^{2q+1} = A_1^1$ and $A_1^{2q} = A_1^2$ for all $q > 0$. Thus we have computed the order of A_1^q.

Lemma 2.24 implies that, for g and any $p \nmid g$ that

$$|A_{pg}^q| = |A_g^q||A_g^{q+1}|.$$

A simple induction shows that

$$|A_{pg}^q| = e_K^{2^{n-1}}.$$

This proves the lemma.

We can now calculate the index $(R_o:U_o)$ using the results of this section; we begin with the index $(R_1:W)$.

For $i = 1,\ldots,r$, let $g_i = p_1 \ldots p_i$, and let $g_o = (1)$. Each g_i is a divisor of h_1, and $W_{g_o} = R_1, W_{g_r} = W$. As noted earlier, each W_{g_i} has rank $|G_1|$ as an abelian group, so the indices $(W_{g_{i-1}} : W_{g_i})$ are defined. Hence $(R_1 : W) = \prod_{i=1}^{r} (W_{g_{i-1}} : W_{g_i})$. This expression is a product of indices of the form $(W_g : W_{gp})$ where p does not divide g. In view of the exact sequences (1) and (2), lemma 2.9 shows that $(W_g : W_{gp}) = (W_g^{T_p} : W_{gp}^{T_p})$. But lemma 2.20 shows that $W_g^{T_p} = W_{gp}^{T_p}$. Hence $(R_1 : W) = 1$.

We use this result to obtain a relation between $(R_o : U_o) = (e_J R_{1,o} : e_J W_o)$ and $((R_{1,o})_J : (W_o)_J)$. By lemma 2.9, $(R_1 : W) = (R_{1,o} : W_o)(s(G_1)R_1 : s(G_1)W)$. Now $s(G_1)R_1 = \mathbb{Z}\, s(G_1)$ and $s(G_1)W = |G_1|\mathbb{Z}\, s(G_1)$, so that $(R_{1,o} : W_o) = |G_1|^{-1}$. Again by lemma 2.9, $(R_{1,o} : W_o) = |G_1|^{-1} = (e_J R_{1,o} : e_J W_o)((R_{1,o})_J : (W_o)_J)$.

We investigate the second factor on the right. First note that $(R_1)_J \subseteq R_{1,o}$, and thus $(R_{1,o})_J = (R_1)_J$; similarly $(W_o)_J = W_J$. Now

$$((R_1)_J : W_J) = ((R_1)_J : (1-j)W)((1-j)W : W_J),$$

where we recall that j generates J. Since $(R_1)_J = (1-j)R_1$,

$$((R_1)_J : W_J) = ((1-j)R_1 : (1-j)W)(W_J : (1-j)W)^{-1}.$$

But $W_J/(1-j)W \simeq H^1(J,W) = A_{h_1}^1$ has order $e_K^{2^{r-1}}$ by lemma 2.25 because r is the number of prime divisors of h_1. Combining these results, we obtain

$$(e_J R_{1,o} : e_J W_o)((1-j)R_1 : (1-j)W) = e_K^{2^{r-1}} \cdot |G_1|^{-1}.$$

It remains to compute $((1-j)R_1:(1-j)W)$. As before, we write

$$((1-j)R_1:(1-j)W) = \prod_{i=1}^{r} ((1-j)W_{g_{i-1}}:(1-j)W_{g_i}),$$

which leads us to indices of form $((1-j)W_g:(1-j)W_{gp})$ with p not dividing g. Since $(1-e_p)(1-j)W_{gp} = (1-e_p)(1-j)W_g$, lemma 2.9 shows that

$$((1-j)W_g:(1-j)W_{gp}) = (((1-j)W_g)^{T_p}:((1-j)W_{gp})^{T_p})$$

By lemma 2.20,

$((1-j)W_{gp})^{T_p} = s(T_p)(1-j)W_g + (1-\lambda_p^{-1})((1-j)W_g)^{T_p}$ and is contained in $((1-j)W_g)^{T_p}$.

Let $B = ((1-j)W_g)^{T_p}/s(T_p)(1-j)W_g$.

Then $B/(1-\lambda_p^{-1})B \simeq (1-j)W_g^{T_p}/(1-j)W_{gp}^{T_p}$,

and $((1-j)W_g^{T_p}:(1-j)W_{gp}^{T_p}) = |B/(1-\lambda_p^{-1})B|$.

We may identify B as one of the cohomology groups of the preceding section as follows. The map $W_g \longrightarrow (1-j)W_g$ given by multiplication by $(1-j)$ induces an exact sequence:

$$0 \longrightarrow W_g^J \longrightarrow W_g \longrightarrow (1-j)W_g \longrightarrow 0.$$

From this we obtain the long exact cohomology sequence (of G_1-modules):

$$\ldots \longrightarrow W_g^{T_p} \longrightarrow (1-j)W_g^{T_p} \longrightarrow H^1(T_p,W_g^J) \longrightarrow H^1(T_p,W_g) \longrightarrow \ldots$$

Now W_g is free over T_p, so $H^1(T_p,W_g) = 0$. Since the image of $W_g^{T_p} = s(T_p)W_g$ in $(1-j)W_g^{T_p}$ is $s(T_p)(1-j)W_g$, we obtain the isomorphism of G_1-modules

$$B \simeq H^1(T_p,W_g^J).$$

Lemma 2.22 shows that $B \simeq H^1(J, W_g^{T_p})$ provided that neither p nor g equals h_1. Now g does not equal h_1, because gp divides h_1. In the case that $p = h_1$, we have $g = 1$, $T_p = G_1$, $W_g = R_1$ and $B = ((1-j)R_1)^{G_1} / s(G_1)(i-j)R_1 = 0$.

We now now compute $((1-j)W_g : (1-j)W_{gp})$. First suppose that $r = 1$; then $h_1 = p$ and $g = 1$. We have just seen that $B = 0$ in this case, so that

$$((1-j)W_g : (1-j)W_{gp}) = 1.$$

Now consider the case $r > 1$. If $gp = h_1$, lemma 2.22 shows that $B \simeq H^1(J_p, W_g^J) = 0$ and so

$$((1-j)W_g : (1-j)W_{gp}) = 1.$$

On the other hand, if $gp = h_1$, $B \simeq A^1_{h_1}$; by lemma 2.23, $(1-\lambda_p^{-1})B = 0$, and so

$$((1-j)W_g : (1-j)W_{gp}) = |A^1_g| = e_K^{2^{r-2}}$$

because the number of primes dividing g is r-1.

We conclude that the index $((1-j)R_1 : (1-j)W)$ equals 1 if $r = 1$, and equals $e_K^{2^{r-2}}$ if $r > 1$. Consequently the value of $(R_o : U_o) = (e_J R_{1,o} : e_J W_o)$ is equal to $e_K |G_1|^{-1} = (\phi(h)/e_K)^{-1}$ if $r = 1$, and equal to $e_K^{2^{r-2}} |G_1|^{-1} = (\phi(h)/e_K^{2^{r-2}})^{-1}$ if $r > 1$.

Applying this to the results of §3 we see that $[S:C]$ equals $12^{[H:K]-1} h_H$ if $r = 1$, and otherwise equals $12^{[H:K]-1} h_H w_1 e_K^{2^{r-2}-r+1} . e_H^{-1}$ where w_1 is the divisor of w specified there.

Chapter 3. The index of elliptic units for fields of division points on an elliptic curve.

This chapter presents the calculation of the index of the elliptic units for fields of division points on an elliptic curve E defined over the imaginary quadratic base field K. The techniques used are similar to those of the preceding chapter, and again are inspired by the work of Sinnott [22]. The results depend upon those of the preceding chapter; hence we assume that K has class number one. Also, as explained below, the conductor of such a field is assumed prime to 6; but it is clear that the relaxation of this assumption introduces a factor divisible by only 2 or 3 (c.f. earlier remarks in chapter 2, and remarks in § 2 of this chapter.), and so does not affect the main results of this chapter.

Let E be an elliptic curve which is defined over K, and whose ring of endomorphisms is isomorphic to the integers o of K. Since K has class number 1, E has a global minimal model (see [28], p40), i.e. E is specified by an equation

$$y^2+a_1xy+a_3y = x^3+a_2x^2+a_4x+a_6$$

where the coefficients a_i lie in o, and the discriminant Δ is a unit except at precisely those points of K where E has bad reduction. Under the transformation

$$\eta = y + \frac{1}{2}(a_1x+a_3)$$

$$\zeta = x + \frac{1}{12}(a_1^2+4a_2)$$

this takes the form $E': \eta^2 = \zeta^3 - \frac{1}{4}g_2\zeta - \frac{1}{4}g_3$ for some constants g_2, g_3 (which are integral except perhaps at primes above 2 and 3). Let $p(z)$ be the associated Weierstrass function satisfying

$$p'(z)^2 = 4p^3(z) - g_2p(z) - g_3.$$

Since K has class number one, there is a complex constant Ω such that $L = \Omega o$ is the period lattice of $p(z)$; the discriminant, $\Delta(L)$, of L, equals Δ. Combining the maps $\mathbb{C}/L \longrightarrow E'$ and $E' \longrightarrow E$ we obtain an analytic parametrization $\xi^*: \mathbb{C}/L \longrightarrow E$. Let ψ be the Grossencharacter for E and $\mathfrak{f}$ its conductor (see [23], theorems 7.40 and 7.42); $\mathfrak{f}$ is divisible by precisely those primes of K where E has bad reduction. As remarked above, we assume that $\mathfrak{f}$ is prime to 6.

Let T denote the set consisting of 2, 3 and all rational primes q such that E does not have good reduction at at least one prime of K lying above q. Throughout, g will denote a fixed ideal of K not dividing any prime of T; in particular g is prime to $6\mathfrak{f}\bar{\mathfrak{f}}$. We will be considering the full group C of elliptic units of the field $M = K(E_g)$ of g-division points over K; recall that M has conductor $\mathfrak{f}g$ (lemma 2.4).

The elliptic units arise from $\mathfrak{f}g$-division points on L. Let P_1 be the group $\prod_{\substack{b \mid \mathfrak{f}g \\ b \neq (1)}} P(b)$ defined in chapter 1 (c.f. remark on p34), and let P be the group generated by the groups $N_{R(b)/R(b)\cap M}P(b)$ where b varies over all divisors, except (1), of $\mathfrak{f}g$. Denoting the global units of M by S, we have $C = S \cap \mu_M P$.

Let f and g denote fixed generators of $\mathfrak{f}$ and g respectively. Suppose that $\mathfrak{f}g$ has the factorization $p_1^{e_1} \ldots p_r^{e_r}$ into primes $p_1, \ldots, p_r$ (with positive integers e_i); we suppose that the first t primes $p_1, \ldots, p_t$ are the prime divisors of g; for each $i = 1, \ldots, r$, let π_i be a fixed generator of p_i.

Since we will be using results of chapter 2, we must assume the following condition on g: if a prime p which divides g is unramified and of degree 1, then its conjugate $\bar{p}$ does not divide g.

Throughout this chapter, G will denote the Galois group $G(M/K)$, and G_1 the group $G(R(\mathfrak{g})/K)$; R and R_1 will denote the corresponding group rings $\mathbb{Z}[G]$ and $\mathbb{Z}[G_1]$. Let $\rho: \mathbb{C}[G_1] \longrightarrow \mathbb{C}[G]$ be the ring homomorphism induced by the natural surjection $G_1 \longrightarrow G$. The letter χ will be reserved for characters of G: these will be regarded as characters of G_1, whose kernel fix M. The conductor will be denoted $\mathfrak{g}_\chi$; note that if $\mathfrak{g}_\chi$ divides $\mathfrak{g}$, χ is principal; the associated primitive character of $G(R(\mathfrak{g}_\chi)/K)$ will be denoted χ'. Similarly, the letter ξ will be reserved for characters of G_1, $\mathfrak{g}_\xi$ for its conductor, ξ' for the associated primitive character of $G(R(\mathfrak{g}_\xi)/K)$. The definition of χ and ξ will be extended in the usual way to the integers and ideals of o. The idempotents attached to χ and ξ (in $\mathbb{C}[G]$ and $\mathbb{C}[G_1]$ resp.) will be denoted e_χ and ε_ξ, and the ring homomorphisms induced by χ and ξ by ρ_χ and ρ_ξ. Note that $\rho(\rho_\xi) = 0$ if ξ is nontrivial on $G(R(\mathfrak{g})/M)$; otherwise ξ induces a character χ of G, and $\rho(\varepsilon_\xi) = e_\chi$.

Throughout, let ℓ denote the R-module mapping

$$\ell: M^\times \longrightarrow \mathbb{R}[G]$$

$$x \longmapsto \sum_{\sigma \in G} -\log|x^\sigma|\sigma^{-1};$$

let $\ell_1 = \ell_{R(\mathfrak{g})}$ denote the R_1-module mapping

$$\ell_1 : R(\mathfrak{g})^{\times} \longrightarrow \mathbb{R}[G_1]$$

$$y \longmapsto \sum_{\tau \in G_1} -\log|y^{\tau}|\tau^{-1};$$

we note that $S/C \simeq \ell(S)/\ell(C)$.

Let S be the subset of 2^r-1 divisors of $\mathfrak{g}$ obtained from products of the ideals $p_1^{e_1},\ldots,p_r^{e_r}$, but omitting (1); set $w_M = e_K^{-r} \prod_{b \in S} e_{R(b)\cap M}$. Let h_M denote the class number of M. For any rational prime p, let $|x|_p$ denote the usual p-adic value of a rational number x.

Our main result is

Theorem 2. The group C is of finite index in S; for any rational prime p not dividing $6\phi(\mathfrak{g})$,

$$|[S:C]|_p = |h_H|_p \cdot |w_1|_p$$

where w_1 is a divisor of w_M. In particular, if g is a power of an unramified split prime of K, which lies above p, $|[S:C]|_p = |h_H|_p$.

The last statement - the case of g a power of an unramified split prime above p - follows because M does not contain any p-power roots of unity.

Finally, for any R-module A, let A_o denote the submodule annihilated by $s(G) = \sum_{\sigma \in G} \sigma$; let A^G denote the submodule fixed by G.

§1. The class number formula.

The proof of theorem 2 relies also on the classical class number formula. Recall that for any nontrivial character ξ of G_1, $u(\xi') = \sum_{t \in B(\mathfrak{f}_\xi)} u(\frac{t}{f_\xi})\xi'(\sigma_t)$ where f_ξ is a generator of the conductor $\mathfrak{f}_\xi$, and $\sigma_t = [t, R(\mathfrak{f}_\xi)/K)]$. In particular this applies for any nontrivial character χ of G. Denoting the regulator of M by R_M, the formula states

$$h_M |R_M| = \frac{e_M}{e_K} \prod_{\chi \neq 1} \frac{|u(\chi')|}{6},$$

where the product is taken over all nontrivial characters χ of G. [See [18], p20].

The proof will use the R_1-modules $V(\mathfrak{f}g)$, $U(\mathfrak{f}g)$ and $I(\mathfrak{f}g)$ defined in §2 of the last chapter. We saw that $I(\mathfrak{f}g)V(\mathfrak{f}g) = \ell_1(P_1)$, and $(1-\varepsilon_1)V(\mathfrak{f}g) = \Omega.U(\mathfrak{f}g)$, where $\Omega = \sum_{\xi \neq 1} u(\bar{\xi}')\varepsilon_\xi$, the sum being taken over all characters ξ of G_1. We will consider the R-modules $V = \rho(V(\mathfrak{f}g))$ and $U = \rho(U(\mathfrak{f}g))$; they are related by the formula $(1-e_1)V = \omega.U$, where $\omega = \rho(\Omega) = \sum_{\chi \neq 1} u(\bar{\chi}')e_\chi$, the sum being taken over all characters χ of G. Now U is contained in $\mathbb{Q}[G]$, and is free of rank $|G|$ as an abelian group. [For as in lemma 2.11, it suffices to show that for all characters χ of G, $\rho_\chi(U) = 0$. Suppose that ξ is the character of G_1 which induces χ; lemma 2.11 shows that $\rho_\xi(U(\mathfrak{f}g) \neq 0$; but
$\rho_\xi(U(\mathfrak{f}g)) = \rho_\chi(\rho(U(\mathfrak{f}g)) = \rho_\chi(U)$, q.e.d.].

The basic step in the proof of theorem 2 is to express the index $[S:C] = (\ell(S):\ell(C))$ in the form

$$(\ell(S):R_o)(R_o:U_o)(U_o:(1-e_1)V)((1-e_1)V:(1-e_1)\ell(P))((1-e_1)\ell(P):\ell(C))$$

and to evaluate each index separately. In section 4, we calculate

the p-adic value of $(R_o:U_o)$. These results rely upon the similar results proved for the elliptic units of $R(\mathfrak{g})$ in the last chapter.

§2. Properties of elliptic units of M.

In this section we discuss some properties of the elliptic units C of M; most of them are simple consequences of the corresponding properties outlined in §3 of chapter 2.

Lemma 3.1. Let $a \in P$. Then $a^{s(G)} \in \mu_K$ if and only if $a \in C$.
The proof is identical to that of lemma 2.12.

Lemma 3.2. Let $a \in P$. Suppose that $a^{\sigma-1} \in \mu_M$ for every $\sigma \in G$. Then $\ell(a)$ lies in the group

$$\sum_{i=1}^{r} 12 \log|\pi_i| \mathbb{Z}\, s(G)$$

(Recall that $(\pi_i) = p_i$ is a prime divisor of $\mathfrak{g}$).

Proof: Lemma 2.13 shows that a, which lies in P_1, must be of the form $\zeta \prod_{i=1}^{r} \pi_i^{12n_i}$ for some integers n_i and some ζ in $\mu_{R(\mathfrak{g})}$.
Consequently, $\zeta \in \mu_M$ and $\ell(a)$ lies in the group mentioned, q.e.d.

The next lemma establishes the connection between $\ell(P)$ and $\ell(C)$, and as in chapter 2, it relies upon the condition imposed upon g, namely that g is not divisible by both an unramified split prime p and its conjugate $\bar{p}$. For brevity we denote $\ell(P)$ by T.

Lemma 3.3. $\ell(C) = T_o$.

Proof: Lemma 3.1 shows that $\ell(C) \subseteq T_o$. For the reverse inclusion, consider an a in T with $\ell(a)$ in T_o. Then $\ell(a^{s(G)}) = 0$ and so $|a^{s(G)}| = 1$. Let $b = a^{s(G)}$; it lies in $K^{\times}$ and satisfies $b\bar{b} = 1$. The fractional ideal (b) factorizes as a product of unramified split prime ideals $q_1, \ldots, q_s$ of K and their conjugates $\bar{q}_1, \ldots, \bar{q}_s$ in the form

$$(q_1\bar{q}_1^{-1})^{n_i}\dots(q_s\bar{q}_s^{-1})^{n_s},$$

for some integer $n_1,\dots,n_s$. Because a lies in P, for each i, either the ideal q_i and its conjugate $\bar{q}_i$ must divide $\mathfrak{f}g$, or $n_i = 0$. Since g is not divisible by such a product $q_i\bar{q}_i$, and is prime to $\mathfrak{f}\bar{\mathfrak{f}}$, we conclude that $q_i\bar{q}_i$ divides $\mathfrak{f}$.

Let D_1 and D_2 denote respectively the set of divisors of $\mathfrak{f}$ and g, excluding (1); let D_3 denote the set of divisors of $\mathfrak{f}g$ which divide neither $\mathfrak{f}$ nor g. Recalling the definition of P, we see that P is generated by the three groups

$$P_i = \prod_{b\in D_i} N_{R(b)/R(b)\cap M}P(b) \qquad (i = 1,2,3)$$

Now a is a product $a_1a_2a_3$ with each $a_i\in P_i$. The element a_3 is a unit; the argument above shows that a_2 is a unit. Thus $|a_1^{s(G)}| = |b| = 1$, and since a_1 lies in K, $|a_1^{\sigma}| = 1$ for each $\sigma\in G$. Hence $\ell(a) = \ell(a_2a_3)$ lies in $\ell(C)$, q.e.d.

The next lemma computes one of the indices to be used in the proof of theorem 2.

Lemma 3.4. $T_o = T\cap(1-e_1)T$. Furthermore, T_o has finite index in T, equal to $\phi(g)/e_K^t$. (Recall that t is the number of distinct prime divisors of g).

Proof: As in the proof of lemma 2.16, $T_o = (1-e_1)T\cap T$ and $(1-e_1)T/T_o \simeq e_1T/T^G$; we compute the groups e_1T and T^G explicitly. Lemma 1.12 shows that

$$e_1T = \frac{1}{|G|}\,\ell(P^{s(G)}) = \frac{1}{|G|}\sum_{i=1}^{r} 12n_{p_i}\log|\pi_i|\mathbb{Z}\, s(G),$$

where the integer n_{p_i} equals $|G|$ if p_i divides $\mathfrak{f}$, or $e_K|G|/\phi(p_i^{e_i})$ if p_i divides g.

Now consider T^G. Let $a \in P$: then $\ell(a) \in T^G$ if and only if $(\sigma-1)\ell(a) = \ell(a^{\sigma-1}) = 0$ for every $\sigma \in G$. Fix $\sigma \in G$. Then $a^{\sigma-1}$ is a unit in M (an elliptic unit) and lies in the kernel of ℓ: hence it is a root of unity. By lemma 3.2, $\ell(a)$ lies in the group $\sum_{i=1}^{r} 12 \log|\pi_i| \mathbb{Z}\, s(G)$. For any prime p_i, it is easy to choose an element a_{p_i} in P such that $\ell(a_{p_i}) = 12 \log|\pi_i| s(G)$ (see lemma 2.16); consequently

$$T^G = \sum_{i=1}^{r} 12 \log|\pi_i| \mathbb{Z}\, s(G).$$

It is now clear that $(1-e_1)T/T_o$ is finite, and has order equal to the product of the factors $\frac{\phi(p_1^{e_1})}{e_K}$, where p_i divides g, i.e. equal to $\phi(g)/e_K^t$, q.e.d.

The next lemma computes another of the indices required for the proof of theorem 2. Recall that S is the collection of 2^r-1 divisors of $\mathfrak{g}g$ generated by products of the ideals $p_1^{e_1},\ldots,p_r^{e_r}$ omitting (1); the element w_M was defined in the introduction to be $\bar{e}_K^r \prod_{b \in S} e_{R(b)\cap M}$. Let w_1 denote the index $[(1-e_1)V:(1-e_1)T]$.

Lemma 3.5. If p does not divide $6\phi(\mathfrak{g})$, $|w_1|_p \geq |w_M|_p$.

Proof: The proof of lemma 2.5 shows that $V(\mathfrak{g}g) = T_1 + \sum_{b \in S} \eta(\mathfrak{g}gb^{-1})\mathbb{Z}$, where $T_1 = \ell(P_1)$. Hence $V = \rho(T_1) + \sum_b \rho(\eta(\mathfrak{g}gb^{-1}))\mathbb{Z}$. Let $V' = \sum_b \rho(\eta(\mathfrak{g}gb^{-1}))\mathbb{Z}$. Since $e_{R(b)\cap M}\mathbb{Z}$ is the ideal generated by the integers $N\mathfrak{a}-1$, where $\mathfrak{a}$ is an ideal of K (prime to $6b$) such that $[\mathfrak{a}, R(b)\cap M/K] = 1$, $e_{R(b)\cap M}\rho(\eta(\mathfrak{g}gb^{-1}))$ lies in $\rho(T_1)$. Hence $V/\rho(T_1) = V'/V' \cap \rho(T_1)$ has order dividing $\prod_b e_{R(b)\cap M}$.

Now $\rho(T_1) = \ell(P_1^{s(G_2)})$, where $G_2 = G(R(\phi g)/M)$. But $P_1^{s(G_2)}$ is clearly of finite index in P, for $P^{\phi(\phi)} \subseteq P_1^{s(G_2)} \subseteq P$. We conclude that $(V:T) = (V:\rho(T_1))(T:\rho(T_1))^{-1}$ exists, and moreover, that $|(V:T)|_p = |(V:\rho(T_1))|_p$. Also $(V^G:T^G) = e_K^r$ (see lemma 2.17), so the statement of the lemma follows immediately.

We have calculated most of the indices to be used in the proof of theorem 2; we gather these results together now. Recall that w_1 denotes the index $[(1-e_1)V: (1-e_1)T]$.

Theorem 2. C has finite index in S, equal to

$$12^{[M:K]-1} h_M (R_o:U_o) \left(\frac{e_M}{e_K}\right)^{-1} w_1 \cdot \frac{\phi(g)}{e_K^t}.$$

Proof: As noted earlier, $S/C \simeq \ell(S)/\ell(C)$. Both $\ell(S)$ and $\ell(C)$ lie in the subspace $X = (1-e_1)\mathbb{R}[G]$. Thus, formally at least,

$$(\ell(S):\ell(C)) = (\ell(S):R_o)(R_o:U_o)(U_o:(1-e_1)V)((1-e_1)V:(1-e_1)T)((1-e_1)T:T_o)$$

where we recall that $T_o = \ell(C)$. In fact, each of the groups appearing is a lattice in X; in the course of the proof this will be demonstrated for each index separately. The last two indices have already been calculated in the last two lemmas. Note that the index $(R_o:U_o)$ is defined, for the span of each R_o and U_o is X (the span of U is $\mathbb{R}[G]$, c.f. page 84), they are discrete, lie inside $\mathbb{Q}[G]$ and are finitely generated over $\mathbb{Z}$. The first index is easily seen to be defined and equal to $2^{[M:K]-1}|R_M^{-1}|$ by the same method on page 62. It remains to consider the third index

$(U_o:(1-e_1)V)$. Clearly $(1-e_1)V \subseteq X$, and it was seen in §2 that $(1-e_1)V = \omega.U$. We first observe that $(1-e_1)U = U_o$. [For, from page 63, $(1-\varepsilon_1)U_1 = U_{1,o}$ is the submodule of U_1 annihilated by $s(G_1)$. Apply ρ to obtain $(1-e_1)U = \rho(U_{1,o}) = U_o$]. Now consider the linear transformation A on X induced by multiplication with ω:

$$Ax = \omega x \text{ for each } x \in X.$$

Then $A(U_o) = (1-e_1)V$. By considering the $\mathbb{C}$-linear extension of A to $(1-e_1)\mathbb{C}[G]$, we have (see page 63),

$$\det A = \prod_{\chi \neq 1} u(\bar{\chi}')$$

where the product is taken over all nonprincipal characters χ of G. By the class number formula, $\det A \neq 0$, so that $(1-e_1)V$ is indeed a lattice in X, and $(U_o:(1-e_1)V) = \left| \prod_{\chi \neq 1} u(\bar{\chi}') \right|$.

Combining these calculations gives

$$[S:C] = 2^{[M:K]-1} |R_M|^{-1} . (R_o:U_o) . \prod_{\chi \neq 1} |u(\bar{\chi}')| . w_1 . \frac{\phi(g)}{e_K^t}$$

$$= 12^{[M:K]-1} h_H (R_o:U_o) . \left(\frac{e_M}{e_K}\right)^{-1} . w_1 . \frac{\phi(g)}{e_K^t},$$

by the class number formula. This proves the stated result.

In the next section we consider the p-adic value of $(R_o:U_o)$ for a rational prime p not dividing $6\phi(g)$. Our results so far show that $|[S:C]|_p = |h_M|_p . |w_1/e_M|_p . |(R_o:U_o)|_p |\phi(g)|_p$.

Remark. If the restriction $(g,6) = 1$ is removed extra factors divisible by 2 or 3 enter the formula, but as remarked on p65, these come from the index $(U_o:(1-e_1)V)$, and can be compensated for by using the slightly larger group of elliptic units mentioned on p35, and modifying V. In particular, the p-adic value for the index is unaffected by removal of this restriction.

§3. The p-part of $(R_o:U_o)$.

In this section we calculate the p-part of $(R_o:U_o)$ for any rational prime p not dividing $6\phi(\mathfrak{f})$; these results immediately imply theorem 2. The prime p will be fixed henceforth and throughout, we will be calculating the p-part of various indices: this is equivalent to considering the index of appropriate $\mathbb{Z}_p$-lattices, as we now explain.

Let X be a finite dimensional vector space over $\mathbb{Q}$, and let M_1, M_2 be lattices which span the same subspace V of X. Then there exists a linear transformation A: V ⟶ V such that $A(M_1) = M_2$; the index $(M_1:M_2)$ was defined to be $|\det A|$. (c.f. section 2, chapter 2).

Now consider a finite dimensional vector space Y over $\mathbb{Q}_p$, and two $\mathbb{Z}_p$-lattices N_1, N_2 which span the same subspace W of Y. As before, there exists a linear transformation B: W ⟶ W such that $B(N_1) = N_2$; in this case we say the p-index of N_2 in N_1 exists, denote it $(N_1:N_2)_p$, and give it the value $|\det B|_p$; the value does not depend upon the choice of B.

It is easily checked that if N_1 and N_2 are finitely generated $\mathbb{Z}_p$-submodules of $\mathbb{Q}_p[G]$, with $N_2 \subseteq N_1$, then $(N_1:N_2)_p$ is defined if and only if N_2 is of finite index in N_1, and in this case $(N_1:N_2)_p^{-1} = [N_1:N_2]$, the index. Also, given three finitely generated $\mathbb{Z}_p$-submodules N_1, N_2, N_3, then $(N_1:N_3)_p = (N_1:N_2)_p(N_2:N_3)_p$ i.e. whenever two of these symbols is defined, so is the third, and this relation holds.

Now consider the original finite dimensional vector space X over $\mathbb{Q}$, and the lattices M_1 and M_2. The tensor product $Y = X \otimes_{\mathbb{Q}} \mathbb{Q}_p$

is a finite dimensional space over $\mathbb{Q}_p$ (of dimension equal to that of X over $\mathbb{Q}$), and the products $N_i = M_i \otimes_{\mathbb{Z}} \mathbb{Z}_p$ $(i = 1,2)$ are $\mathbb{Z}_p$-lattices which generate the same subspace Y, viz. $W = V \otimes_{\mathbb{Q}} \mathbb{Q}_p$. The linear transformation A which mapped M_1 onto M_2 now induces a linear transformation B: $W \longrightarrow W$ such that $B(N_1) = N_2$, and $\det B = \det A$. Thus the index $(N_1:N_2)_p$ is defined, and equals $|\det A|_p$; equivalently, $|(M_1:M_2)|_p = (M_1 \otimes_{\mathbb{Z}} \mathbb{Z}_p : M_2 \otimes_{\mathbb{Z}} \mathbb{Z}_p)_p$. By a slight abuse of notation, we set $(M_1:M_2)_p = |(M_1:M_2)|_p$.

The following analogue of lemma 2.9 is quite useful; it is proved in a similar fashion (see [25] lemma 6.1).

Lemma 3.6. Let N_1 and N_2 be $\mathbb{Z}_p$-lattices in $\mathbb{Q}_p[G]$ and suppose that $(N_1:N_2)_p$ is defined. Let α be an element of $\mathbb{Q}_p[G]$. Let $N_{i,\alpha}$ denote the set of elements $a \in N_i$ such that $\alpha a = 0$ $(i = 1,2)$. Then both $(N_{1,\alpha}:N_{2,\alpha})_p$ and $(\alpha N_1:\alpha N_2)_p$ are defined and $(N_1:N_2)_p = (N_{1,\alpha}:N_{2,\alpha})_p (\alpha N_1:\alpha N_2)_p$.

We now consider the index $(R_o:U_o)$. By lemma 2.9, $(R:U) = (R_o:U_o)(s(G)R:s(G)U)$. Now $s(G)R = \mathbb{Z}\, s(G)$; furthermore, since $U_1 = U_{1,o} + s(G_1)\mathbb{Z}$, $s(G)U = |G||G_1|^{-1}\rho(s(G_1)U_1) = |G_1|s(G)\mathbb{Z}$. Thus $(R_o:U_o) = \frac{e_K}{\phi(\mathfrak{g})}(R:U)$.

We will compute $(R:U)_p$ by considering the p-part of indices related to $(R_1:U_1)$. Denoting by $R_{1,o}$ and $U_{1,o}$ the submodules of R_1 and U_1 annihilated by $s(G_1)$, section 4 of the last chapter shows that $(R_{1,o}:U_{1,o}) = e_K^{2^{r-2}}/\phi(\mathfrak{g})$ (r is the number of distinct primes dividing $\mathfrak{g}$. Thus

$$(R_1:U_1) = (R_{1,o}:U_{1,o})(s(G_1)R_1 : s(G_1)U_1) = e_K^{2^{r-2}},$$

and so $(R_1:U_1)_p = 1$.

Let G_2 be the subgroup of G which fixes M, and let $\varepsilon = s(G_2)/|G_2|$. Then ε is idempotent in R_1 and the restriction homomorphism ρ induces an isomorphism $\varepsilon\mathbb{C}[G_1] \simeq \mathbb{C}[G]$ under which $\varepsilon R_1 \simeq R$ and $\varepsilon U_1 \simeq U$; in particular, $(R:U) = (\varepsilon R_1 : \varepsilon U_1)$. Since $p \nmid 6\phi(\mathfrak{g})$, the idempotent ε lies inside $R_{1,p} = R_1 \otimes_{\mathbb{Z}} \mathbb{Z}_p$. Hence the submodules of $R_{1,p}$ and of $U_{1,p} = U_1 \otimes_{\mathbb{Z}} \mathbb{Z}_p$ annihilated by ε are, respectively, $(1-\varepsilon)R_{1,p}$ and $(1-\varepsilon)U_{1,p}$. Noting that $\varepsilon R_{1,p} = (\varepsilon R_1) \otimes_{\mathbb{Z}} \mathbb{Z}_p$ etc., lemma 3.6 shows that

$$1 = (R_1:U_1)_p = (\varepsilon R_1 : \varepsilon U_1)_p ((1-\varepsilon)R_1 : (1-\varepsilon)U_1)_p .$$

The remainder of this section is devoted to showing that the two factors on the right hand side of this equation have p-adic value less than or equal to one, and so are both equal to one. We will analyse an R_1-module U^*, which is closely related to U_1, in a similar manner to that of §4 in the last chapter.

For a prime p_i dividing $\mathfrak{g}g$, let $T_{p_i} = G(R(\mathfrak{g}g)/R(\mathfrak{g}g p_i^{-e_i}))$ and let $s(T_{p_i})$ denote the group norm $\sum_{\sigma \in T_{p_i}} \sigma$. Furthermore, let $\bar{\sigma}_{p_i} = \sum_{\xi} \bar{\xi}'(p_i)\varepsilon_\xi$, the sum being taken over all characters ξ of G_1, and set $U_{p_i} = s(T_{p_i})R_1 + (1-\bar{\sigma}_{p_i})R_1$. Let U^* be the R_1-module generated by all products of the form $\prod_{i=1}^{r} x_{p_i}$, with $x_{p_i} \in U_{p_i}$.

Lemma 3.7. U^* is a submodule of U_1, of index e_K. Moreover,

$$(1-\varepsilon)U^* = (1-\varepsilon)U_1 \text{ and } \varepsilon_1 U^* = e_K \varepsilon_1 U_1 .$$

Proof: We first show that $(1-\varepsilon_1)U^* = (1-\varepsilon_1)U_1$. Let S be a subset of primes dividing $\mathfrak{g}g$, and let $\alpha_S = \prod_{p \in S} s(T_p) \prod_{p \notin S} (1-\bar{\sigma}_p)$ be a typical generator of U^*. Let a be the largest divisor of $\mathfrak{g}g$ divisible only by primes not in S, and consider the element $\alpha_a = s(H_a) \prod_{p \mid a} (1-\bar{\sigma}_p)$

of U_1 (recall that $H_a = G(R(\mathfrak{g})/R(a))$). It is easily checked that $(1-\varepsilon_1)\alpha_S = (1-\varepsilon_1)\alpha_a$; thus $(1-\varepsilon_1)U^* \subseteq (1-\varepsilon_1)U_1$. The reverse inclusion is similarly established (c.f. lemma 2.19).

Since $\varepsilon_1(1-\bar{\sigma}_p) = 0$, $\varepsilon_1 U^* = \mathbb{Z}\varepsilon_1 \prod_{p|\mathfrak{g}} s(T_p) = \mathbb{Z}\phi(\mathfrak{g})\varepsilon_1$

$= e_K \mathbb{Z} s(G_1)\varepsilon_1 = e_K\varepsilon_1 U_1$. It is now clear that U^* is a submodule of U_1. Finally, since $U_{1,o} = (1-\varepsilon_1) U_1$ (see page 63), and $U_o^* = (1-\varepsilon_1)U^*$ (by a similar argument), we obtain $(U_1:U^*) = (\varepsilon_1 U_1:\varepsilon_1 U^*)((1-\varepsilon_1)U_1:(1-\varepsilon_1)U^*) = e_K$. The lemma is now proved.

We deduce immediately that

$$(\varepsilon R_1:\varepsilon U^*)_p((1-\varepsilon)R_1:(1-\varepsilon)U^*)_p = 1,$$

(because $(U_1:U^*)_p = (\varepsilon U_1:\varepsilon U^*)_p((1-\varepsilon)U_1:(1-\varepsilon_1)U^*)_p = 1$).

For $i = 1,\ldots,r$, let $b_i = p_1,\ldots,p_r$, and let W_{b_i} be the R_1-module generated by the products $\prod_{j=1}^{i} x_{p_j}$ where each $x_{p_j} \in U_{p_j}$; let $b_o = (1)$ and $W_{b_o} = R_1$; note that $W_{b_r} = U^*$. Each W_{b_i} is contained in $\mathbb{Q}[G_1]$ and is free of rank $|G_1|$ over $\mathbb{Z}$ (this is proved as on page 66). Thus $(R_1:U^*) = \prod_{i=1}^{r} (W_{b_{i-1}}:W_{b_i})$. Each factor in this product is of the form $(W_b:W_{bp})$ where b is one of the divisors b_i above, and p is a prime divisor of $\mathfrak{g}$, not dividing b. For the remainder of this section b will denote such an ideal b_i, and p is a prime divisor of $\mathfrak{g}$. We view U^* as being formed from $W_1 = R_1$ by successively multiplying by the modules U_{p_i} $(i = 1,\ldots,r)$. As in chapter 2, the calculation of the indices $(W_b:W_{bp})$ and $(R_1:U^*)$ relies upon a pair of exact sequences.

First, it is necessary to describe the element $\bar{\sigma}_p$ more explicitly. For each prime p_i dividing $\mathfrak{g}g$, let $e_{p_i} = s(T_{p_i})/|T_{p_i}|$; it is idempotent in $\mathbb{Q}[G_1]$. Let t be an integer prime to $6\mathfrak{g}g$ satisfying the congruences

$$t \equiv 1 \bmod p_i^{e_i}$$

$$t \equiv \pi_i \bmod \mathfrak{g}g p_i^{-e_i},$$

and set $\lambda_{p_i} = [t, R(\mathfrak{g}g)/K]$. It is easily checked (c.f. page 68) that $\bar{\sigma}_{p_i} = \lambda_{p_i}^{-1} e_{p_i}$.

Since $(1-e_p)s(T_p) = 0$ and $(1-\bar{\sigma}_p)(1-e_p) = (1-e_p)$, we have $(1-e_p)W_{bp} = (1-e_p)W_b$, for any prime p not dividing b. For any R_1-module A, let A^{T_p} be the submodule fixed by T_p: an element a of A lies in A^{T_p} precisely if $(1-e_p)a = 0$. We obtain the following pair of exact sequences of R_1-modules

$$(1) \qquad \begin{array}{ccccccccc} 0 & \longrightarrow & W_b^{T_p} & \longrightarrow & W_b & \longrightarrow & Y & \longrightarrow & 0 \\ 0 & \longrightarrow & W_{bp}^{T_p} & \longrightarrow & W_{bp} & \longrightarrow & Y & \longrightarrow & 0, \end{array}$$

where $Y = (1-e_p)W_b = (1-e_p)W_{bp}$, and the surjections in (1) and (2) are induced by multiplication with $(1-e_p)$.

But the following two pairs of sequences are also exact:

$$(2) \qquad \begin{array}{ccccccccc} 0 & \longrightarrow & ((1-\varepsilon)W_b)^{T_p} & \longrightarrow & (1-\varepsilon)W_b & \longrightarrow & (1-\varepsilon)Y & \longrightarrow & 0 \\ 0 & \longrightarrow & ((1-\varepsilon)W_{bp})^{T_p} & \longrightarrow & (1-\varepsilon)W_{bp} & \longrightarrow & (1-\varepsilon)Y & \longrightarrow & 0. \end{array}$$

$$(3) \qquad \begin{array}{ccccccccc} 0 & \longrightarrow & (\varepsilon W_b)^{T_p} & \longrightarrow & \varepsilon W_b & \longrightarrow & \varepsilon Y & \longrightarrow & 0 \\ 0 & \longrightarrow & (\varepsilon W_{bp})^{T_p} & \longrightarrow & \varepsilon W_{bp} & \longrightarrow & \varepsilon Y & \longrightarrow & 0. \end{array}$$

Lemma 2.9 shows that $(\varepsilon W_b : \varepsilon W_{bp}) = ((\varepsilon W_b)^{T_p} : (\varepsilon W_{bp})^{T_p})$ and $((1-\varepsilon)W_b : (1-\varepsilon)W_{bp}) = (((1-\varepsilon)W_b)^{T_p} ((1-\varepsilon)W_{bp})^{T_p})$.

Now $W_{bp} = W_b W_p$ (the R_1-module generated by products $x_b x_p$ with x_b in W_b, x_p in W_p), and it is easily checked (c.f. lemma 2.20) that

$$W_{bp}^{T_p} = s(T_p) W_b + (1-\lambda_p^{-1}) W_b^{T_p},$$

$$(\varepsilon W_{bp})^{T_p} = s(T_p) \varepsilon W_b + (1-\lambda_p^{-1})(\varepsilon W_b)^{T_p},$$

and $$((1-\varepsilon)W_{bp})^{T_p} = s(T_p)(1-\varepsilon)W_b + (1-\lambda_p^{-1})((1-\varepsilon)W_b)^{T_p}.$$

In particular, $(\varepsilon W_{bp})^{T_p} \subseteq (\varepsilon W_b)^{T_p}$ and $((1-\varepsilon)W_{bp})^{T_p} \subseteq ((1-\varepsilon)W_{bp})^{T_p}$.

Thus $(\varepsilon W_b : \varepsilon W_{bp})$ and $((1-\varepsilon)W_b : (1-\varepsilon)W_{bp})$ are rational integers.

Since $(\varepsilon R_1 : \varepsilon U^*) = \prod_i (\varepsilon W_{b_{i-1}} : \varepsilon W_{b_i})$ and $((1-\varepsilon)R_1 : (1-\varepsilon)U^*)$ $= \prod_i ((1-\varepsilon)W_{b_{i-1}} : (1-\varepsilon)W_{b_i})$, these two indices are also rational integers. But

$$1 = (R_1 : U)_p = (R_1 : U^*)_p = (\varepsilon R_1 : \varepsilon U^*)_p ((1-\varepsilon)R_1 : (1-\varepsilon)U^*)_p;$$

we conclude that both the factors on the right equal one; so $(R:U)_p = (\varepsilon R_1 : \varepsilon U^*)_p = 1$, and $(R_o : U_o)_p = |\phi(fg)/e_K|_p^{-1}$.

Applying this to the result obtained in section 3, the index of the elliptic units of M has p-adic value equal to $|b_M|_p . |w_1/e_M|_p$ (where w_1 is the divisor of w_M specified there).

§4. The index for other abelian extensions.

The method of this chapter can be applied to calculate the p-part of the index of the elliptic units for other abelian extensions of K. See [10] for the index of related subgroups of units.

Let N be such an abelian extension, with conductor h; let H be the ray class field modulo h, and d = [H:N]. Let h have factorization $p_1^{e_1},\ldots,p_r^{e_r}$ into primes $p_1,\ldots,p_r$ of K ($e_1,\ldots,e_r$ positive integers); let π_i be a fixed generator of p_i (i = 1,...,r).

Since we use results of chapter 2, we suppose that h is prime to 6 (but as remarked earlier, this affects the actual index by factors of 2 and 3 only), and moreover that if the prime p dividing h is unramified and of degree one, then <u>either</u> the conjugate $\bar{p}$ does not divide h, <u>or</u> $R(p^e)\cap N = R(\bar{p}^f)\cap N = K$, where p^e and $\bar{p}^f$ denote the exact powers of p and $\bar{p}$ dividing h.

The elliptic units arise from h-division points on a fixed lattice L with order o. Let P_1 be the group $\prod_{\substack{b\mid h\\ b\neq(1)}} P(b)$ defined in chapter 1, and let P be the group generated by the groups $N_{R(b)/R(b)\cap N}P(b)$, where b varies over all divisions of h, except (1). Denoting the global units of N by S, we have $C = S\cap\mu_N P$.

Let S be the set of 2^r-1 divisors of h generated by products of the ideals $p_1^{e_1},\ldots,p_r^{e_r}$, except (1); let $w_N = e_K^{-r}\prod_{b\in S} e_{R(b)\cap N}$. Let h_N denote the class number of N. For each i, let $d_{p_i} = [N\cap R(p_i^{e_i}):K]$.

<u>Theorem 3</u>. The group C has finite index in S; if p is a rational prime not dividing 6d,

$$|[S:C]|_p = |h_N|_p \cdot |w_1/e_N|_p$$

where w_1 is a divisor of w_N.

Throughout this section, let G and G_1 denote the groups $G(N/K)$ and $G(H/K)$ respectively, and $R = \mathbb{Z}[G]$ and $R_1 = \mathbb{Z}[G_1]$ the respective group rings. Let $\rho:\mathbb{C}[G_1] \longrightarrow \mathbb{C}[G]$ be the ring homomorphism induced by the surjection $G_1 \longrightarrow G$. The letters χ and ξ will be reserved for characters of G and G_1 (resp.); χ will be regarded as a character of G_1 whose kernel fixes N. The conductors will be denoted $\mathfrak{f}_\chi$ and $\mathfrak{f}_\xi$ (resp.); the associated primitive characters by χ' and ξ' (resp.). The ring homomorphisms associated to χ and ξ will be denoted ρ_χ (mapping $\mathbb{C}[G] \longrightarrow \mathbb{C}$) and ρ_ξ (mapping $\mathbb{C}[G_1] \longrightarrow \mathbb{C}$); the idempotents attached to χ and ξ will be denoted e_χ and ε_ξ. If A is any R-module, the submodule annihilated by $s(G) = \sum_{\sigma \in G} \sigma$ will be denoted A_o. Let ℓ denote the mapping

$$\begin{aligned} \ell: N^\times &\longrightarrow \mathbb{R}[G] \\ x &\longmapsto \sum_{\sigma \in G} -\log|x^\sigma|\sigma^{-1}; \end{aligned}$$

let $\ell_H: H^\times \longrightarrow \mathbb{R}[G_1]$ denote the mapping defined in chapter 2; note that $S/C \simeq \ell(S)/\ell(C)$.

§5. Proof of theorem 3.

The proof of theorem 3 relies on the classical class number formula. Denoting by R_N the regulator of N, it states ([18] p20)

$$h_N|R_N| = \frac{e_N}{e_K} \prod_{\chi\neq 1} \frac{|u(\chi')|}{6}$$

where the product is taken over all nontrivial characters χ of G.

We will use the R_1-modules $V(h)$, $U(h)$ and $I(h)$ defined in §2 of chapter two. Recall that $I(h)V(h) = \ell_H(P_1)$, and $(1-\varepsilon_1)V(h) = \Omega.U(h)$, where $\Omega = \sum_{\xi\neq 1} u(\bar{\xi}')\varepsilon_\xi$. We consider the R-modules $V = \rho(V(h))$ and $U = \rho(U(h))$; denoting $\rho(\Omega) = \sum_{\chi\neq(1)} u(\bar{\chi}')e_\chi$ by ω (the sum over all characters χ of G), we have $(1-e_1)V = \omega.U$. It is easily seen that U, which is contained in $\mathbb{Q}[G]$, is free of rank $|G|$ over $\mathbb{Z}$ [c.f. lemma 2.11, and page 84]. The basic step in the proof is to express $[S:C] = (\ell(S):\ell(C))$ in the form

$$(\ell(S):R_o)(R_o:U_o)(U_o:(1-e_1)V)((1-e_1)V:(1-e_1)\ell(P))((1-e_1)\ell(P):\ell(C))$$

and evaluate each index separately; in the final stage we calculate the p-adic value of $(R_o:U_o)$.

The following lemmas establish properties of C analogous to those of §3 in the last chapter.

Lemma 3.8. Let $a\in C$. Then $a^{s(G)}\in\mu_K$ if and only if $a\in C$.

The proof is identical to that of lemma 2.12.

Lemma 3.9. Let $a\in P$. Suppose $a^{\sigma-1}\in\mu_N$ for every $\sigma\in G$. Then $\ell(a)$ lies in the group

$$\sum_{i=1}^{r} 12\log|\pi_i|\mathbb{Z}\, s(G).$$

The proof is very similar to lemma 3.2. The next lemma establishes the connection between $T = \ell(P)$ and $\ell(C)$; it uses the condition imposed upon h earlier.

Lemma 3.10. $\ell(C) = T_o$.

Proof: Lemma 3.8 shows that $\ell(C) \subseteq T_o$. For the reverse inclusion consider an a in T with $\ell(a) = 0$. Then $\ell(a^{s(G)}) = 0$ and so $|a^{s(G)}| = 1$. Let $b = a^{s(G)}$; it lies in $K^\times$ and satisfies $b\bar{b} = 1$. The fractional ideal (b) of K factorizes as a product of unramified split prime ideals $q_1,\ldots,q_s$ of K and their conjugates $\bar{q}_1,\ldots,\bar{q}_s$ in the form

$$(q_1\bar{q}_1^{-1})^{n_1}\ldots(q_s\bar{q}_s^{-1})^{n_s}$$

for some integers $n_1,\ldots,n_s$. Because a lies in P, either $q_i\bar{q}_i$ divides h or $n_i = 0$, for each $i = 1,\ldots,r$.

Let $\mathfrak{h}$ be the largest divisor of h, which is divisible only by unramified rational primes q which split in K, and set $g = h\mathfrak{h}^{-1}$.

Let D_1 and D_2 denote respectively the set of prime power divisors of $\mathfrak{h}$ and g, excluding (1); let D_3 denote the remaining divisors of h, excluding (1) (they are divisible by at least two distinct primes). Now P is generated by the three groups

$$P_i = \prod_{b\in D_i} N_{R(b)/R(b)\cap N} P(b) \qquad (i = 1,2,3),$$

so a is a product $a_1a_2a_3$ with each $a_i\in P_i$. The element a_3 is a unit; the condition on h implies that a_2 is a unit. Thus $|a_1^{s(G)}| = |b| = 1$, and since a_1 lies in $K^\times$, $|a_1^\sigma| = 1$ for each $\sigma\in G$. Hence $\ell(a) = \ell(a_2a_3)$ lies in $\ell(C)$, q.e.d.

The next two lemmas compute two of the indices mentioned above.

Lemma 3.11. $T_o = T\cap(1-e_1)T$. Furthermore T_o has finite index in $(1-e_1)T$, equal to $\prod_{i=1}^{r} d_{p_i}$. (Recall that $d_{p_i} = [N\cap R(p_i^{e_i}):K]$).

Proof: As in the proof of lemma 2.16, $T_o = (1-e_1)T \cap T$ and $(1-e_1)T/T_o \simeq e_1T/T^G$; we compute the groups e_1T and T^G explicitly. Lemma 1.12 shows that

$$e_1T = \frac{1}{|G|}\,\ell(P^{s(G)}) = \frac{1}{|G|}\sum_{i=1}^{r} 12n_{p_i}\log|\pi_i|\mathbb{Z}s(G),$$

where $n_{p_i} = [N: N\cap R(p_i^{e_i})]$; note that $n_{p_i}d_{p_i} = |G|$.

Now consider T^G. Let $a\in P$. If $\ell(a)\in T^G$, a now familiar argument shows that $a^{\sigma-1}\in\mu_N$, for every $\sigma\in G$, and so by lemma 3.9, $\ell(a)$ lies in $\sum_{i=1}^{r} 12\log|\pi_i|\mathbb{Z}\, s(G)$. For any prime p_i, it is easy to choose an element a_{p_i} in P such that $\ell(a_{p_i}) = 12\log|\pi_i|s(G)$ (see lemma 2.16); consequently $T^G = \sum_{i=1}^{r} 12\log|\pi_i|\mathbb{Z}\, s(G)$. It is now clear that T_o is of finite index in $(1-e_1)T$, equal to $\prod_{i=1}^{r} d_{p_i}$.

The next lemma describes another index needed in the proof of theorem 3. Let $w_1 = [(1-e_1)V:(1-e_1)T]$; recall that w_N was defined in the introduction.

Lemma 3.12. If p does not divide 6d, $|w_1|_p \geq |w_N|_p$.

The proof is very similar to lemma 3.5. We now gather together these results.

Theorem 3 bis. C has finite index in S equal to

$$12^{[N:K]-1}h_N(R_o:U_o)\left(\frac{e_N}{e_K}\right)^{-1}w_1\cdot\prod_{i=1}^{r} d_{p_i}.$$

Proof: As explained earlier, we write $[S:C] = (\ell(S):\ell(C))$ in the form

$$(\ell(S):R_o)(R_o:U_o)(U_o:(1-e_1)V)((1-e_1)V:(1-e_1)T)((1-e_1)T:T_o).$$

Each of these groups is a lattice in $X = (1-e_1)\mathbb{R}[G]$, as we shall see. The fourth and fifth indices have been computed above; the index $(R_o:U_o)$ is defined, because, as we noted above, U has rank $|G|$ over $\mathbb{Z}$. The first index is easily shown to equal $2^{[N:K]-1}|R_N|^{-1}$ (c.f. page 62). Finally an argument similar to that of the proof of theorem 2 (page 63) shows that the third index equals $\prod_{\chi\neq 1} |u(\bar{\chi}')|$ (the product over all characters χ of G). The class number formula implies that

$$[S:C] = 2^{[N:K]-1}|R_N|^{-1}.(R_o:U_o) \prod_{\chi\neq 1} |u(\bar{\chi}')|.w_1 . \prod_{i=1}^{r} d_{p_i}$$

$$= 12^{[N:K]-1}h_N(R_o:U_o)\left(\frac{e_N}{e_K}\right)^{-1} w_1 \prod_{i=1}^{r} d_{p_i}, \text{ q.e.d.}$$

We finally address ourselves to the p-adic evaluation of $(R_o:U_o)$. Fix a prime p not dividing 6d. By lemma 2.9, $(R:U) = (R_o:U_o)(s(G)R: s(G)U)$. Now $s(G)R = \mathbb{Z}s(G)$; furthermore, since $U_1 = U_{1,o} + s(G_1)\mathbb{Z}$, $s(G)U = |G||G_1|^{-1}\rho(s(G_1)U_1) = |G_1|s(G)\mathbb{Z}$. Thus $(R_o:U_o) = |G_1|^{-1}(R:U)$.

Denoting by $R_{1,o}$ and $U_{1,o}$ the submodules of R_1 and U_1 annihilated by $s(G_1)$, section 4 of the last chapter showed that $(R_{1,o}:U_{1,o})_p = |\phi(h)|_p^{-1} = |G_1|_p^{-1}$, and so $(R_1:U_1)_p = 1$.

Let G_2 denote the subgroup G_1 which fixes N, and let $\varepsilon = S(G_2)/|G_2|$. Then ε is idempotent in R_1 and the restriction homomorphism ρ induces an isomorphism $\varepsilon\mathbb{C}[G_1] \simeq \mathbb{C}[G]$ under which $\varepsilon R_1 \simeq R$ and $\varepsilon U_1 = U$; in particular $(R:U) = (\varepsilon R_1:\varepsilon U_1)$. Since $p\nmid 6d$, the idempotent ε lies inside $R_{1,p} = R_1\otimes_{\mathbb{Z}}\mathbb{Z}_p$; thus the submodules of $R_{1,p}$ and $U_{1,p} = U_1\otimes_{\mathbb{Z}}\mathbb{Z}_p$ annihilated by ε are, respectively, $(1-\varepsilon)R_{1,p}$ and $(1-\varepsilon)U_{1,p}$. Hence, by lemma 3.6,

$$1 = (R_1:U_1)_p = (\varepsilon R_1:\varepsilon U_1)_p((1-\varepsilon)R_1:(1-\varepsilon)U_1)_p.$$

The remainder of this section is devoted to showing that the indices on the right have p-adic value less than or equal to one, and so both equal one. We need an analogue of the module U^* defined in the last section. For any prime p_i dividing h, let $T_{p_i} = G(H/R(hp_i^{-e_i}))$, and $\bar{\sigma}_{p_i} = \sum_{\xi} \bar{\xi}'(p_i)\varepsilon_\xi$, the sum being over all characters ξ of G_1. Let $U_{p_i} = s(T_{p_i})R_1+(1-\bar{\sigma}_{p_i})R_1$, and let U^* be the R_1-module generated by products $\prod_{i=1}^{r} x_{p_i}$ with $x_{p_i} \in U_{p_i}$. It is easily checked (c.f. lemma 3.7) that U^* is a submodule of U_1, of index e_K, and that $(1-\varepsilon_1)U^* = (1-\varepsilon_1)U_1$ and $\varepsilon_1 U^* = e_K\varepsilon_1 U_1$; thus

$$1 = (R_1:U_1)_p = (R_1:U^*)_p = (\varepsilon R_1:\varepsilon U^*)_p((1-\varepsilon)R_1:(1-\varepsilon)U^*)_p.$$

For $i = 1,\ldots,r$ let $b_i = p_1,\ldots,p_i$, and let W_{b_i} be the R_1-module generated by products $\prod_{j=1}^{i} x_{p_j}$ with $x_{p_j} \in U_{p_j}$; set $b_o = (1)$, and $W_{b_o} = R_1$; note that $W_{b_r} = U^*$. As before, each W_{b_i} is contained in $\mathbb{Q}[G_1]$ and is free of rank $|G_1|$ over $\mathbb{Z}$. Thus, $(R_1:U^*) = \prod_{i=1}^{r} (W_{b_{i-1}}:W_{b_i})$. Each factor is of the form $(W_b:W_{bp})$, where b is one of the divisors b_i above, and p is a prime divisor of h, not dividing b. For the remainder of this section, let b denote such an ideal b_i, and p a prime divisor of h. As before, we view U^* as being formed from $W_1 = R_1$ by successively multiplying by the modules U_{p_i} $(i = 1,\ldots,r)$; the main tool is provided by two pairs of exact sequences.

For each prime p, let $e_p = s(T_p)/|T_p|$; then e_p is idempotent, and $(1-e_p)W_{bp} = (1-e_p)W_b$. Let α denote either the idempotents ε or $(1-\varepsilon)$. The following pair of sequences is exact:

$$
\begin{array}{ccccccccc}
0 & \longrightarrow & (\alpha W_b)^{T_p} & \longrightarrow & \alpha W_b & \longrightarrow & \alpha Y & \longrightarrow & 0 \\
0 & \longrightarrow & (\alpha W_{bp})^{T_p} & \longrightarrow & \alpha W_{bp} & \longrightarrow & \alpha Y & \longrightarrow & 0,
\end{array} \tag{1}
$$

where $Y = (1-e_p)W_{bp} = (1-e_p)W_b$; the surjections are induced by multiplication with $(1-e_p)$. Lemma 3.6 shows that $(\alpha W_b : \alpha W_{bp}) = ((\alpha W_b)^{T_p} : (\alpha W_{bp})^{T_p})$. But it is easily checked (c.f. lemma 2.20) that

$$(\alpha W_{bp})^{T_p} = s(T_p)\alpha W_b + (1-\lambda_p^{-1})(\alpha W_b)^{T_p},$$

where λ_p is defined, as before, so that $\bar{\sigma}_p = \lambda_p^{-1} e_p$. In particular, $(\alpha W_{bp})^{T_p} \subseteq (\alpha W_b)^{T_p}$, so that $(\alpha W_b : \alpha W_{bp})$ is a rational integer. Hence $(\alpha R_1 : \alpha U^*) = \prod_{i=1}^{r} (\alpha W_{b_{i-1}} : \alpha W_{b_i})$ is a rational integer. But $1 = (\varepsilon R_1 : \varepsilon U^*)_p ((1-\varepsilon)R_1 : (1-\varepsilon)U^*)_p$; we conclude that both factors on the right are equal to one. So $(R:U)_p = (\varepsilon R_1 : \varepsilon U^*)_p = 1$, and $(R_o : U_o)_p = |G_1|_p^{-1}$.

Applying this to the earlier index result, we see that the p-adic value of the index of the elliptic units is equal to

$|h_N|_p \cdot |w_1/e_N|_p \cdot \prod_{i=1}^{r} |d_{p_i}|_p \cdot |G_1|_p^{-1}$, where w_1 is a divisor of w_N.

Clearly, $[R(p_i^{e_i}) : R(p_i^{e_i}) \cap N] = \phi(p_i^{e_i})/e_K d_{p_i}$ divides d, so that if p does not divide 6d, this index has p-adic value 1.

This then implies the result of theorem 3.

Chapter 4. Applications to the arithmetic of elliptic curves.

In this chapter we consider the relation between the rank of the group of F-rational points on an elliptic curve E over a number field F, and the order of the zero of the Hasse-Weil zeta function $L(E/F,s)$ for E over F at $s = 1$. It is conjectured that $L(E/F,s)$, which is defined in the half plane $\mathrm{Re}(s) > \frac{3}{2}$, has an analytic continuation to the whole plane, and given this, Birch and Swinnerton-Dyer [1] conjectured that the rank of $E(F)$ modulo torsion is precisely the order of the zero at $s = 1$. (See also [3], [26]).

For the case we consider here, namely, when E has complex multiplication, Deuring [9] has proven the analytic continuation of the Hasse-Weil zeta function by identifying it with a product of Hecke L-series with Grossen characters. If ψ denotes the Grossen character of E, and has conductor $\mathfrak{f}$, let

$$L(\psi,s) = \prod_{\substack{q \nmid \mathfrak{f} \\ q \text{ prime}}} (1-\psi(q)(Nq)^{-s})^{-1},$$ and define $L(\bar{\psi},s)$ similarly.

Then if E is defined over K, $L(E/K,s) = L(\psi,s)L(\bar{\psi},s)$.

Let E be the elliptic curve described in chapter 3; we use the same notation for the objects attached to E; in particular, ψ denotes the Grossen character, $\mathfrak{f}$ its conductor, $L = \Omega_0$ the period lattice described there, and T the set consisting of 2, 3 and all rational primes q for which E does not have good reduction at at least one prime of K above q. Throughout, let p be a fixed rational prime which splits in K and does not lie in T; let p and $\bar{p}$ be the distinct factors of p, and let $\pi = \psi(p)$, so that π is a generator of p in K (see [23] §7.8).

For each nonnegative integer n, let $F_n = K(E_{p^{n+1}})$ and $G_n = G(F_n/K)$. The prime p totally ramifies in F_n (lemma 2.1); let p_n be the unique prime of F_n above p. Let $\Phi_n = F_{n,p_n}$ be the completion of F_n at p_n, U_n the units of Φ_n congruent to 1 modulo p_n, and U_n' the subgroup of such units with norm 1 to K_p.

Let $F_\infty = \bigcup_{n\geq o} F_n$ and $G_\infty = G(F_\infty/K)$. Let $\Gamma = G(F_\infty/F_o)$; then G_∞ is canonically isomorphic to $\Gamma\times\Delta$, where Δ is isomorphic to G_o. Γ is isomorphic to $\mathbb{Z}_p$, so let γ be a fixed topological generator of Γ. Let $K: G_\infty \longrightarrow \mathbb{Z}_p^\times$ be the canonical character giving the action of G_∞ on the group $E_{p^\infty} = \bigcup_{n\geq o} E_{p^{n+1}}$ of p-power division points on E: $u^\sigma = \kappa(\sigma)u$ for each $u\in E_{p^\infty}$ and $\sigma\in G_\infty$. We write χ for the restriction of κ to Δ; χ takes values which are (p-1)-st roots of unity in $\mathbb{Z}_p$. For any $\mathbb{Z}_p[\Delta]$-module A, let $A^{(i)}$ denote the $\mathbb{Z}_p$-submodule of A on which Δ acts via χ^i: A then decomposes into a direct sum $A = \bigoplus_{i=o}^{p-2} A^{(i)}$. We will be particularly interested in three such modules X_∞, Y_∞ and Z_∞ which will be decomposed in this fashion; the module X_∞ relates to the arithmetic of the curve E, while Y_∞ and Z_∞ are formed from the elliptic units of the fields F_n - the results we can prove about Y_∞ and Z_∞ imply results about X_∞ and the arithmetical properties of E.

Suppose X is a p-profinite abelian group (so that it is a compact $\mathbb{Z}_p$-module) on which Γ operates continuously. Let $\Lambda = \mathbb{Z}_p[[T]]$ be the ring of formal power series over $\mathbb{Z}_p$ in one indeterminate T. The Γ-module structure on X gives rise to a unique Λ-module structure satisfying $(1+T)x = \gamma.x$ for each $x\in X$. (Recall that γ generates topologically). The general properties

of such Λ-modules and the structure theorem for finitely generated Λ-modules are discussed in [20]. Two such modules are said to be pseudo-isomorphic if there is a Λ-homomorphism between them with finite kernel and finite cokernel. For each integer $n \geq 0$, let $\Gamma_n = G(F_\infty/F_n)$, and $\omega_n = \omega_n(T)$ be the polynomial $(1+T)^{p^n}-1$. The Γ_n-invariance of X, denoted X_{Γ_n} is defined to be the quotient $X/\omega_n X$; if $n = 0$ this is simply denoted X_Γ.

We now define the first module X_∞. Let M_n denote the maximal abelian p-extension of F_n unramified outside p_n, and $X_n = G(M_n/F_\infty)$. Define $X_\infty = \varprojlim X_n$ where the projective limit is taken in the obvious way. Γ acts on X_n via inner automorphisms: let $\tilde{\gamma}$ denote any extension of γ to an element of $G(M_n/F_o)$, and then γ acts on $\sigma \in X_n$ via $\tilde{\gamma}\sigma\tilde{\gamma}^{-1}$. It is easily seen that $(X_\infty)_{\Gamma_n} = X_n$ (see for example [4]). Let $M_\infty = \bigcup_{n\geq o} M_n$.

Now for the second module Y_∞. For each $n \geq 0$, let $C_{o,n}$ be the subgroup $N_{R(\wp p^{n+1})/F_n} W(\wp p^{n+1})$ of the group of elliptic units of F_n c.f. the definition of chapter 1, §5. Each element of $C_{o,n}$ is congruent to 1 mod p_n (see [7]), so let $Y_n = U_n'/\bar{C}_{o,n}$, where $\bar{C}_{o,n}$ denotes the closure of $C_{o,n}$ in the p_n-adic topology. Define $Y_\infty = \varprojlim Y_n$, where the projective limit is taken with respect to the norm maps N_{F_m/F_n} $(m \geq n \geq 0)$. The Λ-module structure of Y_∞ is described in [8]; for each $i = 0,\ldots,p-2$, $Y_\infty^{(i)}$ is pseudo-isomorphic to a quotient $\Lambda/g_i(T)\Lambda$ where $g_i(T)$ is, as we now explain, a p-adic L-function.

For each integer $k \geq 1$, let $L_\wp(\bar{\psi}^k, s)$ be the Hecke L-function of $\bar{\psi}^k$, viewed as a (not necessarily primitive) Grossen character

mod $\mathfrak{f}$ (the conductor of $\bar{\psi}$): $L_{\mathfrak{f}}(\bar{\psi}^k,s) = \prod_{\substack{q \nmid \mathfrak{f} \\ q \text{ prime}}} (1-\bar{\psi}(q)\ (Nq)^{-s})^{-1}$

(for $\mathrm{Re}(s) > \frac{3}{2}$). Note that it possesses an analytic contribution to the whole plane. The numbers $\Omega^{-k}L(\bar{\psi}^k,k)$ belong to K (see [7]), and therefore may be viewed as lying inside K_p. Let Ω_p denote the completion of the maximal unramified extension of K_p, and I_p the ring of integers of Ω_p.

Let f be a fixed generator of $\mathfrak{f}$, and write $\mu_k = 12(-1)^{k-1}(k-1)!(\Omega/f)^{-k}$; also set $u = \kappa(\gamma)$ (recall γ is the generator of Γ fixed above).

It is shown in [8] that for each nonzero class i mod(p-1), there exists a power series $G_i(T)$ in the ring of formal power series $I_p[[T]]$ with the following interpolation property:

$$G_i(u^k-1) = \gamma_p^{1-k}\ \mu_k\ (1 - \frac{\bar{\psi}(p)^k}{Np})\ L(\bar{\psi}^k,k)$$

for all positive integers $k \equiv i \bmod(p-1)$; here γ_p is a unit in I_p. Then $Y_\infty^{(i)}$ is pseudo-isomorphic to $\Lambda/g_i(T)\Lambda$, where $g_i(T)$ is a power series in Λ which generates the same ideal in $I_p[[T]]$ as $G_i(T)$; moreover $(Y_\infty^{(i)})_{\Gamma_n} = Y_n^{(i)}$. In fact, if $i \not\equiv 0$ or $1 \bmod(p-1)$, $Y_\infty^{(i)}$ is <u>isomorphic</u> to the stated module; the same is true for the case $i \equiv 1$, provided p is not <u>anomolous</u> i.e. $\pi+\bar{\pi} = 1$.

The third module Z_∞ is formed in a similar fashion with the full groups C_n of elliptic units of F_n; let C_n' be the subgroup of such units congruent to 1 modulo p_n. Define $Z_n = U_n'/\bar{C}_n'$, where $\bar{C}_n'$ denotes the closure in the p_n-adic topology; set $Z = \varprojlim U_n'/\bar{C}_n'$. As noted in [8], it is easily seen that $Z^{(i)}$ is pseudo-isomorphic to a quotient $\Lambda/h_i(T)\Lambda$ for some $h_i \in \Lambda$; the following more precise description of h_i can be proved by the methods

of [8], but the details are omitted because of length.

For each integer $k \geq 1$, let $\mathfrak{f}_k$ be the conductor of $\bar{\psi}^k$ (it divides $\mathfrak{f}$), and let f_k be a fixed generator of it. Define $\nu_k = 12(-1)^{k-1}(k-1)!(\Omega/f_k)^{-k}$. Then there exists a power series $H_i(T)$ in $I_p[[T]]$ with the following interpolation property:

$$H_i(u^k-1) = \delta_p \nu_k \left(1 - \frac{\bar{\psi}(p)^k}{Np}\right) L_{\mathfrak{f}_k}(\bar{\psi}^k, k)$$

for all positive integers $k \equiv i \bmod (p-1)$; here δ_p is a unit in I_p, and $L_{\mathfrak{f}_k}(\bar{\psi}^k, s) = \prod_{q \nmid \mathfrak{f}_k} (1-\bar{\psi}^k(q)(Nq)^{-s})^{-1}$ is the Hecke L-function of $\bar{\psi}^k$, now viewed as a primitive Grossen character mod $\mathfrak{f}_k$. Then $Z_\infty^{(i)}$ will be pseudo-isomorphic to $\Lambda/h_i(T)\Lambda$, where $h_i(T)$ is a power series in Λ generating the same ideal in $I_p[[T]]$ as $H_i(T)$; moreover $(Z_\infty^{(i)})_{\Gamma_n} = Z_n^{(i)}$.

The close connection between X_∞ and Y_∞, Z_∞ is provided by considering the global units S_n of F_n; let S_n' denote the global units congruent to 1 mod p_n, and $\bar{S}_n'$ the closure in U_n. Denoting by L_n the p-Hilbert class field of F_n, global class field theory shows (see [6]) that $U_n'/\bar{S}_n'$ is isomorphic as a G_n-module to $G(M_n/L_nF_\infty)$, which is a subgroup of $X_n = G(M_n/F_\infty)$ of order the p-part of the class number of F_n. On the other hand $\bar{S}_n'/\bar{C}_n'$ has precisely this order also, and it is conjectured that X_∞ and Y_∞ (and Z_∞) are pseudo-isomorphic and that the components $X_\infty^{(i)}$, $Y_\infty^{(i)}$, $Z_\infty^{(i)}$ are individually pseudo-isomorphic. The establishment of this property would have deep consequences for the arithmetic of E. The cyclotomic analogue of these modules are discussed in [4]; the analogous pseudo-isomorphism has been recently proved by Wiles and Mazur. Indeed, the work of [8] was motivated by Iwasawa's work on cyclotomic units [11], [12].

In the next section we prove the theorem of Coates and Wiles using the module Y_∞; in the final section we relate the Iwasawa invariants of Z_∞ and X_∞ (which are defined in that section) to the rank of $E(F_0)$ as an o-module. Our results are:

Theorem 4. If $E(K)$ has infinitely many points, then $L(E/K,1) = 0$.

Theorem 5. Suppose that p (which does not lie in T) is prime to $\phi(\mathfrak{f})$. Then the Iwasawa λ- and μ-invariants of X_∞ and Z_∞ are equal. Furthermore the λ-invariant is at least as large as the rank of $E(F_0)$ (mod torsion) as an o-module.

§1. The Coates-Wiles theorem.

In this section, we suppose that E(K) has infinitely many points, and hence in particular, has a point P of infinite order. Further we assume throughout that p is not anomolous; infinitely many such primes exist (see [7], lemma 12).

The idea of the proof is to show that $g_1(u-1) = 0$ by constructing sufficiently large submodules of $(U_n'/\bar{C}_{o,n})^{(1)}$ for each n. The proof may be broken into several stages.

First, let $Y_\infty^{(1)}(-1)$ denote the Tate twist by (-1) (explained below). Then, as a Λ-module,

$$Y_\infty^{(1)}(-1) \simeq \Lambda/(h(T))$$

where $h(T) = g_1((u(1+T)-1)$ (recall $u = \kappa(\gamma)$).

Second, we show that either $h(0) = 0$ or $|h(0)|_p^{-1}$ is the number of elements in $(\Lambda/h\Lambda)_\Gamma$.

At the third stage, we construct extensions H_n of F_n for each n, as follows. Let Q_n be a point defined over the algebraic closure of K such that $\pi^{n+1}Q_n = P$. Set $H_n = F_n(Q_n)$, and recall that L_n is the p-Hilbert class field of F_n. The extension $H_nL_nF_\infty/L_nF_\infty$ will be shown to have degree p^{n+1-c}, where c is a constant independent of n, and depending only on P. The Galois group $G(H_nL_nF_\infty/L_nF_\infty)$ is a homomorphic image of $(U_n'/\bar{C}_{o,n})^{(1)}$, and thus of $Y_\infty^{(1)}$; from this it will follow that $|h(0)|_p \leq p^{-(n+1-c)}$, and letting $n \longrightarrow \infty$, we conclude that

$$h(0) = g_1(u-1) = 0 = L(\bar{\psi},1) = L(E/K,1).$$

We now proceed with the proof in stages. For $\mathbb{Z}_p$-modules A and B on which a group G acts, we define the action of G on the $\mathbb{Z}_p$-homomorphism group Hom(A,B) as follows. Let g belong to Hom(A,B). Define g^σ, for $\sigma \in G$ to be the homomorphism $g: A \longrightarrow B$ such that $g(a) = (f(a^{\sigma^{-1}}))^\sigma$ for every $a \in A$.

Let T be the Tate module $\varprojlim_{\pi^{n+1}} E$ (the connecting homomorphisms are multiplication by powers of π). G_∞ acts on T via the character κ. Define the G_∞-module $T(-1) = \mathrm{Hom}_{\mathbb{Z}_p}(T, \mathbb{Z}_p)$; here the action of G_∞ on $\mathbb{Z}_p$ is trivial. Thus G_∞ acts on T(-1) via κ^{-1}: for $t \in T$, and any homomorphisms $g: T \longrightarrow \mathbb{Z}_p$,

$$g^\sigma(t) = g(t^{\sigma^{-1}}) = g(\kappa(\sigma^{-1})t) = \kappa^{-1}(\sigma)g(t).$$

Define the twist of $Y_\infty^{(1)}$ by T(-1), denoted $Y_\infty^{(1)}(-1)$, to be the $\mathbb{Z}_p$-module $Y_\infty^{(1)} \otimes_{\mathbb{Z}_p} T(-1)$, with G_∞ acting diagonally on tensor products. Then for any $\sigma \in G_\infty$, $y \in Y_\infty^{(1)}$ and $g \in T(-1)$,

$$\sigma(y \otimes g) = \sigma y \otimes g^\sigma = \kappa^{-1}(\sigma)(\sigma y \otimes g).$$

The $\mathbb{Z}_p$-module $Y_\infty^{(1)}(-1)$ is isomorphic as a $\mathbb{Z}_p$-module to $Y_\infty^{(1)}$; only the action of G_∞ has been changed. There is an isomorphism $\theta: Y_\infty^{(1)} \longrightarrow Y_\infty^{(1)}(-1)$ such that

$$\theta(\sigma y) = \kappa(\sigma)\sigma\theta(y) \text{ for all } y \in Y_\infty^{(1)}.$$

Now for any y in $Y_\infty^{(1)}$, and h(T) in Λ, we have

$$\theta(h(T)y) = h(u(1+T)-1)\theta(y);$$

this clearly holds if h(T) is a constant, or if h(T) = T (for then $T\alpha = (\gamma-1)\alpha$, and $u = \kappa(\gamma)$) and the result follows for general h(T)

by linearity and continuity, since the module is compact. Thus

$$Y_\infty^{(1)}(-1) \simeq \Lambda/h(T)\Lambda,$$

where $h(T) = g_1(u(1+T)-1)$.

The next step in the argument is to consider the value $h(0)$.

Lemma 4.1. Either $h(0) = 0$, or $|h(0)|_p^{-1}$ is the number of elements of $(\Lambda/(h(T))_\Gamma$.

Proof: Suppose $h(0) \neq 0$, and $|h(0)|_p^{-1} = p^m$. There is a surjective homomorphism ϕ: $\Lambda/h\Lambda \longrightarrow \mathbb{Z}/p^m\mathbb{Z}$ induced by mapping an element $g \in \Lambda$ to $g(0)$. Since $h(0) \equiv 0$ modulo $p^m\mathbb{Z}_p$, the mapping $g(\text{mod } h) \longmapsto g(0) \text{ mod } p^m\mathbb{Z}_p$ is well defined (noting that $\mathbb{Z}_p/p^m\mathbb{Z}_p \simeq \mathbb{Z}/p^m\mathbb{Z}$). The kernel of ϕ clearly contains $T.\Lambda/h\Lambda$. Suppose $g+h\Lambda$ lies in the kernel of ϕ: so $p^m | g(0)$. Write

$$g(T) = p^m g_o + Tq_1(T)$$

$$h(T) = p^m h_o + Tq_2(T),$$

where q_1 and q_2 belong to Λ, g_o and h_o belong to $\mathbb{Z}_p$, and h_o is a unit. Then

$$g(T) = g_o h_o^{-1} h(T) - T(G_o h_o^{-1} q_2(T) - q_1(T))$$

$$\equiv Tq_3(T) \text{ modulo } h\Lambda$$

for some $q_3(T) \in \Lambda$. Thus the kernel of ϕ is equal to $T\Lambda/h\Lambda$, so that

$$(\Lambda/h\Lambda)_\Gamma \simeq \mathbb{Z}/p^m\mathbb{Z}$$

has p^m elements. The lemma is proved.

For the next step, let n be a nonnegative integer. As explained in detail in [6], global class field theory describes the Galois group $G(M_n/L_nF_\infty)$ as a G_n-module: $U_n'/\bar{S}_n'$ is isomorphic to $G(M_n/L_nF_\infty)$. In particular, since $G_n \simeq G_o \times G(F_n/F_o)$, we have

$$(U_n'/\bar{S}_n')^{(l)} \simeq G(M_n/L_nF_\infty)^{(l)}.$$

(G_n operates on $G(M_n/L_nF_\infty)$ via inner automorphisms: if $\sigma \in G_n$ and $x \in G(M_n/L_nF_\infty)$, then $x^\sigma = \rho x \rho^{-1}$, where ρ is any element of $G(M_n/K)$ whose restriction to F_n is equal to σ). There is a natural surjection of $\mathbb{Z}_p[G_n]$ modules

$$(U_n'/\bar{C}_{o,n})^{(l)} \longrightarrow (U_n'/\bar{S}_n')^{(l)} \longrightarrow o. \qquad (1)$$

We will show that $(U_n'/\bar{S}_n')^{(l)}$ has a submodule of order at least p^{n+1-c}, where c is a constant depending only on P.

Choose Q_n over the algebraic closure of K such that $\pi^{n+1}Q_n = P$; set $H_n = F_n(Q_n)$. The extension H_n/F_n is cyclic of degree dividing p^{n+1}, and it is unramified outside p_n: thus $H_n \subseteq M_n$ (see lemma 33 of [7]).

The group G_o (or Δ) acts via χ on $G(H_n/F_n)$. For, let $x \in G(H_n/F_n)$, $\sigma \in G_o$, and let σ_1 be any element of $G(H_n/K)$ whose restriction to F_n is equal to σ. Define $(x,P) = xQ_n - Q_n$. (Subtraction in $E(\mathbb{C})$). This is independent of the choice of Q_n: its value lies in $E_{\pi^{n+1}}$. Then

$$(x^\sigma, P^\sigma) = x^\sigma(Q_n^{\sigma_1}) - Q_n^{\sigma_1} = (xQ_n - Q_n)^{\sigma_1} = (x,P)^\sigma.$$

Now $P \in E(K)$, so that $(x^\sigma, P) = \chi(\sigma)(x,P)$. Hence $x^\sigma = \chi(\sigma)x$ for all $x \in G(H_n/F_n)$.

The key step now is to show that H_n/F_n is nontrivial, and is sufficiently large; more exactly, that $G(H_nL_nF_\infty/L_nF_\infty)$, which is a homomorphic image of $G(M_n/L_nF_\infty)^{(1)}$, is sufficiently large.

As noted in lemma 35 of [6], we may assume that P belongs to the kernel of reduction modulo P on $E(K_p)$. There is an isomorphism over o_p between the formal group $\hat{E}(p)$ on E corresponding to the parameter $t = 2p(z)/p'(z)$ and the formal group $\mathcal{E}(p)$ on which the endomorphism corresponding to π is given by $[\pi]\omega = \omega^p + \pi\omega$ (see [7] p228). Let δ be the point on $\hat{E}(p)$ corresponding to P, and α the image in $\mathcal{E}(p)$ under this isomorphism. For any integer $n \geq 0$, let $\mathcal{E}_{\pi^{n+1}}$ denote the points β in the algebraic closure of K_p satisfying $[\pi^{n+1}]\beta = 0$: these correspond to the points of $E_{\pi^{n+1}}$. We shall denote addition in the group $\mathcal{E}(p)$ by a star (*) and subtraction by a tilde (~).

Let $\Phi_n = \bigcup_{n\geq o} \Phi_n$ (recall that Φ_n is the completion of F_n at p_n). Then as explained in lemma 35 of [7], $\Phi_n(Q_n) = \Phi_n(\alpha_n)$ and $\Phi_\infty(Q_n) = \Phi_\infty(\alpha_n)$, where α_n are defined inductively by the formulae

$$[\pi]\alpha_o = \alpha, \quad [\pi]\alpha_{m+1} = \alpha_m \text{ for all } m \geq 0.$$

By our remarks above, $\Phi_\infty(\alpha_n)/\Phi_\infty$ is cyclic of degree dividing p^{n+1}. The following lemma is a refinement of theorem 11 of [7].

Lemma 4.2. Let c be the least positive integer such that $\alpha \notin [\pi^{c+1}]\mathcal{E}(p)$. For each $n \geq c$, the extension $\Phi_\infty(\alpha_n)/\Phi_\infty$ is totally ramified, and of degree p^{n+1-c}.

(We stress that c depends only on P, and not on n).

Proof: First we note that because F_o/K is totally ramified at p, the Galois group $G(\Phi_o/K_p)$ may be identified with G_o. Since α belongs to $E(p)$, one sees easily that G_o operates on $G(\Phi_\infty(\alpha_n)/\Phi_\infty)$ via χ. Thus Φ_∞ is the maximal abelian extension of K_p contained in $\Phi_\infty(\alpha_n)$. As any unramified extension of Φ_∞ is abelian over K_p, it suffices to prove that $\Phi_\infty(\alpha_n)/\Phi_\infty$ has degree p^{n+1-c}.

We may assume, without loss of generality, that $c = 0$. Indeed, choose β in $E(p)$ such that $[\pi^c]\beta = \alpha$, then β satisfies the hypotheses of the lemma with $c = 0$, and $\Phi_\infty(\alpha_n) = \Phi_\infty(\beta_{n-c})$; here β_m satisfies $[\pi]\beta_o = \beta$ and $[\pi]\beta_{m+1} = \beta_m$ for all $m \geq 0$.

Suppose therefore that $c = 0$. The proof is by induction on n. If $n = 0$, suppose that $\Phi_\infty(\alpha_o) = \Phi_\infty$. Then the map $\sigma \longmapsto \alpha_o^\sigma \sim \alpha_o$ is clearly a cocycle on G_∞ with values in E_π. But by Sah's lemma (see [19]) $H^1(G_\infty, E_\pi) = 0$. Hence there must exist v_o on E_π such that $\alpha_o^\sigma \sim \alpha_o = v_o^\sigma \sim v_o$ for all σ in G_∞. Thus $\alpha_o \sim v_o$ is fixed by G_∞, and so lies in K_p. But then $\alpha = [\pi](\alpha_o \sim v_o)$ belongs to $[\pi]E(p)$, which is a contradiction. Hence the lemma is true for $n = 0$.

Suppose it has been proven for n, but that $\Phi_\infty(\alpha_n) = \Phi_\infty(\alpha_{n+1})$. Let τ denote a generator of $G(\Phi_\infty(\alpha_n)/\Phi_\infty)$. Now

$$\alpha_{n+1}^\tau = \alpha_{n+1} * \eta$$

for some $\eta \in E_{\pi^{n+2}}$, whence

$$\alpha_{n+1}^{\tau^k} = \alpha_{n+1} * [k]\eta$$

for all $k \geq 0$. As $\tau^{p^n} = 1$, it follows that $\eta \in E_{\pi^{n+1}}$. Therefore $[\pi^{n+1}](\alpha_{n+1})^\tau = [\pi^{n+1}](\alpha_{n+1})$; but $[\pi^{n+1}]\alpha_{n+1} = \alpha_o$, so that α_o belongs to Φ_∞. But we have already shown that this is not the case, and so the proof of the lemma is complete.

This lemma implies that $G(H_nL_nF_\infty/L_nF_\infty)$, which is cyclic, has order at least p^{n+1-c}. (2)

The surjection (1) (see above) gives rise to the injection $0 \longrightarrow \mathrm{Hom}((U_n'/\bar{S}_n')^{(1)}, E_{\pi^{n+1}}) \longrightarrow \mathrm{Hom}((U_n'/\bar{C}_n)^{(1)}, E_{\pi^{n+1}})$ of $\mathbb{Z}_p$-$[G_n]$ modules; this gives an injection

$$0 \longrightarrow \mathrm{Hom}((U_n'/\bar{S}_n')^{(1)}, E_{\pi^{n+1}})^{G(F_n/F_o)} \longrightarrow \mathrm{Hom}((U_n'/\bar{C}_{o,n})^{(1)}, E_{\pi^{n+1}})^{G(F_n/F_o)}$$

(where for a $G(F_n/F_o)$ module A, $A^{G(F_n/F_o)}$ denotes the elements of A fixed by $G(F_n/F_o)$).

We saw above that G_o operates on $G(H_nL_nF_\infty/L_nF_\infty)$ via χ. Also any homomorphism $g: G(H_nL_nF_\infty/L_nF_\infty) \longrightarrow E_{\pi^{n+1}}$ satisfies $f^\sigma = f$ for all $\sigma \in G_\infty$. (Let $\tau \in G(H_nL_nF_\infty/L_nF_\infty)$. Then

$$f^\sigma(\tau) = (f(\tau^{\sigma^{-1}}))^\sigma = \kappa(\sigma)f(\kappa(\sigma^{-1})\tau) = f(\tau)$$

since σ acts on $E_{\pi^{n+1}}$ via κ, and on τ via κ also). Therefore there is an injection

$$0 \longrightarrow \mathrm{Hom}(G(H_nL_nF_\infty/L_nF_\infty), E_{\pi^{n+1}}) \longrightarrow \mathrm{Hom}((U_n'/\bar{C}_{o,n})^{(1)}, E_{\pi^{n+1}})^{G(F_n/F_o)}.$$

We may now quickly deduce theorem 2. First, we see that

$$\mathrm{Hom}(Y_\infty^{(1)}, E_{\pi^{n+1}})^\Gamma \simeq \mathrm{Hom}((U_n'/\bar{C}_{o,n})^{(1)}, E_{\pi^{n+1}})^{G(F_n/F_o)},$$

because $$(Y_\infty^{(1)})_{\Gamma_n} \simeq (U_n'/\bar{C}_{o,n})^{(1)}.$$

Also $$\mathrm{Hom}(Y_\infty^{(1)}, E_{\pi^{n+1}})^\Gamma \simeq \mathrm{Hom}(Y_\infty^{(1)}(-1), \mathbb{Z}/p^{n+1}\mathbb{Z})^\Gamma$$

where G_∞ acts trivially on $\mathbb{Z}/p^{n+1}\mathbb{Z}$.

But $$\mathrm{Hom}(Y_\infty^{(1)}(-1), \mathbb{Z}/p^{n+1}\mathbb{Z})^\Gamma \simeq \mathrm{Hom}((Y_\infty^{(1)}(-1))_\Gamma, \mathbb{Z}/p^{n+1}\mathbb{Z}).$$

From (2) above, there is a surjective homomorphism

$$\phi\colon G(H_nL_nF_\infty/L_nF_\infty) \longrightarrow E_{\pi^{n+1-c}};$$

consequently, there is a surjective homomorphism

$$\phi_1\colon (Y_\infty^{(1)}(-1))_\Gamma \longrightarrow \mathbb{Z}/p^{n+1-c}\mathbb{Z}\ .$$

Thus either $g_1(u-1) = h(0) = 0$,

or $\quad |g_1(u-1)|_p \leq p^{c-(n+1)}$.

Since this holds for all n, $g_1(u-1) = 0$.

But this implies that $L(E/K,1) = 0$.

§2. Proof of theorem 5.

The main result of this section is the relation between the rank of the F_o-rational points on E (mod torsion) and the Iwasawa invariants of the Λ-modules X_∞, and $\mathbb{Z}_\infty$.

Suppose X is a Λ-torsion Λ-module. Then it is pseudo isomorphic to a direct sum of the form

$$\Lambda/p^{\mu_1}\Lambda \oplus \ldots \oplus \Lambda/p^{\mu_k}\Lambda \oplus \Lambda/f_1(T)\Lambda \oplus \ldots \oplus \Lambda/f_\ell(T)\Lambda$$

where $\mu_1,\ldots,\mu_k$ are positive integers, and $f_1(T),\ldots,f_\ell(T)$ are distinguished polynomials in Λ, that is, of the form

$$f_i(T) = T^{\lambda_i} + b_{\lambda_i-1}T^{\lambda_i-1} + \ldots + b_o$$

where p divides each b_i, and $\lambda_i = \deg f_i$. Suppose that the Γ_n-invariance of X, that is, $X/\omega_n X$ ($\omega_n = (1+T)^{p^n}-1$), is finite; let p^{e_n} denote its order. Then (see [15] p127 , or [20]) for all sufficiently large n, $e_n = n\sum_{i=1}^{\ell}\lambda_i + p^n\sum_{j=1}^{k}\mu_j + \nu$, where ν is a constant depending only on X. The coefficients of n and p^n are known as the Iwasawa λ- and μ-invariants of X.

We now turn to the proof of theorem 5 and first establish the equality of the invariants: it depends upon the following lemma.

Lemma 4.3 For each $n \geq 0$, the index of $\bar{C}_n'$ in $\bar{S}_n'$ equals the p-part of the class number of F_n.

Proof: Theorem 2 shows that $|[S_n:C_n]|_p = |h_n|_p$, where h_n denotes the class number of F_n. Now $S_n'/C_n' \simeq \bar{S}_n'/\bar{C}_n'$ is a $\mathbb{Z}_p$-module and so is a p-group; furthermore there is an injection $S_n'/C_n' \hookrightarrow S_n/C_n$, so that S_n'/C_n' has order dividing $|h_n|_p^{-1}$. But $S_n'/C_n' \simeq S_n'C_n/C_n$, and

since $S_n/S_n'C_n$ has no p-torsion, we conclude that S_n'/C_n' has order precisely $|h_n|_p^{-1}$ ($S_n/S_n'C_n$ has no p-torsion; because S_n/S_n' has none: for if $x\epsilon S_n$ and $x^p\epsilon S_n'$, then $x \equiv x^p \equiv 1 \bmod p_n$, so that $x\epsilon S_n'$), q.e.d.

We consider the exact sequences

$$0 \longrightarrow G(M_n/L_nF_\infty) \longrightarrow G(M_n/F_\infty) \longrightarrow G(L_nF_\infty/F_\infty) \longrightarrow 0$$

$$0 \longrightarrow \bar{S}_n'/\bar{C}_n' \longrightarrow U_n'/\bar{C}_n' \longrightarrow U_n'/\bar{S}_n' \longrightarrow 0.$$

Now $G(M_n/L_nF_\infty)$ is isomorphic to $U_n'/\bar{S}_n'$ as a $G(F_n/K)$-module (see [6], theorem 11); these are both finite groups, because the p-adic rank of the global units of F_n equals the $\mathbb{Z}$-rank (this is Leopoldt's conjecture which holds because F_n is abelian over K; see [2]). Also the order of $G(L_nF_\infty/F_\infty) \simeq G(L_n/F_n)$ is $|h_n|_p^{-1} = [\bar{S}_n':\bar{C}_n']$.

Recalling that

$$X_\infty/\omega_n X_\infty = X_n = G(M_n/F_\infty)$$

and

$$Z_\infty/\omega_n Z_\infty = Z_n = U_n'/\bar{C}_n' ,$$

we conclude that X_n and Z_n have the same finite order for every n. Consequently the λ- and μ-invariants are equal; denote these by λ and μ respectively.

To calculate a lower bound for λ, we need the following result (a similar result is due to Bashmakov [29]).

Let $T = T_\pi = \varprojlim_{\pi^{n+1}} E$ denote the Tate module . Let r be the rank of $E(F_o)$ as an o-module, and let $P_1,\ldots,P_r$ be a basis for $E(F_o)$ (modulo torsion) over o. Let A denote the o-submodule of $E(F_o)$ generated by $P_1,\ldots,P_r$; let $\bar{A}$ denote the set of points P on E, defined over the algebraic closure of F_o, for which there

exists an integer n (depending upon P) such that $\pi^n P$ lie in A; note that $\bar{A}$ contains all the π-power division points. Let $H = F_\infty(\bar{A})$ be the field obtained by the adjunction of the coordinates of the points in A; it is a Galois extension of F_o. We wish to describe the Galois group $G(H/F_\infty)$. Recall that $\Gamma = G(F_\infty/F_o)$.

Lemma 4.4 $G(H/F_\infty)$ is isomorphic, as a Γ-module, to a Γ-submodule of T_π^r.

Proof: For each $i = 1,\ldots,r$, let $P_{n,i}$ $(n = 0,1,2,\ldots)$ denote the sequence in $\bar{A}$ defined by the relations

$$P_{o,i} = P_i,\ \pi P_{n+1,i} = P_{n,i}\ (n \geq 0).$$

For each σ in $G(H/F_\infty)$, define $\langle \sigma, P_i \rangle_n = \sigma P_{n,i} - P_{n,i}$. The sequence $\langle \sigma, P_i \rangle_n$ $(n = 1,2,\ldots)$ lies in T and is independent of the choice of sequence $(P_{n,i})$. Thus if $\tilde{\gamma}$ is any extension of γ to an element of $G(H/F_o)$ the image σ^γ of σ under γ (namely $\tilde{\gamma}\sigma\tilde{\gamma}^{-1}$) is mapped to the sequence $\langle \sigma^\gamma, P_i \rangle_n = \gamma \langle \sigma, \tilde{\gamma}^{-1} P_i \rangle_n = \gamma \langle \sigma, P_i \rangle_n$. We thus obtain a Γ-injection of $G(H/F_\infty)$ into T^r.

Clearly $G(H/F_\infty)$ has $\mathbb{Z}_p$-rank at most r; we now show it has $\mathbb{Z}_p$-rank at least r and so is of finite index in T^r. For any point P in $E(F_o)$, let Q be such that $\pi^n Q = P$ for some integer n.

Let $\bar{F}_o$ denote the algebraic closure of F_o. The map

$$\begin{array}{ccc} G(\bar{F}_o/F_o) & \longrightarrow & E_{p^\infty} \\ \sigma & \longmapsto & \sigma Q - Q \end{array}$$

is a well defined cocycle. Performing a similar construction for $E(F_\infty)$, we obtain the following commutative diagram with exact rows and columns:

$$\begin{array}{ccccccc} 0 & \longrightarrow & * & \longrightarrow & H^1(G(F_\infty/F_0),E_{p^\infty}) & \longrightarrow & \cdots \\ & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & E(F_0)\otimes K_p/o_p & \longrightarrow & H^1(G(\bar{F}_0/F_0),E_{p^\infty}) & \longrightarrow & \cdots \\ & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & E(F_\infty)\otimes K_p/o_p & \longrightarrow & H^1(G(\bar{F}_\infty/F_\infty),E_{p^\infty}) & \longrightarrow & \cdots \end{array}$$

Now because γ-1 is an automorphism of E_{p^∞}, Sah's lemma [19]shows that $H^1(\Gamma,E_{p^\infty}) = 0$. Hence $E(F_0)\otimes K_p/o_p \simeq (K_p/o_p)^r$ injects into $H^1(G(\bar{F}_\infty/F_\infty),E_{p^\infty}) = \mathrm{Hom}(G(\bar{F}_\infty/F_\infty),E_{p^\infty})$; we conclude that $G(H/F_\infty)$ has $\mathbb{Z}_p$-rank at least r, and the proof of the lemma is complete.

Let W denote the Γ-submodule of T^r to which $G(H/F_\infty)$ is isomorphic. Lemma 33 of [7] shows that H is contained in M_∞, so there is a surjection f: $G(M_\infty/F_\infty) \longrightarrow W$.

According to the structure theorem, $X_\infty = G(M_\infty/F_\infty)$ may be decomposed as a direct sum $X_\infty = X_\infty' \oplus X_\infty''$ where X_∞' is a p-torsion group (i.e. annihilated by a sufficiently large power of p) and X_∞'' is a direct sum $\oplus_j \Lambda/f_j(T)\Lambda$ of a finite number of quotients by distinguished polynomials f_j. Since W has no p-torsion, $f(X_\infty') = 0$ and $f(X_\infty) = f(X_\infty'')$; the λ-invariants of X_∞ and X_∞'' are the same, and the μ-invariant of X_∞'' is zero. The surjection f induces a surjection

$$X_\infty''/\omega_n X_\infty'' \longrightarrow W/(\gamma^{p^{n+1}}-1)W$$

(Recall that γ is a topological generator of γ and acts on X_∞ via $\gamma.x = (1+T)x$, for $x\in X_\infty$). Since W is of finite index in T^r, $W/(\gamma^{p^{n+1}}-1)W$ has order p^{rn-m} (for some constant m depending only on W) for sufficiently large n. Thus the λ-invariant of X_∞ is at least as large as r. This completes the proof of theorem 5.

References

[1] Birch, B. and Swinnerton-Dyer, P.: Note on elliptic curves II. J. Reine Angew. Math. 218, 79-108 (1965).

[2] Brumer, A.: On the units of algebraic number fields. Mathematika 14, 121-124 (1967).

[3] Cassels, J.W.S.: Diophantine equations with special reference to elliptic curves. Survey article. J.London Math. Soc. 41, 193-291 (1966).

[4] Coates, J.: p-adic L-functions and Iwasawa's theory. In: Algebraic number fields. ed. A. Frohlich. Academic Press, 1977.

[5] Coates, J. and Sinnott, W.: Integrality properties of the values of partial zeta functions. Proc. London Math. Soc. (3) 34, 365-384 (1977).

[6] Coates, J. and Wiles, A.: Kummer's criterion for Hurwitz numbers. Paper, Kyoto int. symp. 1976, 9-23 (1977).

[7] Coates, J. and Wiles, A.: On the conjecture of Birch and Swinnerton-Dyer. Inventiones Math. 39, 223-251 (1977).

[8] Coates, J. and Wiles, A.: On p-adic L-functions and elliptic units. J. Australian Math. Soc. (A), 26, 1-25 (1978).

[9] Deuring, M.: Die Zetafunktionen einer algebraischen Kurve vom Geschlechter Eins, I, II, III, IV. Nachr. Akad. Wiss Göttingen 85-94 (1953); 13-42 (1955); 37-76 (1956); 55-80 (1957).

[10] Gillard, R.: Remarques sur Les Unités Cyclotomiques et les Unités Elliptiques. J. Number Theory 11, 21-48 (1979).

[11] Iwasawa, K.: On some modules in the theory of cyclotomic fields. J. Math. Soc. Japan 16, 42-82 (1964).

[12] Iwasawa, K.: On p-adic L-functions. Annals of Math. 89, 198-205 (1969).

[13] Kubert, D. and Lang, S.: Units in the modular function field. In: Modular functions of one variable V. Lecture Notes in Math. 601 Springer Verlag 1977.

[14] Lang, S.: Elliptic functions. Addison-Wesley, 1973.

[15] Lang, S.: Cyclotomic fields. Springer-Verlag, 1978.

[16] Lubin, J., Tate, J.: Formal complex multiplication in local fields. Ann. Math. 81, 380-387 (1965).

[17] Ramachandra, K.: Some applications of Kronecker's limit formulas. Ann. of Math. 80, 104-148 (1964).

[18] Robert, G.: Unités Elliptiques. Bull. Soc. Math. France, Memoire 36 (1973).

[19] Sah, H.: Automorphisms of finite groups. J. Algebra 10, 47-68 (1968).

[20] Serre, J.P.: Classes des corps cyclotomiques, d'après Iwasawa. Seminaire Bourbaki, 1958.

[21] Serre, J.P.: Corps Locaux. Hermann Paris, 1962.

[22] Serre, J.P. and Tate, J.: Good reduction of abelian varieties. Ann. Math. 88, 492-517 (1968).

[23] Shimura, G.: Introduction to the arithmetic theory of automorphic forms. Pub. Math. Soc. Japan 11 (1971).

[24] Siegel, C.: Lecture notes on advanced analytic number theory. Tata Inst. of Fund. Research, Bombay (1961).

[25] Sinnott, W.: On the Stickleberger ideal and the circular units of a cyclotomic field. Ann. Math. (2) 108, 107-134 (1978).

[26] Tate, J.: The Arithmetic of Elliptic Curves. Inventiones Math. 23, 179-206 (1974).

[27] Tate, J.: p-divisible groups. In: Proc. Conf. on Local Fields at Driebergen, 1966. Ed. T.A. Springer, Springer-Verlag, 1967.

[28] Tate, J.: Algorithm for determining the type of a singular fibre in an elliptic pencil. In: Modular functions of one variable IV. Lecture Notes in Math. 476, Springer-Verlag, 1975.

[29] Bashmakov, M.I.: The cohomology of abelian varieties over a number field. Russian Maths. Surveys, Vol.27, no.6 (1972).

[30] Lang, S.: Elliptic curves: Diophantine analysis. Springer-Verlag, (1978).