Vol. 90, No. 3 DUKE MATHEMATICAL JOURNAL © 1997

EXPLICIT ELLIPTIC UNITS, I

FARSHID HAJIR AND FERNANDO RODRIGUEZ VILLEGAS

Elliptic units are units in abelian extensions of an imaginary quadratic field $K \subset \mathbb{C}$ that are obtained as values of certain modular functions at points in $K \cap \mathscr{H}$ (with $\mathscr{H}$ denoting the upper half-plane). In this series of papers, we are concerned with those elliptic units that are expressible as ratios of values of the Dedekind eta function η. In particular, we will describe explicitly how the absolute Galois group of K acts on these units. This action is completely characterized by the Shimura reciprocity law [Sh], but the calculations are greatly complicated by the presence of 24th roots of unity in the transformation formulas for η.

The subject of values of particular modular functions at points in $K \cap \mathscr{H}$—the description of their algebraic and Galois properties, the explicit determination of their minimal polynomials, and so on—is very old. We have not attempted the monumental task of sorting out the history of these *singular moduli*, as they were classically known, or that of providing a full bibliography. Instead, we will just mention the following.

In his 1828 paper on elliptic functions [Ab, *Oeuvres*, pp. 380–382], Abel proves, among many other things, the following identity, here written in modern notation:

$$\frac{\eta^2(\sqrt{-5}/2)}{2\eta^2(2\sqrt{-5})} = \frac{1+\sqrt{5}}{2} + \sqrt{\frac{1+\sqrt{5}}{2}}.$$

(The left-hand side is an example of an elliptic unit; its minimal polynomial is $x^4 - 2x^3 - 2x^2 - 2x + 1$.)

In the 1930s, G. N. Watson computed the minimal polynomials of a number of ratios of values of η by an ad hoc, trial and error process for the selection of the appropriate 24th roots of unity. He managed to calculate in this way, working by hand with expansions of up to 10 decimal places, many examples of degrees less than 20. In the third paper of his *Singular Moduli* series, he remarks [Wa, p. 89 footnote], "I have dealt successfully with $n = 479$ and $n = 599$; for each of these values of n, $h = 25$ [the degree of the equation] and the selection has to be made from $3^{12} = 531,441$ values. Each of the corresponding computations required twelve hours' work." Weber's book [We] contains many of these polynomials for degrees less than 10.

Received 2 May 1996.

The second author was supported in part by a grant from the National Science Foundation and by a fellowship from the John Simon Guggenheim Memorial Foundation.

It is precisely the efficient management of these 24th roots of unity that forms the core of this paper. We may always raise η to the 24th power and avoid these problems altogether, but there are many reasons why this is not convenient. For example, (1) the group of units obtained would not be optimal, in the sense that the index of this group in the full group of units of the ring class field contains extraneous factors (powers of 2 and 3 not arising from the class number of this field), and (2), in computational terms, the size of the coefficients of the minimal polynomial of the units obtained, as well as the precision needed for calculating them, would be unnecessarily large. This last point is important if one wants, for example, to calculate efficiently explicit generators for ring class fields of K of small height or, say, the minimal polynomial of $j(z)^{1/3}$ ($z \in K \cap \mathscr{H}$), as in the elliptic-curve-primality-proving algorithm of Atkin-Morain [AM]. Also, knowing the precise field where these ratios of values of η lie is crucial for Heegner's original proof of Gauss's conjecture on imaginary quadratic fields with class number 1.

The plan of the paper is as follows: §1 is essentially a review of some elementary facts about the group $GL_2(\mathbb{Z}/12\mathbb{Z})$ and their relation to the multiplier of η^2. In §2, we consider an order $\mathfrak{o}$ of K with corresponding ring class field H and define $\eta(\mathscr{A})$ for an $\mathfrak{o}$-ideal $\mathscr{A}$ (satisfying some mild restrictions). Let us call a product of integral powers of ratios $\eta(\mathscr{A})/\eta(\mathfrak{o})$ simply an "η-quotient"; in this section we describe the action of Galois on them. In §3, we introduce and study a certain character κ from $(\mathfrak{o}/12\mathfrak{o})^*$ into the group of 12th roots of unity. A central theme of this paper, namely, that κ encodes the Galois properties of η-quotients, is illustrated in §4, where we prove again some classical results about singular moduli.

We state and prove the main theorem in §5: an η-quotient α always generates a Kummer extension of the ring class field H, and we give explicitly its associated character in terms of κ, as well as the expressions for its Galois conjugates as η-quotients. In particular, one immediately reads off the degree of $H(\alpha)/H$. We verify that what we obtain is sharp, in the sense that this degree cannot be lowered by considering $\zeta\alpha$, with ζ a root of unity.

The final section contains various applications and illustrations of the main theorem; some special cases of these have appeared throughout the literature, including [H1], but usually in weaker and less explicit form. The majority of the section concerns a detailed study of the units appearing in the first limit formula of Kronecker [Kr]. Finally, we give a brief indication of how to use our results to carry out numerical calculations, such as finding a defining equation of small height for the ring class field H, as well as finding the minimal polynomial of $j(\mathfrak{o})^{1/3}$ for many types of $\mathfrak{o}$. (The remaining cases will be treated in the sequel to this paper in which we will consider more general η-quotients, $\eta(\mathscr{A}')/\eta(\mathscr{A})$, where the endomorphism rings of $\mathscr{A}, \mathscr{A}'$ are distinct.) We end the paper with some numerical examples.

Notation. For a ring R with unit, R^* is the group of its invertible elements. For a positive integer n, $\boldsymbol{\mu}_n$ is the group of nth roots of unity in $\mathbb{C}^*$, whose ele-

ments we write as $e_n(a) = e^{2\pi ia/n}$ with $a \in \mathbb{Z}$. For a number field F, $\mathfrak{O}_F$ and μ_F are, respectively, the ring of integers and the group of roots of unity of F. The Dirichlet characters we will need are the trivial character χ_1 and the quadratic characters χ_4 and χ_8, of the indicated conductor, defined by $\chi_4(a) = (-1/a)$, $\chi_8(a) = (-2/a)$ (a odd), where $(\frac{\cdot}{\cdot})$ is the Kronecker symbol. For a group G and right G-module M, we have the group of 1-cocycles $Z^1(G, M)$, consisting of maps $\lambda : G \to M$ such that $\lambda(\sigma\tau) = \lambda(\sigma)^\tau \lambda(\tau)$ for all $\sigma, \tau \in G$, as well as the subgroup $B^1(G, M)$ of 1-coboundaries, namely, the 1-cocycles of the form $\sigma \mapsto m^{\sigma-1}$ with fixed $m \in M$. We denote the class of a 1-cocycle λ in the cohomology group $H^1(G, M) = Z^1(G, M)/B^1(G, M)$ by $[\lambda]$. For an integer a, we put $\hat{a} = \left(\begin{smallmatrix} a & 0 \\ 0 & 1 \end{smallmatrix}\right)$; we write $1_2 = \hat{1}$ for the identity matrix. For odd a, let $a^\star = \chi_4(a)a$. The square root symbol will denote the usual branch of square root, for instance, $\sqrt{a^\star} = e_8(a-1)\sqrt{a}$. More notation will be introduced in the body of the paper, especially in §2.1.

1. The multiplier system of $\eta^2(z)$. Dedekind's eta function η is defined by

$$\eta(z) = e^{2\pi iz/24} \prod_{n=1}^{\infty} (1 - e^{2\pi izn}), \qquad \Im(z) > 0.$$

As is well known (e.g., [Si, p. 17]), η^2 satisfies the transformation formula

$$\eta^2(M \circ z) = \phi(M)(\gamma z + \delta)\eta^2(z), \qquad M = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in SL_2(\mathbb{Z}), \tag{1}$$

where $\circ$ denotes the standard action of $SL_2(\mathbb{Z})$ on the upper half-plane, and $\phi(M)$ is independent of z. It follows immediately from (1) that ϕ defines a group homomorphism $SL_2(\mathbb{Z}) \to \mathbb{C}^*$, and that $\phi(T) = e_{12}(1)$, where $T = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$. In this section, we point out some properties of ϕ we will need and give a simple algorithm for computing it. The arguments are group theoretical.

First, it is easy to see that any character $\psi : SL_2(\mathbb{Z}) \to \mathbb{C}^*$ is determined by $\psi(T)$. Indeed, let $S = \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$ and note that $(ST)^3 = S^4 = 1_2$. Then $\psi(S)^3 = \psi(T)^{-3}$ and $\psi(S)^4 = 1$ together imply that $\psi(S) = \psi(T)^3$. But S and T generate $SL_2(\mathbb{Z})$; hence ψ is completely determined by its value on T. Moreover, $\psi(T)^{12} = \psi(S)^4 = 1$; therefore any character of $SL_2(\mathbb{Z})$ has order dividing 12. For our character $\phi : SL_2(\mathbb{Z}) \to \mu_{12}$, we have $\phi(T) = e_{12}(1)$, $\phi(S) = e_{12}(3)$, $\phi(-1_2) = \phi(S^2) = -1$.

For the remainder of this section, let $N = 3$ or 4. Define characters ϕ_N of order N by $\phi = \phi_3/\phi_4$. It is easy to establish that ϕ_N factors through the reduction map $SL_2(\mathbb{Z}) \to SL_2(\mathbb{Z}/N\mathbb{Z})$. To see this, let $\Gamma_N = SL_2(\mathbb{Z}/N\mathbb{Z})$. A simple calculation

shows that Γ_4 has order 48, with commutator subgroup Γ_4' isomorphic to A_4, the alternating group on four letters. The subgroup generated by T has order 4, and acts by conjugation on Γ_4', giving the semidirect product decomposition $\Gamma_4 = \langle T \rangle \rtimes \Gamma_4'$. Hence, there is a unique character of Γ_4 into μ_4, mapping T to $\phi_4(T) = e_4(1)$, whose composition with the reduction map above is none other than ϕ_4. Similarly, Γ_3 has order 24, with commutator subgroup isomorphic to the quaternion group of order 8, and again, $\Gamma_3 = \langle T \rangle \rtimes \Gamma_3'$.

Every $M \in SL_2(\mathbb{Z}/N\mathbb{Z})$ can be taken to an element in the commutator subgroup via left multiplication by a unique power of T; that is, $T^a M \in \Gamma_N'$ for a unique $a \pmod N$, and then $\phi_N(M) = \phi_N(T)^{-a}$. Together with the elements of Γ_N' (see Tables 1 and 2), this gives an algorithm for computing $\phi(M)$ for any $M \in SL_2(\mathbb{Z})$. Although we will not need them, explicit formulas using Dedekind sums or of the type $\phi_N(M) = e^{-2\pi i p_N(M)/N}$ where $p_N(M)$ is a polynomial in the entries of M can be given. For example, with $M = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$, Herglotz [He] gave the following:

$$p_3(M) = ac(b^2 + 1) + bd(a^2 + 1)$$

$$p_4(M) = (b^2 - a + 2)c + (a^2 - b + 2)\,d + ad\,.$$

TABLE 1
Commutator subgroup of $SL_2(\mathbb{Z}/4\mathbb{Z})$

$\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$	$\left(\begin{smallmatrix} -1 & 2 \\ 0 & -1 \end{smallmatrix}\right)$	$\left(\begin{smallmatrix} 1 & 2 \\ 2 & 1 \end{smallmatrix}\right)$	$\left(\begin{smallmatrix} -1 & 0 \\ 2 & -1 \end{smallmatrix}\right)$
$\left(\begin{smallmatrix} -1 & 1 \\ -1 & 0 \end{smallmatrix}\right)$	$\left(\begin{smallmatrix} -1 & -1 \\ 1 & 0 \end{smallmatrix}\right)$	$\left(\begin{smallmatrix} 0 & -1 \\ 1 & -1 \end{smallmatrix}\right)$	$\left(\begin{smallmatrix} 0 & 1 \\ -1 & -1 \end{smallmatrix}\right)$
$\left(\begin{smallmatrix} 1 & 1 \\ 1 & 2 \end{smallmatrix}\right)$	$\left(\begin{smallmatrix} 1 & -1 \\ -1 & 2 \end{smallmatrix}\right)$	$\left(\begin{smallmatrix} 2 & 1 \\ 1 & 1 \end{smallmatrix}\right)$	$\left(\begin{smallmatrix} 2 & -1 \\ -1 & 1 \end{smallmatrix}\right)$

TABLE 2
Commutator subgroup of $SL_2(\mathbb{Z}/3\mathbb{Z})$

$\pm\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$	$\pm\left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$	$\pm\left(\begin{smallmatrix} 1 & 1 \\ 1 & -1 \end{smallmatrix}\right)$	$\pm\left(\begin{smallmatrix} -1 & 1 \\ 1 & 1 \end{smallmatrix}\right)$

Incidentally, these tables appear in Hurwitz's thesis [Hu], which is somewhat in the same spirit as this paper.

We now make a study of the "cocycle liftings" of ϕ to $GL_2(\mathbb{Z}/12\mathbb{Z})$; these will play a key role in §3. Consider the exact sequence

$$1 \to \Gamma_N \to GL_2(\mathbb{Z}/N\mathbb{Z}) \xrightarrow{\det} (\mathbb{Z}/N\mathbb{Z})^* \to 1\,,$$

which admits a splitting $(\mathbb{Z}/N\mathbb{Z})^* \hookrightarrow GL_2(\mathbb{Z}/N\mathbb{Z})$ given by $a \mapsto \hat{a} = \begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix}$. This gives a natural (right) action of $(\mathbb{Z}/N\mathbb{Z})^*$ on Γ_N by $M.a = \hat{a}M\hat{a}$ (note that $\hat{a}$ is its own inverse). We therefore have $GL_2(\mathbb{Z}/N\mathbb{Z}) = (\mathbb{Z}/N\mathbb{Z})^* \rtimes \Gamma_N$. Also, we let $(\mathbb{Z}/N\mathbb{Z})^*$ act on $\boldsymbol{\mu}_N$ by $\zeta.a = \zeta^a$.

LEMMA 1. *The character $\phi_N : \Gamma_N \to \boldsymbol{\mu}_N$ is $(\mathbb{Z}/NZ)^*$-equivariant.*

Proof. It is enough to check this on the generators T, S. Since $N = 3$ or 4, $(\mathbb{Z}/N\mathbb{Z})^* = \{\pm 1\}$. We then only need to verify that $\phi_N(T.(-1)) = \phi_N(T)^{-1}$ and $\phi_N(S.(-1)) = \phi_N(S)^{-1}$, both of which are clear, since $T.(-1) = T^{-1}$ and $S.(-1) = S^{-1}$. We also remind the reader that $\phi(-1_2) = -1$; hence, for $a \in (\mathbb{Z}/N\mathbb{Z})^*$,

$$\phi_N\left(\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}\right) = \begin{cases} \left(\frac{-1}{a}\right) & \text{if } N = 4 \\ 1 & \text{if } N = 3. \end{cases}$$ ■

Definition 2. Let $\delta_\pm$ be the 1-cocycles on $(\mathbb{Z}/4\mathbb{Z})^*$ with values in $\boldsymbol{\mu}_4$ given by

$$\delta_\pm(1) = 1, \delta_\pm(-1) = \begin{cases} 1 & \text{for } + \\ i & \text{for } -. \end{cases}$$

LEMMA 3. (i) $Z^1((\mathbb{Z}/4\mathbb{Z})^*, \boldsymbol{\mu}_4) \cong (\mathbb{Z}/2\mathbb{Z})^2$ *with basis* δ_-, χ_4.
(ii) $B^1((\mathbb{Z}/4\mathbb{Z})^*, \boldsymbol{\mu}_4) \cong \mathbb{Z}/2\mathbb{Z}$ *with basis* χ_4.
(iii) $H^1((\mathbb{Z}/4\mathbb{Z})^*, \boldsymbol{\mu}_4) \cong \mathbb{Z}/2\mathbb{Z}$ *with basis* $[\delta_-]$.
(iv) $H^1((\mathbb{Z}/3\mathbb{Z})^*, \boldsymbol{\mu}_3)$ *is trivial.*

Proof. (i) The conditions for a map $\delta : (\mathbb{Z}/4\mathbb{Z})^* \to \boldsymbol{\mu}_4$ to be a 1-cocycle are just $\delta(1) = 1, \delta(-1)^{-1}\delta(-1) = 1$; that is, $\delta(-1)$ is free to take any value in $\boldsymbol{\mu}_4$. The result follows. For (ii) and (iii), note that $\chi_4(a) = i^{a-1}$. Finally, (iv) is clear, since the group and the module have coprime cardinality. ■

Definition 4. For $\delta \in Z^1((\mathbb{Z}/4\mathbb{Z})^*, \boldsymbol{\mu}_4)$, define $\phi_\delta : GL_2(\mathbb{Z}/4\mathbb{Z}) \to \boldsymbol{\mu}_4$ by

$$\phi_\delta(M) = \delta(m)\phi_4(\hat{m}M), \qquad M \in GL_2(\mathbb{Z}/4\mathbb{Z}), \qquad \det M = m. \tag{2}$$

PROPOSITION 5. (i) *For every $\delta \in Z^1((\mathbb{Z}/4\mathbb{Z})^*, \boldsymbol{\mu}_4)$, $\phi_\delta \in Z^1(GL_2(\mathbb{Z}/4\mathbb{Z}), \boldsymbol{\mu}_4)$, and ϕ_δ coincide with ϕ_4 when restricted to $SL_2(\mathbb{Z}/4\mathbb{Z})$.*
(ii) *Conversely, if $\tilde{\phi} \in Z^1(GL_2(\mathbb{Z}/4\mathbb{Z}), \boldsymbol{\mu}_4)$ coincides with ϕ_4 when restricted to $SL_2(\mathbb{Z}/4\mathbb{Z})$, then $\tilde{\phi} = \phi_\delta$ for some $\delta \in Z^1((\mathbb{Z}/4\mathbb{Z})^*, \boldsymbol{\mu}_4)$.*
(iii) $[\phi_\delta] = [\phi_{\delta'}]$ *if and only if* $[\delta] = [\delta']$.

Proof. (i) Note that $\phi_\delta(\hat{m}) = \delta(m)\phi_4(1_2) = \delta(m)$. We now show that ϕ_δ is a 1-cocycle. For $M_j \in GL_2(\mathbb{Z}/4\mathbb{Z}), m_j = \det M_j, j = 1, 2$, the identity

$$\widehat{m_1 m_2} M_1 M_2 = ((\widehat{m_1} M_1).m_2)(\widehat{m_2} M_2),$$

combined with Lemma 1, gives

$$\begin{aligned}\phi_\delta(M_1M_2) &= \delta(m_1m_2)\phi_4(\widehat{m_1m_2}M_1M_2)\\ &= \delta(m_1m_2)\phi_4(((\widehat{m_1}M_1).m_2)(\widehat{m_2}M_2))\\ &= \delta(m_1m_2)\phi_4(\widehat{m_1}M_1)^{m_2}\phi_4(\widehat{m_2}M_2)\\ &= \frac{\delta(m_1m_2)}{\delta(m_1)^{m_2}\delta(m_2)}\phi_\delta(M_1)^{m_2}\phi_\delta(M_2)\\ &= \phi_\delta(M_1)^{m_2}\phi_\delta(M_2).\end{aligned}$$

(ii) Let $\delta(m) = \tilde{\phi}(\hat{m})$. Then $\delta \in Z^1((\mathbb{Z}/4\mathbb{Z})^*, \mu_4)$, and for a determinant m matrix $M \in GL_2(\mathbb{Z}/4\mathbb{Z})$,

$$\begin{aligned}\tilde{\phi}(M) &= \tilde{\phi}(\hat{m})\tilde{\phi}(\hat{m}M)\\ &= \delta(m)\phi_4(\hat{m}M)\\ &= \phi_\delta(M).\end{aligned}$$

(iii) By restriction to the subgroup $\{\hat{1}, \widehat{-1}\}$, we see that $\phi_\delta, \phi_{\delta'}$ are not cohomologous, whenever δ, δ' are not. Conversely, if $\zeta \in \mu_4$ splits δ/δ', then it also splits $\phi_\delta/\phi_{\delta'}$. ■

Remark. A 1-cocycle $\tilde{\phi}$ lifting ϕ_4 to $GL_2(\mathbb{Z}/4\mathbb{Z})$ is never a character. Otherwise, we would have $\tilde{\phi}(M_2)^{\det M_1 - 1} = 1$ for all $M_1, M_2 \in GL_2(\mathbb{Z}/4\mathbb{Z})$; in particular, $\tilde{\phi}(M_2)^2 = 1$ for all M_2. This contradicts the fact that the restriction to $SL_2(\mathbb{Z}/4\mathbb{Z})$ of $\tilde{\phi}$, namely, ϕ_4, is surjective onto μ_4. However, *abelian* subgroups of $GL_2(\mathbb{Z}/4\mathbb{Z})$ admit character lifts of ϕ_4, as we now show.

Definition 6. Put $\phi_\pm = \phi_{\delta_\pm}$.

Note that ϕ_+, ϕ_- represent all 1-cohomology classes of lifts of ϕ_4 to $GL_2(\mathbb{Z}/4\mathbb{Z})$.

PROPOSITION 7. *Let G be a group and $\rho : G \to GL_2(\mathbb{Z}/4\mathbb{Z})$ a representation with abelian image. Then*

(i) *for some choice of sign $\varepsilon = \pm$, the map $\varkappa_\rho = \phi_\varepsilon \circ \rho$ is a character of G;*

(ii) *if $\mathrm{Im}(\rho) \not\subseteq SL_2(\mathbb{Z}/4\mathbb{Z})$, then $\varkappa_\rho^2 = 1$.*

Proof. We may assume $\mathrm{Im}(\rho) \not\subseteq SL_2(\mathbb{Z}/4\mathbb{Z})$, the other case being trivial. For $M_1, M_2 \in \mathrm{Im}(\rho)$, $\phi_\pm(M_1M_2) = \phi_\pm(M_1)^{m_2}\phi_\pm(M_2) = \phi_\pm(M_2)^{m_1}\phi_\pm(M_1)$, since M_1, M_2 commute; hence

$$\phi_\pm(M_1)^{1-m_2} = \phi_\pm(M_2)^{1-m_1}. \tag{3}$$

Take any $M_2 \in \mathrm{Im}(\rho)$ with determinant $m_2 = -1$, and put $\varepsilon = \phi(\widehat{m_2}M_2)^2 \in \{+,-\}$. For this choice of sign, we have

$$\begin{aligned}\phi_\varepsilon(M_2)^2 &= \delta_\varepsilon(m_2)^2\phi_4(\widehat{m_2}M_2)^2\\ &= \varepsilon\delta_\varepsilon(-1)^2\\ &= \begin{cases}1 & \text{if } \varepsilon = +\\ -i^2 & \text{if } \varepsilon = -\end{cases}\\ &= 1.\end{aligned}$$

By (3), for any $M_1 \in \mathrm{Im}(\rho)$,

$$\phi_\varepsilon(M_1)^2 = \phi_\varepsilon(M_2)^{1-m_1} = 1\,,$$

since $1 - m_1$ is even. In other words, $\phi_\varepsilon \circ \rho$ is a 1-cocycle taking values in μ_2, which implies that it is a character. Incidentally, for the other choice of sign, we have $\phi_{-\varepsilon}(M_2)^2 = \varepsilon\delta_{-\varepsilon}(-1)^2 = -1$. This shows that $\phi_{-\varepsilon}$ is not a character, because by the cocycle property, $\phi_{-\varepsilon}(M_2^2) = \phi_{-\varepsilon}(M_2)^{-1}\phi_{-\varepsilon}(M_2) = 1$. ■

Remark. When $\mathrm{Im}(\rho) \not\subseteq SL_2(\mathbb{Z}/4\mathbb{Z})$, a different choice of cocycle representative would give $\varkappa_\rho \cdot \chi_4 \circ \det$ instead of $\varkappa_\rho$.

2. Galois properties of eta-quotients

2.1. Basic setup and notation. In this section, for the reader's convenience, we recall various classical results concerning orders in an imaginary quadratic field and set up some additional notation that we will use throughout the paper.

We fix an order $\mathfrak{o}$ of discriminant $-d$ in an imaginary quadratic field $K \subset \mathbb{C}$. With a bar we denote complex conjugation in $\mathbb{C}$ and also its restriction to K, and with $\mathbb{N}$, the norm map in $K/\mathbb{Q}$. For an ideal $\mathscr{A} \subset \mathfrak{o}$ (by ideal we will always mean an integral ideal unless otherwise stated), we let $\mathbb{N}(\mathscr{A}) = [\mathfrak{o} : \mathscr{A}]$ be its norm. We say $\mathscr{A}$ is *proper* if $\mathrm{End}_K(\mathscr{A}) = \mathfrak{o}$; this is equivalent to $\mathscr{A}$ being invertible, in which case $\mathscr{A}\bar{\mathscr{A}} = \mathbb{N}(\mathscr{A})\mathfrak{o}$. Products of proper ideals are proper. We remark that if $\mathbb{N}(\mathscr{A})$ is prime to $[\mathfrak{O}_K : \mathfrak{o}]$, then $\mathscr{A}$ is automatically proper. Also, the norm map is multiplicative on proper ideals (that is, $\mathbb{N}(\mathscr{A}\mathscr{A}') = \mathbb{N}(\mathscr{A})\mathbb{N}(\mathscr{A}')$), but not necessarily so on arbitrary ideals. An ideal $\mathscr{A} \subset \mathfrak{o}$ is *primitive* if it is not of the form $m\mathscr{A}'$ for some integer $m > 1$ and some $\mathfrak{o}$-ideal $\mathscr{A}'$. For example, if $\mathfrak{o}' \subset \mathfrak{o}$ is a suborder of index r, then $r\mathfrak{o}$ is a primitive $\mathfrak{o}'$-ideal, though not proper, and it is a proper $\mathfrak{o}$-ideal, though not primitive.

For an ideal $\mathscr{F} \subset \mathfrak{o}$, we let $I^*(\mathscr{F})$ be the set of proper, primitive, integral ideals of $\mathfrak{o}$ coprime to $\mathscr{F}$. We also let $P^*(\mathscr{F})$ be the principal ideals in $I^*(\mathscr{F})$; that is, those of the form $\mu\mathfrak{o}$ for $\mu \in \mathfrak{o}$. Let $\mathrm{Cl}(\mathfrak{o})$ be the ideal class group of $\mathfrak{o}$, namely, the

quotient of the group of proper fractional ideals of $\mathfrak{o}$ by the subgroup of principal ones. To lighten the notation, we write $\mu \in P^\star(\mathscr{F})$ instead of $(\mu) \in P^\star(\mathscr{F})$ and, for integers m, $I^\star(m), P^\star(m)$ instead of $I^\star(m\mathfrak{o}), P^\star(m\mathfrak{o})$.

We let K^{ab} denote the maximal abelian extension of K in $\mathbb{C}$. If $F \subset K^{ab}$ is a finite extension of K, and $\mathscr{A}$ is a proper ideal of $\mathfrak{o}$ prime to $\mathrm{disc}(F/K)$, we let $\sigma_{\mathscr{A}}$ denote the corresponding Artin-Frobenius automorphism of F/K. It is not hard to show that, for any ideal $\mathscr{F}$ of $\mathfrak{o}$, the set $I^\star(\mathscr{F}\,\mathrm{disc}(F/K))$ covers the Galois group $\mathrm{Gal}(F/K)$ via the Artin map. In fact, every $\sigma \in \mathrm{Gal}(F/K)$ equals $\sigma_{\mathscr{P}}$, with $\mathscr{P} \in I^\star(\mathscr{F}\,\mathrm{disc}(F/K))$ a prime ideal, infinitely often by a theorem of Chebotarev. For $\mu \in \mathfrak{o}$ and $\mathscr{A} \in I^\star(1)$, $\mathrm{let}(\mu/\mathscr{A})_K = (\sqrt{\mu})^{\sigma_{\mathscr{A}}-1}$ be the quadratic symbol of K at $\mathscr{A}\mathfrak{D}_K$.

Let $H \subset K^{ab}$ be the ring class field corresponding to $\mathfrak{o}$; this field may be described as the subfield of K^{ab} fixed by all $\sigma_{(\mu)}$ for $\mu \in P^\star(d\mathscr{F})$, where $\mathscr{F}$ is an arbitrary $\mathfrak{o}$-ideal. The Artin map gives an isomorphism $\mathrm{Cl}(\mathfrak{o}) \xrightarrow{\sim} \mathrm{Gal}(H/K)$. We let $H^+ = H \cap \mathbb{R}$ be the maximal real subfield of H. We let $w = |\boldsymbol{\mu}_H|$ be the number of distinct roots of unity in H. This number is a divisor of 24 and equals the greatest common denominator of $\{\mathbb{N}(\mu) - 1 | \mu \in \mathfrak{o} \text{ prime to } 6\}$; both of these facts are easy to verify (e.g., [KL, pp. 216–217], [St, p. 220]). For a positive divisor N of 24, put $w_N = \gcd(w, N)$. The quantity w_{12} will play a key role in this paper. Because it will appear in many formulas, we also put $\tilde{w} = w_8/2$.

We call $\alpha \in K^{ab}$ *Kummer over* H if $\alpha^w \in H$. In this case, there is an $\mathfrak{o}$-ideal $\mathscr{F}$ such that the map $(\mathfrak{o}/\mathscr{F}\mathfrak{o})^* \to \boldsymbol{\mu}_w$ defined by $\mu \mapsto \alpha^{\sigma_{(\mu)}-1}$ is a homomorphism, which we call the *associated character*. This character completely determines the extension $H(\alpha)/H$. For instance, by Kummer theory, the degree of this extension is the order of the associated character.

Any $\mathscr{A} \in I^\star(1)$ has a *standard basis*, namely, one of the form

$$\mathscr{A} = \left[\frac{b + \sqrt{-d}}{2}, a\right] \tag{4}$$

with $a = \mathbb{N}\mathscr{A}$, b an integer determined modulo $2a$ satisfying $b^2 \equiv -d \pmod{4a}$. In the equivalent language of quadratic forms, $\mathscr{A}$ corresponds, under this choice of basis, to the primitive form $ax^2 + bxy + cy^2$ of discriminant $-d$. We shall always deal with ideals that are primitive and therefore have a standard basis.

If $\mathscr{A}, \mathscr{A}_1 \in I^\star(\mathscr{F})$ are relatively prime, then $\mathscr{A}\mathscr{A}_1 \in I^\star(\mathscr{F})$; if $[(b + \sqrt{-d})/2, aa_1]$ is a standard basis of $\mathscr{A}\mathscr{A}_1$, then $[(b + \sqrt{-d})/2, a]$ is a standard basis of $\mathscr{A}$, $[(b + \sqrt{-d})/2, a_1]$ is a standard basis of $\mathscr{A}_1$, and conversely.

2.2. Definition of η on ideals

Definition 8. For any $\mathscr{A} \in I^\star(6)$ with standard basis $[(b + \sqrt{-d})/2, a]$, let

$$\eta(\mathscr{A}) = e_{48}(a(b + 3\tilde{w}))\eta\left(\frac{-b + \sqrt{-d}}{2a}\right).$$

Verifying that $\eta(\mathscr{A})$ is well defined, that is, that it does not depend on the choice of standard basis for $\mathscr{A}$, is an easy exercise based on the following facts: b is determined modulo $2a$, $a^2 \equiv 1 \pmod{24}$ since a is prime to 6, and $\phi(T) = e_{12}(1)$.

Our main technical tool in this paper is the Shimura reciprocity law [Sh, Theorem 6.31]; Stark's less general formulation of it [St, Theorem 3′] will suffice for our applications, as in the following lemma, for instance.

LEMMA 9. *Suppose a is a positive integer, and $\mathscr{P} \in I^*(6a)$ is a prime ideal of norm p. Let $[(b+\sqrt{-d})/2, p]$ be a standard basis of $\mathscr{P}$, $g(z) = \eta(z/a)/\eta(z)$, and $z_0 = (-b+\sqrt{-d})/2$. Then*

$$g(z_0) \in K^{ab} \quad \text{and} \quad g(z_0)^{\sigma_{\mathscr{P}}} = \left(\frac{a}{p}\right) g(z_0/p)\,.$$

Proof. According to [St, Theorem 3′], we have $g(z_0) \in K^{ab}$ and

$$(g(z_0))^{\sigma_{\mathscr{P}}} = (g \circ pB^{-1})(B \circ z_0)\,,$$

where $B = \begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix}$. Note that $B \circ z_0 = z_0/p$ and that $pB^{-1} = S^{-1}BS$. For a function $h(z)$ on the upper half-plane, put $h^*(z) = (h \circ S)(z) = (h \circ S^{-1})(z)$. Then $g^*(z) = \sqrt{a}\eta(az)/\eta(z)$. Since $\eta(az)/\eta(z)$ has rational Fourier coefficients at $i\infty$, B acts trivially on it, and, of course, B acts on $\sqrt{a}$ via multiplication by the Kronecker symbol $\left(\frac{a}{p}\right)$. Hence,

$$\begin{aligned} g \circ pB^{-1} &= (g^* \circ B) \circ S \\ &= \left(\frac{a}{p}\right) g^* \circ S \\ &= \left(\frac{a}{p}\right) g\,, \end{aligned}$$

proving the lemma. ■

PROPOSITION 10. *Suppose $\mathscr{A} \in I^*(6)$, $\mathscr{A}_1 \in I^*(6a)$ are two ideals of $\mathfrak{o}$, with norms $a = \mathbb{N}(\mathscr{A})$ and $a_1 = \mathbb{N}(\mathscr{A}_1)$. Then*

(i) *(Galois action)*

$$\overline{\eta(\mathscr{A})} = e_8(-\tilde{w}a)\eta(\bar{\mathscr{A}})\,,$$

$$\left(\frac{\eta(\mathscr{A})}{\eta(\mathfrak{o})}\right)^{\sigma_{\mathscr{A}_1}} = \left(\frac{a}{a_1}\right)\frac{\eta(\mathscr{A}_1\mathscr{A})}{\eta(\mathscr{A}_1)}\,;$$

(ii) *(Integrality)* $\eta(\mathscr{A})/\eta(\mathfrak{o})$ *and* $\sqrt{a}\,\eta(\mathfrak{o})/\eta(\mathscr{A})$ *are algebraic integers in* K^{ab};
(iii) *(Reciprocity)*

$$\left(\frac{\eta(\mathscr{A})}{\eta(\mathfrak{o})}\right)^{\sigma_{\mathscr{A}_1}-1} = (-1)^{((a-1)/2)((a_1-1)/2)}\left(\frac{\eta(\mathscr{A}_1)}{\eta(\mathfrak{o})}\right)^{\sigma_{\mathscr{A}}-1};$$

(iv) *(Capitulation) If* $\alpha = \eta^2(\mathscr{A})/\eta^2(\mathfrak{o})$, *then in some finite extension* $F \subset K^{ab}$ *of* K *we have* $\alpha\mathfrak{O}_F = \mathscr{A}\mathfrak{O}_F$.

Proof. The action of complex conjugation follows immediately from $\eta(-\bar{z}) = \overline{\eta(z)}$. All remaining claims are consequences of the Shimura reciprocity law. The functions $g(z) = \eta(z/a)/\eta(z)$ and $\sqrt{a}/g(z)$ are modular functions of level $24a$ with Fourier coefficients in $\mathbb{Z}[\mu_{24a}]$ at every cusp. By [St, Theorem 3′], the integrality of Fourier coefficients at all cusps and formula (5) below imply (ii). To prove (i), we may assume without loss of generality that $\mathscr{A}_1$ is a prime ideal $\mathscr{P}$ of norm $a_1 = p$, thanks to the multiplicativity of the Kronecker symbol. Choose a standard basis $[(b+\sqrt{-d})/2, ap]$ of $\mathscr{A}\mathscr{P}$ and put $z_0 = (-b+\sqrt{-d})/2$. From the definitions,

$$\frac{\eta(\mathscr{A})}{\eta(\mathfrak{o})} = e_{48}((b+3\tilde{w})(a-1))\,g(z_0)\,, \tag{5}$$

and

$$\frac{\eta(\mathscr{A}\mathscr{P})}{\eta(\mathscr{P})} = e_{48}(p(b+3\tilde{w})(a-1))\,g(z_0/p)\,.$$

We have

$$\left(\frac{\eta(\mathscr{A})}{\eta(\mathfrak{o})}\right)^{\sigma_{\mathscr{P}}} = e_{48}(p(b+3\tilde{w})(a-1))g(z_0)^{\sigma_{\mathscr{P}}}\,,$$

and we compute via the reciprocity law (in the form of Lemma 9) that

$$g(z_0)^{\sigma_{\mathscr{P}}} = \left(\frac{a}{p}\right)g(z_0/p)\,.$$

This proves (i), from which (iii) follows by quadratic reciprocity.

As for (iv), it suffices to show that α^{12} (which equals $a^{12}\Delta(\mathscr{A})/\Delta(\mathfrak{o})$, where Δ is the discriminant modular form) generates $\mathscr{A}^{12}\mathfrak{O}_H$, and this amounts to a standard result about Δ-quotients [St, Lemma 2]. However, we give a direct proof. We can find $\mathscr{A}_1 \in I^*(6a)$ such that $\mathscr{A}\mathscr{A}_1 = (\mu)$ for some $\mu \in \mathfrak{o}$. Let $\alpha_1 = \eta^2(\mathscr{A}_1)/\eta^2(\mathfrak{o})$. Then

$$\alpha\alpha_1^{\sigma_{\mathscr{A}}} = \zeta\mu$$

for some 12th root of unity ζ. Let $F = K(\alpha, \zeta)$; we then have the equality as ideals of $\mathfrak{O}_F$, $(\alpha)(\alpha_1)^{\sigma_{\mathscr{A}}} = \mathscr{A}\mathscr{A}_1\mathfrak{O}_F$. By (ii), we know that (α) divides (a) and (α_1) divides (a_1). Since a and a_1 are relatively prime, we conclude that $(\alpha) = \mathscr{A}\mathfrak{O}_F$. ■

3. The character κ. In this section we introduce and study a character $\kappa : (\mathfrak{o}/12\mathfrak{o})^* \to \boldsymbol{\mu}_{12}$, which will be instrumental in the description of Kummer extensions generated by η-quotients.

Definition 11. We define

$$\kappa(\mu) = \chi_4(\mathbb{N}\mu)\frac{1}{\mu}\frac{\eta^2(\mu\mathfrak{o})}{\eta^2(\mathfrak{o})}, \qquad \mu \in P^*(6).$$

LEMMA 12. *Suppose $\mu \in P^*(6)$.*

(i) *If $\zeta \in \mathfrak{o}^*$, then $\kappa(\zeta\mu) = \zeta^{-1}\kappa(\mu)$; in particular, $\kappa(-1) = -1$.*

(ii) $\overline{\kappa(\mu)} = \chi_4(\mathbb{N}\mu)^{\tilde{w}}\kappa(\bar{\mu})$.

(iii) *If $\nu, \mu\nu \in P^*(6)$, then $\kappa(\mu\nu) = \kappa(\mu)^{\mathbb{N}\nu}\kappa(\nu)$.*

(iv) $\kappa(\mu) \in \boldsymbol{\mu}_{12}$.

(v) *Let $a = \mathbb{N}\mu$. Choose a standard basis $\mu\mathfrak{o} = [(b + \sqrt{-d})/2, a]$, and let M_μ be the multiplication by μ matrix under the basis $\mathfrak{o} = [(-b + \sqrt{-d})/2, 1]$; that is,*

$$M_\mu\begin{pmatrix}(-b+\sqrt{-d})/2\\ 1\end{pmatrix} = \mu\begin{pmatrix}(-b+\sqrt{-d})/2\\ 1\end{pmatrix}, \qquad \det M_\mu = a.$$

Then

$$\kappa(\mu) = e_{24}((b + 3\tilde{w} + 6)(a - 1))\phi(\hat{a}M_\mu),$$

where $\hat{a}M_\mu$ is (the reduction modulo $12\mathbb{Z}$ of) $\left(\begin{smallmatrix}a & 0\\ 0 & 1\end{smallmatrix}\right)M_\mu$.

Proof. The definition of κ gives (i) immediately, and (ii) follows from Proposition 10(i). To prove (iv) and (v), note that both $[(-b + \sqrt{-d})/2, a]$ and $[\bar{\mu}(-b + \sqrt{-d})/2, \bar{\mu}]$ are bases for $\bar{\mu}\mathfrak{o}$, so there is a matrix

$$M = \begin{pmatrix}\alpha & \beta\\ \gamma & \delta\end{pmatrix} \in SL_2(\mathbb{Z})$$

affecting the change of basis:

$$M\begin{pmatrix}\bar{\mu}(-b+\sqrt{-d})/2\\ \bar{\mu}\end{pmatrix} = \begin{pmatrix}(-b+\sqrt{-d})/2\\ a\end{pmatrix}, \tag{6}$$

$$M \circ (-b + \sqrt{-d})/2 = (-b + \sqrt{-d})/(2a), \qquad \mu = \gamma(-b + \sqrt{-d})/2 + \delta.$$

We now apply (1) and (6) to the definition of κ:

$$\kappa(\mu) = \chi_4(a)e_{24}((b+3\tilde{w})(a-1))\frac{1}{\mu}\frac{\eta^2(M\circ(-b+\sqrt{-d})/2)}{\eta^2((-b+\sqrt{-d})/2)}$$

$$= e_{24}((b+3\tilde{w}+6)(a-1))\phi(M)\frac{\gamma(-b+\sqrt{-d})/2+\delta}{\mu}$$

$$= e_{24}((b+3\tilde{w}+6)(a-1))\phi(M).$$

Since $a-1$ is even, this much suffices to prove (iv). One checks easily that $\hat{a}M = M_\mu$, which proves (v) since $\hat{a} \pmod{12}$ is its own inverse and since ϕ factors through $SL_2(\mathbb{Z}/12\mathbb{Z})$. The cocycle property (iii) is a simple consequence of the way the Galois group acts:

$$\frac{\kappa(\mu\nu)}{\kappa(\nu)} = \frac{\chi_4(\mathbb{N}\mu\mathbb{N}\nu)\mu^{-1}\nu^{-1}\eta^2(\mu\nu\mathfrak{o})/\eta^2(\mathfrak{o})}{\chi_4(\mathbb{N}\nu)\nu^{-1}\eta^2(\nu\mathfrak{o})/\eta^2(\mathfrak{o})}$$

$$= \chi_4(\mathbb{N}\mu)\mu^{-1}\left(\frac{\eta^2(\mu\mathfrak{o})}{\eta^2(\mathfrak{o})}\right)^{\sigma(\nu)}$$

$$= \kappa(\mu)^{\sigma(\nu)}$$

$$= \kappa(\mu)^{\mathbb{N}\nu},$$

where the last line is justified by (iv). ■

LEMMA 13. *If $\mu, \mu' \in P^*(6)$ and $\mu - \mu' \in 12\mathfrak{o}$, then $\kappa(\mu) = \kappa(\mu')$. The assignment $\mu \mapsto \kappa(\mu)$ induces a map $(\mathfrak{o}/12\mathfrak{o})^* \to \boldsymbol{\mu}_{12}$.*

Proof. Let $a = \mathbb{N}\mu$, $a' = \mathbb{N}\mu'$. Clearly, $M_\mu \equiv M_{\mu'} \pmod{12\mathbb{Z}}$ and $a \equiv a' \pmod{12}$. Since $(aa', 6) = 1$, we may choose standard bases $(\mu) = [(b+\sqrt{-d})/2, a]$ and $(\mu') = [(b'+\sqrt{-d})/2, a']$ such that $b \equiv b' \pmod{24}$. It follows from Lemma 12(v) that

$$\frac{\kappa(\mu)}{\kappa(\mu')} = e_{24}((b+3\tilde{w}+6)(a-a')).$$

If d is odd, then so are b and $\tilde{w}$, and we are done. If d is even, one checks easily that $a \equiv a' \pmod{24}$, again giving the desired result. We conclude that we have a well-defined mapping $(\mathfrak{o}/12\mathfrak{o})^* \to \boldsymbol{\mu}_{12}$, because every element of $(\mathfrak{o}/12\mathfrak{o})^*$ has a representative $\mu \in P^*(6)$. ■

Remark. With slight abuse of notation, we reuse the letter κ for the character $(\mathfrak{o}/12\mathfrak{o})^* \to \boldsymbol{\mu}_{12}$ induced by $\mu \mapsto \kappa(\mu)$. For instance, for an integer a prime to 6, $\kappa(a)$ makes sense even though $\kappa(\mu)$ was originally defined only for primitive μ.

Our next goal is to prove that κ is a character; to this end, we decompose κ into its 3-component κ_3 and 4-component κ_4 by writing $\kappa = \kappa_3/\kappa_4$. Checking that κ_3 is a character is straightforward; to do the same for κ_4, we relate it to the character $\varkappa_\rho$ of the previous section.

We first classify the isomorphism classes of the rings $\mathfrak{o}/N\mathfrak{o}$ for $N = 3$ and 4. To give a compact notation for the isomorphism class of $\mathfrak{o}/4\mathfrak{o}$, which is determined by the value of d (mod 16), let us say $\mathfrak{o}$ is of "4-type" $2^n_{(\delta)}$ if $n = v_2(d)$ and δ (if required) is a certain quadratic symbol as follows: if $v_2(d) = 0, \delta = \chi_8(-d)$ and if $v_2(d) = 2$, $\delta = \chi_4(d/4)$. Similarly, saying $\mathfrak{o}$ is of "3-type" $3^n_{(\delta)}$ means $n = v_3(d)$ where, for $v_3(d) = 0$, $\delta = \frac{-d}{3}$. To list the various 12-types, it will be convenient to put

$$d_0 = \begin{cases} d & \text{if } d \text{ is odd} \\ d/4 & \text{if } d \text{ is even.} \end{cases}$$

The six 4-types of $\mathfrak{o}$, together with the corresponding values of d_0 (mod 8) and w_8, as well as the three 3-types and the corresponding d (mod 3) and w_3 are listed in Tables 3 and 4.

TABLE 3

4-type	d_0 (mod 8)	w_8
2^0_+	7	2
2^0_-	3	2
2^2_+	1, 5	4
2^2_-	3, 7	2
2^3	2, 6	2
$2^{\geq 4}$	0, 4	8

TABLE 4

3-type	d (mod 3)	w_3
3^0_+	2	1
3^0_-	1	1
$3^{\geq 1}$	0	3

LEMMA 14. (i) *The map* $\kappa : (\mathfrak{o}/12\mathfrak{o})^* \to \boldsymbol{\mu}_{12}$ *is a character of order precisely* $w_{12} = \gcd(w, 12)$.

(ii) *Given any positive integer* m, *there is a* $\mu \in \mathfrak{o}$ *such that* $\mathbb{N}\mu \equiv 1 \pmod{m}$ *and* $\kappa(\mu)$ *is a primitive* w_{12}*th root of unity.*

Proof. (i) We begin with a remark about the order of κ. By Lemma 12(iii), κ is a character if and only if $\kappa(\mu)^{\mathbb{N}\nu - 1} = 1$ for all $\mu, \nu \in P^\star(6)$, in other words, if and only if $\kappa^{w_{12}} = 1$. We break up the problem into its 3-primary and 4-primary components and first show that each component of κ is a character; to complete the proof of the lemma, it will then suffice to prove part (ii).

Choose a standard basis for $\mathfrak{o}$, and let ρ be the associated representation

$$\rho : (\mathfrak{o}/4\mathfrak{o})^* \to GL_2(\mathbb{Z}/4\mathbb{Z}).$$

Clearly, ρ has abelian image. We now claim that, for each 4-type of $\mathfrak{o}$, $\kappa_4(\mu)/\varkappa_\rho(\mu)$ is a character of order 2 on $(\mathfrak{o}/4\mathfrak{o})^*$. This will show that κ_4 is a character, since $\varkappa_\rho$ is a character by construction (Proposition 7). The calculations are routine; we indicate the steps, leaving some of the details to the reader.

When $w_4 = 2$, $\mathrm{Im}(\rho) \not\subseteq SL_2(\mathbb{Z}/4\mathbb{Z})$; hence to determine $\varkappa_\rho = \phi_\varepsilon \circ \rho$ according to the recipe in the proof of Proposition 7, we must evaluate $\varepsilon = \phi_4(\widehat{-1}M)^2$ for an arbitrary determinant -1 matrix M in the image of ρ. For example, $M = \rho(\sqrt{-d_0})$ is such a matrix in every case except for 4-type 2^3, where we can take $M = \rho(1 + \sqrt{-d_0})$ instead. We find that $\varepsilon = (-1)^{d+1}$. Together with Lemma 12(v), one checks in every case that $\kappa_4(\mu)/\varkappa_\rho(\mu)$ in fact factors through the norm map. Moreover, it is either $\chi_1(\mathbb{N}\mu)$ or $\chi_4(\mathbb{N}\mu)$, except for type 2^2_-, where it is $\chi_8(\mathbb{N}\mu)$.

When $w_4 = 4$, ρ maps into $SL_2(\mathbb{Z}/4\mathbb{Z})$ and $\varkappa_\rho = \phi_4 \circ \rho$ is a character. One checks using Lemma 12(v) that $\kappa_4 = \varkappa_\rho$.

It remains to show that κ_3 is a character of order w_3. Recall from Lemma 12(iii) that

$$\frac{\kappa_3(\mu\nu)}{\kappa_3(\mu)\kappa_3(\nu)} = \kappa_3(\mu)^{\mathbb{N}\nu-1} = \kappa_3(\nu)^{\mathbb{N}\mu-1}.$$

We want to show that this is identically 1; the only nontrivial case being $\mathbb{N}\mu \equiv \mathbb{N}\nu \equiv -1 \pmod 3$, it suffices to prove that

$$\mathbb{N}\mu \equiv -1 \pmod 3 \Rightarrow \kappa_3(\mu) = 1. \tag{7}$$

To prove this, note that by Lemma 12, $\kappa_3(-1) = 1$ and $\kappa_3(\bar{\mu}) = \overline{\kappa_3(\mu)} = \kappa_3(\mu)^{-1}$. If $\mathbb{N}\mu = \bar{\mu}\mu \equiv -1 \pmod 3$, then

$$\begin{aligned}\kappa_3(\bar{\mu}\mu) &= \kappa_3(\bar{\mu})^{-1}\kappa_3(\mu)\\ &= \kappa_3(\mu)^2\\ &= \kappa_3(-1)\\ &= 1,\end{aligned}$$

proving (7). Therefore κ_3 is a character.

(ii) As before, we consider the 3- and 4-components separately. For the 4-component, it clearly suffices to consider the case where m is a power of 2. If $w_4 = 2$, take μ to be -1. If $w_4 = 4$, one easily finds a $\mu_0 \in \mathfrak{o}$ with norm $\mathbb{N}\mu_0 \equiv 1 \pmod 8$ and $\kappa(\mu_0) = i$. Let x be a square root of $\mathbb{N}\mu_0^{-1}$ in the 2-adic integers $\mathbb{Z}_2$, and take $\mu = (x \bmod m)\mu_0$. A similar argument works for the 3-component. ■

Although the definition of κ involves a certain number of choices, this character depends, to a certain extent, only on the 12-type of $\mathfrak{o}$; we make this precise in the following lemma.

LEMMA 15. (i) *Suppose $\mathfrak{o}'$ is an imaginary quadratic order of discriminant d' with associated character κ'. Let $N = 3$ or 4. Suppose there exists a ring isomorphism $\psi : \mathfrak{o}'/N\mathfrak{o}' \to \mathfrak{o}/N\mathfrak{o}$. Then there exists an integer r prime to N, depending on ψ, such that for all primitive $\mu' \in \mathfrak{o}'$ prime to 6,*

$$\kappa_N(\psi(\mu')) = \chi_4(\mathbb{N}\mu)^{(r-1)/2}\kappa'_N(\mu')^r .$$

In particular, $\kappa_N \circ \psi$ and κ'_N have the same order.

(ii) *Up to composition with automorphisms of $(\mathfrak{o}/12\mathfrak{o})^*$ and twisting by $\chi_4 \circ \mathbb{N}$, the character κ depends only on the 12-type of $\mathfrak{o}$.*

Proof. Choose standard bases $\mu'\mathfrak{o}' = [(b'+\sqrt{-d'})/2, a']$, $\mathfrak{o} = [(\tilde{b}+\sqrt{-d})/2, 1]$, where $a' = \mathbb{N}\mu'$. There exists an integral matrix $\tilde{P}$ such that

$$\begin{pmatrix} \psi((b'+\sqrt{-d'})/2) \\ \psi(1) \end{pmatrix} = \tilde{P}\begin{pmatrix} (\tilde{b}+\sqrt{-d})/2 \\ 1 \end{pmatrix}.$$

Note that $r = \det \tilde{P}$ is prime to N; moreover, since $\psi(1) = 1$, $\tilde{P}$ must be of the form $\tilde{P} = \begin{pmatrix} r & s \\ 0 & 1 \end{pmatrix}$. Therefore, we can find another basis $\mathfrak{o} = [(b+\sqrt{-d})/2, 1]$ so that

$$\begin{pmatrix} \psi((b'+\sqrt{-d'})/2) \\ 1 \end{pmatrix} = P\begin{pmatrix} (b+\sqrt{-d})/2 \\ 1 \end{pmatrix}, \qquad P = \hat{r}.$$

Since ψ is a homomorphism of rings, we have

$$\mathrm{Tr}(\psi((b'+\sqrt{-d})/2)) = \mathrm{Tr}(r(b+\sqrt{-d})/2) = rb \equiv b' \pmod{N}. \tag{8}$$

In the notation of Lemma 12(v), $M_{\psi(\mu')} \equiv P^{-1}M_{\mu'}P \pmod{N}$, since P is the change of basis matrix. Let $a = \mathbb{N}(\psi(\mu'))$ and note that $a \equiv a' \pmod{N}$. By Lemma 12(v), we have

$$\frac{\kappa_N(\psi(\mu'))}{\kappa'_N(\mu')^r} = \xi_N \frac{\phi_N(\hat{a}P^{-1}M_{\mu'}P)}{\phi_N(\hat{a}'M_{\mu'})^r},$$

where ξ_N is the N-component of the 12th root of unity

$$\begin{aligned}\xi &= \xi_3/\xi_4 \\ &= \frac{e_{24}((b+3\tilde{w}+6)(a-1))}{e_{24}((b'+3\tilde{w}+6)(a'-1)r)} \\ &= e_3(b(a-1)-rb'(a'-1))e_8((\tilde{w}+2)(a-1)(1-r)+(a-a')(b-r(\tilde{w}+2))).\end{aligned}$$

Using (8), one easily checks that $\xi_3 = 1$. Verifying $\xi_4 = \chi_4(a)^{(r-1)/2}$ is a bit more tedious, but it is routine once one notes the following: when d is odd, so are b and $\tilde{w}$, while when d is even, $a \equiv a' \pmod 8$. To complete the proof of (i), we merely observe that by Lemma 1, $\phi_N(\hat{a}P^{-1}M_{\mu'}P) = \phi_N(\hat{a}'M_{\mu'})^r$. Finally, (ii) follows from (i) by taking $\mathfrak{o}' = \mathfrak{o}$. ■

Remark. Since there are only finitely many isomorphism classes of the (finite) rings $(\mathfrak{o}/12\mathfrak{o})^*$, the task of deducing the properties of κ is reduced, by the preceding lemma, to a finite calculation. In light of this fact, an alternative approach to understanding the character κ would have been to study it for a single discriminant $-d$ in each residue class of $-d \pmod{48}$; this is the approach advocated by Stark in similar situations, for instance, in [St, p. 219].

4. The functions γ_2 and γ_3. To give a preview of the role of κ in the sequel, we now show how the key properties of this character translate easily into a classical result about the field generated by the singular values of the functions $\gamma_2(z)$ and $\gamma_3(z)$; these functions are related to the modular invariant $j(z)$ via $\gamma_2^3 = j$, $\gamma_3^2 = j - 1728$. Calculation of the minimal polynomial of these singular moduli is one of the steps in the Atkin-Morain primality proving algorithm [AM]; we will treat some of the Weber class invariants, which are also used by Atkin and Morain, in the final section.

Let g_2, g_3 be the level-1 modular forms of weights 4 and 6 given by

$$g_2(\Lambda) = 60 \sum_{\lambda \in \Lambda - 0} \lambda^{-4}, \qquad g_4(\Lambda) = 140 \sum_{\lambda \in \Lambda - 0} \lambda^{-6}.$$

As usual, we put $g_k(z) = g_k([z, 1])$ for $\Im(z) > 0$, and then

$$\gamma_2(z) = g_2(z)/\eta^8(z), \qquad \gamma_3(z) = g_3(z)/\eta^{12}(z).$$

Definition 16. For $\mathscr{A} \in I^*(6)$, with standard basis $[(b + \sqrt{-d})/2, a]$, let

$$\gamma_2(\mathscr{A}) = \frac{g_2((-b + \sqrt{-d})/2a)}{\eta^8(\mathscr{A})}, \qquad \gamma_3(\mathscr{A}) = \frac{g_3((-b + \sqrt{-d})/2a)}{\eta^{12}(\mathscr{A})}.$$

Notice that $\gamma_k(\mathscr{A}) = a^{2k} g_2(\bar{\mathscr{A}})/\eta^8(\mathscr{A})$; hence $\gamma_2(\mathscr{A})$ and $\gamma_3(\mathscr{A})$ do not depend on the choice of standard basis for $\mathscr{A}$.

THEOREM 17. *Suppose $\mathscr{A} \in I^*(6)$ has norm a.*

(i) *For $k = 2, 3$, $\gamma_k(\mathscr{A}) \in K^{ab}$, and if $\mathscr{A}_1 \in I^*(6a)$, $\gamma_k(\mathscr{A})^{\sigma_{\mathscr{A}_1}} = \gamma_k(\mathscr{A}\mathscr{A}_1)$.*

(ii) *$\gamma_2(\mathscr{A})$ is Kummer over H with character κ_3^{-1} of order w_3.*

(iii) *$\gamma_3(\mathscr{A})$ is Kummer over H with character κ_4^2 of order $w_4/2$.*

(iv) *If $w_3 = 1$, $\gamma_2(\mathscr{A}) \in H^+$; if $w_4 = 2$, $\gamma_3(\mathscr{A})/\sqrt{-d} \in H^+$.*

Proof. (i) Without loss of generality, we may assume that $\mathscr{A}_1$ is a prime ideal $\mathscr{P}$ of degree 1 and norm p. Choose a standard basis $\mathscr{A}\mathscr{P} = [(b+\sqrt{-d})/2, ap]$ where $a = \mathbb{N}\mathscr{A}$. By definition, we have

$$\gamma_2(\mathscr{A}) = e_6(-a(b+3\tilde{w}))\frac{g_2((-b+\sqrt{-d})/2a)}{\eta^8((-b+\sqrt{-d})/2a)}$$

$$= e_6(-a(b+3\tilde{w}))\gamma_2\left(\frac{-b+\sqrt{-d}}{2a}\right).$$

Now $\gamma_2(z)$ is a modular function, so the Shimura reciprocity law [St, Theorem 3′] applies: $\gamma_2(\mathscr{A}) \in K^{ab}$, and

$$\gamma_2(\mathscr{A})^{\sigma_{\mathscr{P}}} = e_6(-ap(b+3\tilde{w}))(\gamma_2 \circ pB^{-1})\left(B \circ \frac{-b+\sqrt{-d}}{2}\right),$$

where $B = \begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix}$. Note that $pB^{-1} = S^{-1}BS$, with $S = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$. Since $\phi(S) = e_{12}(3)$, one checks easily that $\gamma_2(S \circ z) = \gamma_2(S^{-1} \circ z) = \gamma_2(z)$. Owing to the rationality of the Fourier coefficients of $\gamma_2(z)$ at $i\infty$, B acts trivially on $\gamma_2(z)$ as well. Therefore,

$$\gamma_2(\mathscr{A})^{\sigma_{\mathscr{P}}} = e_6(-ap(b+3\tilde{w}))\gamma_2\left(\frac{-b+\sqrt{-d}}{2ap}\right)$$

$$= \gamma_2(\mathscr{A}\mathscr{P}).$$

The proof for γ_3 follows exactly the same pattern; one checks using $\phi(S) = e_{12}(3)$ that $\gamma_3(S \circ z) = \gamma_3(S^{-1} \circ z) = -\gamma_3(z)$; hence pB^{-1} acts trivially on $\gamma_3(z)$.

(ii) We have by (i)

$$\gamma_2(\mathscr{A})^{\sigma(\mu)-1} = \frac{\gamma_2(\mathscr{A}\mu)}{\gamma_2(\mathscr{A})}$$

$$= \frac{a^4(\mathbb{N}\mu)^4 g_2(\bar{\mathscr{A}}(\bar{\mu}))}{a^4 g_2(\bar{\mathscr{A}})}\frac{\eta^8(\mathscr{A})}{\eta^8(\mathscr{A}(\mu))}$$

$$= \mu^4\left(\frac{\eta^8(\mathfrak{o})}{\eta^8((\mu))}\right)^{\sigma_{\mathscr{A}}}$$

$$= \mu^4(\mu\kappa(\mu))^{-4\sigma_{\mathscr{A}}}$$

$$= \kappa(\mu)^{-4a}.$$

As $(a, 6) = 1$, and as every class in $(\mathfrak{o}/12\mathfrak{o})^*$ has a representative in $P^*(6ad)$, $\gamma_2(\mathscr{A})$ is Kummer over H with character $\kappa^{-4a} = \kappa_3^{-a}$, which has order w_3 by Lemma 14. Note that $\kappa_3^{-a} = \kappa_3^{-1}$, since $a \equiv 1 \pmod 3$ when $w_3 = 3$. Without difficulty, one proves (iii) in the same manner. To prove (iv), simply note that by Proposition 10.i $\gamma_2(\mathscr{A}) = \gamma_2(\bar{\mathscr{A}})$ and $\gamma_3(\mathscr{A}) = -\gamma_3(\bar{\mathscr{A}})$. ■

Remark. For prime $d > 3$, part (iv) of the above theorem is used by Gross [Gr] to give a model over H^+ for the CM elliptic curve $A(d)$ with discriminant ideal $(-d^3)$.

5. Main theorem

Definition 18. Let $\mathbb{D}_0$ be the group of degree-0 divisors supported on $I^*(6d)$, that is, formal linear combinations

$$\mathcal{D} = \sum_{j=1}^{r} n_j \mathscr{A}_j,$$

with $n_j \in \mathbb{Z}$, $\mathscr{A}_j \in I^*(6d)$ and $\sum_{j=1}^r n_j = 0$. Given such $\mathcal{D} \in \mathbb{D}_0$, we define its exponent $e_{\mathcal{D}} = (1/2)\sum_{j=1}^r n_j(\mathbb{N}\mathscr{A}_j - 1) \in \mathbb{Z}$, its support $\mathscr{F}_{\mathcal{D}} = \prod_{n_j \neq 0} \mathscr{A}_j$, and its ideal $\mathscr{A}_{\mathcal{D}} = \prod_{j=1}^r \mathscr{A}_j^{n_j}$, which is a fractional ideal of $\mathfrak{o}$. We put $\bar{\mathcal{D}} = \sum_{j=1}^r n_j \bar{\mathscr{A}}_j$, and if $\mathscr{B} \in I^*(6\mathscr{F})$, $\mathscr{B}\mathcal{D} = \sum_{j=1}^r n_j \mathscr{A}_j \mathscr{B}$. We also extend the definition of η to $\mathbb{D}_0$ by multiplicativity, that is,

$$\eta(\mathcal{D}) = \prod_{j=1}^{r} \eta(\mathscr{A}_j)^{n_j}.$$

THEOREM 19. *Suppose $\mathcal{D} \in \mathbb{D}_0$ has exponent e, support $\mathscr{F}$, and ideal $\mathscr{A}$. Then*

(i) *$\eta(\mathcal{D})$ is Kummer over H with character $\kappa^e(\frac{\cdot}{\mathscr{A}})_K$;*
(ii) *for $\mathscr{B} \in I^*(6\mathscr{F})$, $\eta(\mathcal{D})^{\sigma_{\mathscr{B}}} = \eta(\mathscr{B}\mathcal{D})$; $\overline{\eta(\mathcal{D})} = e_4(-\tilde{w}e)\eta(\bar{\mathcal{D}})$;*
(iii) *$\eta(\mathcal{D})^2 \mathfrak{O}_{K^{ab}} = \mathscr{A}\mathfrak{O}_{K^{ab}}$;*
(iv) *for no root of unity ζ is the degree of $H(\zeta\eta(\mathcal{D}))/H$ less than the degree of $H(\eta(\mathcal{D}))/H$.*

Proof. The proof of (i) is a straightforward application of reciprocity (Proposition 10(iii)). Suppose that $\mathcal{D} = \sum n_j \mathscr{A}_j$ with $a_j = \mathbb{N}\mathscr{A}_j$, and that $\mu \in I^*(6da_1 \cdots a_r)$ has norm m. Then

$$\eta(\mathcal{D})^{\sigma(\mu)-1} = \prod_j \left(\frac{\eta(\mathscr{A}_j)}{\eta(\mathfrak{o})}\right)^{(\sigma(\mu)-1)n_j}$$

$$= \prod_j \left(\frac{\eta(\mu\mathfrak{o})}{\eta(\mathfrak{o})}\right)^{(\sigma_{\mathscr{A}_j}-1)n_j} (-1)^{((a_j-1)/2)((m-1)/2)n_j}$$

$$= (-1)^{((m-1)/2)e} \prod_j (\chi_4(m)\mu\kappa(\mu))^{(1/2)(\sigma_{\mathscr{A}_j}-1)n_j}$$

$$= \prod_j \left(\frac{\mu}{\mathscr{A}_j}\right)_K^{n_j} \kappa(\mu)^{(1/2)(a_j-1)n_j}$$

$$= \kappa(\mu)^e \left(\frac{\mu}{\mathscr{A}}\right)_K.$$

The proofs of (ii) and (iii) are immediate from Proposition 10. As for (iv), suppose $\zeta^m = 1$ and let $t = [H(\eta(\mathcal{D})) : H]$. Consider the abelian extension $H(\zeta\eta(\mathcal{D}))/H$. By part (i), Lemma 14(ii), and the Chinese remainder theorem, there exists $\mu \in \mathfrak{o}$ with $\mathbb{N}\mu \equiv 1 \pmod{m}$ such that $(\zeta\eta(\mathcal{D}))^{\sigma(\mu)^{-1}}$ has order t. ■

Remark. We note in passing that when K does not have discriminant -3 or -4, there exist divisors $\mathcal{D} \in \mathbb{D}_0$ such that $H(\eta(\mathcal{D}))/H$ achieves the maximal degree, namely, w_{12}. Indeed, there are $\mathfrak{o}$-ideals $\mathscr{A}$ prime to 6 whose Frobenius acts nontrivially on $\boldsymbol{\mu}_{12}$; such an ideal is automatically not the square of another $\mathfrak{o}$-ideal. The divisor $\mathcal{D} = \mathscr{A} - \mathfrak{o} \in \mathbb{D}_0$ has exponent $e_{\mathcal{D}}$ coprime to $w/2$ and non-square ideal $\mathscr{A}_{\mathcal{D}} = \mathscr{A}$; hence, by Theorem 19, $\eta(\mathcal{D})$ generates an extension of degree w_{12} over H.

6. Applications of the main theorem. As our first application of Theorem 19, we give examples of the well-known phenomenon that $\Delta(\mathscr{A})/\Delta(\mathfrak{o})$ is often a high power in H (e.g., [De], [St], [Ro], [KL]). The novelty here is that we say exactly which roots are in H and even give an explicit formula for the conjugates. The latter is especially useful for numerical calculations, as we will indicate briefly below.

THEOREM 20. *Suppose* $\mathscr{A} \in I^*(6d)$. *Let* $\alpha = \eta(\mathscr{A})/\eta(\mathfrak{o})$. *Then*
(i) $\alpha^{w_{12}} \in H$; *in particular,* $\alpha^{12} \in H$;
(ii) *if* $\mathscr{A} = \mathscr{A}_1^2$ *for some ideal* $\mathscr{A}_1$ *of* $\mathfrak{o}$, *then* $\alpha \in H$.

Proof. Let $\mathcal{D} = \mathscr{A} - \mathfrak{o} \in \mathbb{D}_0$. The divisor $w_{12}\mathcal{D}$ has exponent $w_{12}(\mathbb{N}\mathscr{A} - 1)/2 \equiv 0 \pmod{w_{12}}$, and ideal $\mathscr{A}^{w_{12}}$, which is a square. By Lemma 14 and the main theorem, $\eta(w_{12}\mathcal{D})$ is Kummer over H with trivial character, proving (i). If $\mathscr{A} = \mathscr{A}_1^2$, $\mathscr{A}_{\mathcal{D}}$ is a square and $e_{\mathcal{D}} = (\mathbb{N}\mathscr{A}_1^2 - 1)/2 \equiv 0 \pmod{12}$, and again we apply Lemma 14 and the main theorem to prove (ii). ■

As our second application, we show how to recover the quadratic reciprocity law over K via κ; this approach to the quadratic reciprocity law over K is neither novel nor surprising, but we include it as an illustration of the theme that κ captures much information about the Galois action on abelian extensions of K. The reader may wish to compare our treatment with that of Herglotz [He].

THEOREM 21. *Suppose* $\mathfrak{o}$ *is the maximal order of* K. *For all relatively prime numbers* $\mu, \nu \in \mathfrak{o}$ *with odd norms* $\mathbb{N}(\mu) = m$, $\mathbb{N}(\nu) = n$, *we have*

$$\left(\frac{\mu}{\nu}\right)_K \left(\frac{\nu}{\mu}\right)_K = (-1)^{((m-1)/2)((n-1)/2)} \kappa_4(\mu)^{(n-1)/2} \kappa_4(\nu)^{(m-1)/2}.$$

Proof. It suffices to prove this for $\mu, \nu \in P^*(6d)$ and $(m, n) = 1$. By reciprocity, we have

$$\left(\frac{\eta(\mu\mathfrak{o})}{\eta(\mathfrak{o})}\right)^{\sigma(\nu)-1} = \left(\frac{\eta(\nu\mathfrak{o})}{\eta(\mathfrak{o})}\right)^{\sigma(\mu)-1} (-1)^{((m-1)/2)((n-1)/2)}.$$

When we evaluate each side of this equality using the main theorem, we obtain

$$\left(\frac{\mu}{\nu}\right)_K (\chi_4(m)\kappa(\mu))^{(n-1)/2} = \left(\frac{\nu}{\mu}\right)_K (\chi_4(n)\kappa(\nu))^{(m-1)/2} (-1)^{((m-1)/2)((n-1)/2)}.$$

We now must recall that $\kappa(\mu)^{n-1} = \kappa(\nu)^{m-1} = 1$ (Lemma 14); in particular, we may replace κ by κ_4 in the above formula without altering it. All that remains now is to rearrange the terms. ■

The next application of the main theorem is to attach to each $\mathfrak{o}$-ideal class a real unit that generates, over K, a Kummer extension of H. In some cases, this unit is closely connected to the j-invariant of $\mathfrak{o}$; its logarithm appears in the Kronecker limit formula.

Definition 22. Given any primitive proper ideal $\mathscr{A}$ of $\mathfrak{o}$, with standard basis (4), define

$$u_{\mathscr{A}} = \frac{1}{\sqrt{a}} \frac{|\eta((b+\sqrt{-d})/2a)|^2}{|\eta((b+\sqrt{-d})/2)|^2}.$$

Note that $u_{\mathscr{A}} = u_{\bar{\mathscr{A}}} = \overline{u_{\mathscr{A}}}$ is a positive real number ($u_{\mathfrak{o}} = 1$), canonically defined for all proper primitive ideals, not just those prime to 6.

LEMMA 23. *Let* $\mathscr{A}, \mathscr{A}_1$ *be proper primitive ideals of* $\mathfrak{o}$ *with norm* a, a_1, *respectively.*

(i) *Suppose* $\mathscr{A}, \mathscr{A}_1$ *are in the same* $\mathfrak{o}$*-ideal class. Then* $u_{\mathscr{A}_1} = u_{\mathscr{A}}$.

(ii) *If* $\mathscr{A} \in I^*(6d)$, *then*

$$u_{\mathscr{A}} = \pm \frac{\eta(\mathscr{A})\eta(\bar{\mathscr{A}})}{\sqrt{a^*}\eta(\mathfrak{o})^2},$$

where $\pm = e_8((\tilde{w}-1)(a-1))$.

(iii) $u_{\mathscr{A}}$ *is a unit in* K^{ab}.

(iv) $u_{\mathscr{A}}$ *is Kummer over* H *with character* κ^{a_1-1}, *which has order* $w_{12}/\gcd(w_{12}, a_1 - 1)$, *where* a_1 *is the norm of any ideal* $\mathscr{A}_1 \in I^*(6d)$ *in the same* $\mathfrak{o}$*-ideal class as* $\mathscr{A}$.

(v) *If* $\mathscr{A} \in I^*(6d)$ *and* $\mathscr{A}_1 \in I^*(6a)$ *has norm* a_1, *then*

$$u_{\mathscr{A}}^{\sigma_{\mathscr{A}_1}} = e_8((\tilde{w} - 1)(a - 1)a_1)\left(\frac{a_1}{a^*}\right)\frac{\eta(\mathscr{A}\mathscr{A}_1)\eta(\bar{\mathscr{A}}\mathscr{A}_1)}{\sqrt{a^*}\eta(\mathscr{A}_1)^2}.$$

Proof. It suffices to prove (i) under the assumption $\mathscr{A} = (\mu)\mathscr{A}_1$ with $\mu \in \mathfrak{o}$. We may choose b such that

$$\mathscr{A} = \left[a, \frac{b + \sqrt{-d}}{2}\right], \qquad \mathscr{A}_1 = \left[a_1, \frac{b + \sqrt{-d}}{2}\right],$$

with $a = \mathbb{N}\mathscr{A}, a_1 = \mathbb{N}\mathscr{A}_1$. There is a unimodular matrix $M = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ such that

$$\mu\begin{pmatrix} \dfrac{b + \sqrt{-d}}{2} \\ a_1 \end{pmatrix} = M\begin{pmatrix} \dfrac{b + \sqrt{-d}}{2} \\ a \end{pmatrix}.$$

In particular, $M \circ (b + \sqrt{-d})/2a = (b + \sqrt{-d})/2a_1$, and

$$\left|\gamma\frac{b + \sqrt{-d}}{2a} + \delta\right| = |\mu|\frac{a_1}{a} = \frac{\sqrt{a_1}}{\sqrt{a}}.$$

It is now clear from (1) that $u_{\mathscr{A}_1} = u_{\mathscr{A}}$. As for (ii), it follows from definitions that

$$\frac{1}{\sqrt{a^*}}\frac{\eta(\mathscr{A})}{\eta(\mathfrak{o})}\frac{\eta(\bar{\mathscr{A}})}{\eta(\mathfrak{o})} = \frac{e_8((a-1)\tilde{w})}{\sqrt{a^*}}\frac{\left|\eta\left(\dfrac{b + \sqrt{-d}}{2a}\right)\right|^2}{\left|\eta\left(\dfrac{b + \sqrt{-d}}{2}\right)\right|^2}$$
$$= e_8((a-1)(\tilde{w}-1))u_{\mathscr{A}}.$$

It is easy to see that this equals $\pm u_{\mathscr{A}}$, proving (ii). To prove (iii) and (iv), we apply Theorem 19 to the expression for $u_{\mathscr{A}}$ in (ii). Let $\mathcal{D} = \mathscr{A} + \bar{\mathscr{A}} - 2\mathfrak{o}$, which is a divisor in $\mathbb{D}_0$ with exponent $a - 1$ and ideal (a); clearly, $u_{\mathscr{A}}^2 = \eta(\mathcal{D})^2/a^*$; hence $u_{\mathscr{A}}^2$ is a unit by Theorem 19(iii), and this proves (iii). Furthermore, by Theorem 19(i),

$$u_{\mathscr{A}}^{\sigma(\mu)-1} = (\eta(\mathcal{D})/\sqrt{a^*})^{\sigma(\mu)-1}$$
$$= \left(\frac{\mu}{a}\right)_K\left(\frac{a^*}{\mu}\right)_K\kappa(\mu)^{a-1}.$$

Thus, we must show that the product of the two quadratic symbols above is 1. For this we make use of the quadratic reciprocity law we proved earlier: if we let $m = \mathbb{N}\mu$, $v = a^*$, then $n = \mathbb{N}v = a^2 \equiv 1 \pmod 8$, and Theorem 21 gives

$$\left(\frac{\mu}{a}\right)_K \left(\frac{a^*}{\mu}\right)_K = \kappa_4(\mu)^{(a^2-1)/2} \kappa_4(a^*)^{(m-1)/2}$$
$$= 1,$$

since $\kappa_4(a^*) = \kappa_4(1) = 1$. Finally, (v) is immediate from (ii) and Proposition 10. ■

Definition 24. For a class $C \in \mathrm{Cl}(\mathfrak{o})$, choose any ideal $\mathscr{A} \in I^*(6d)$ representing C and put

$$u_C = u_{\mathscr{A}}, \quad v_C = u_C^{n_C},$$

where $n_C = w_{12}/\gcd(w_{12}, \mathbb{N}\mathscr{A} - 1)$.

By the previous lemma, u_C, v_C, n_C are all well defined. Moreover, n_C divides 6. In fact, the possible values for n_C are the divisors of $2w_{12}/|\mu_K|$ each with multiplicity $|\mathrm{Cl}(\mathfrak{o})|/\varphi(2w_{12}/|\mu_K|) \geqslant |\mathrm{Cl}(\mathfrak{o})|/4$. In particular, there exists a nontrivial class C with $n_C = 1$, except for finitely many orders $\mathfrak{o}$. The importance of the above units for arithmetic applications is due to their appearance in the limit formula of Kronecker, which can be phrased as follows.

THEOREM 25 (Kronecker's first limit formula). *Let $\zeta_{\mathfrak{o}}(s, C)$ be the partial Dedekind zeta function of a class $C \in \mathrm{Cl}(\mathfrak{o})$. Then*

$$\zeta_{\mathfrak{o}}'(0, C) - \zeta_{\mathfrak{o}}'(0, [\mathfrak{o}]) = -\log(u_C).$$

Proof. This is typically written $\zeta_{\mathfrak{o}}'(0, C) = (-1/24) \log |\mathbb{N}\mathscr{A}^6 \Delta(\mathscr{A})|^2$, with $\mathscr{A}$ any ideal in C^{-1} [St, p. 206]. The formula we have given is easily seen to follow from this. ■

The limit formula implies that the units u_C are highly nontrivial in various senses. For instance, one can use them to give a subgroup of finite index in the unit group of H (e.g., [Si], [KL], [H1]); also, as we now indicate, for nontrivial C, u_C has maximal degree over $\mathbb{Q}$.

THEOREM 26. *Suppose $\mathscr{A} \in I^*(6)$ is not principal in $\mathfrak{o}$, and $\alpha = \eta(\mathscr{A})/\eta(\mathfrak{o})$. For all positive integers n divisible by w_{12}, $K(\alpha^n) = H$.*

Proof. A proof for n a multiple of 24 is given by Schertz [Sc], and it works equally well here, thanks to Theorem 19 and Lemma 14. We sketch it briefly. It suffices to consider $\mathscr{A} = \mathscr{P}$ a prime ideal of norm p. For a character ψ of

$G = \mathrm{Gal}(H/K)$, we put $L(s, \psi, \mathscr{P}) = L(s, \psi)(1 - \psi(\sigma_{\mathscr{P}})\mathbb{N}\mathscr{P}^{-s})$, which vanishes at $s = 0$ with the leading term

$$L'(0, \psi, \mathscr{P}) = \begin{cases} L(0, \psi_1) \log p & \psi = \psi_1 \\ L'(0, \psi)(1 - \psi(\sigma_{\mathscr{P}})) & \psi \neq \psi_1. \end{cases}$$

Now suppose $G_1 = \mathrm{Gal}(H/K(\alpha^n))$ is nontrivial. One easily finds a character ψ of G such that $\psi|_{G_1}$ and $\psi(\sigma_{\mathscr{P}})$ are nontrivial. For such a ψ, the Kronecker limit formula reads (see [H1])

$$L'(0, \chi, \mathscr{P}) = -\frac{1}{n} \sum_{\sigma \in G} \psi(\sigma) \log |(p^{12n}\alpha^n)^{\sigma}|^2.$$

By rewriting the sum over G/G_1 and using the orthogonality relations, one concludes that $L'(0, \psi, \mathscr{P}) = 0$, hence $L'(0, \psi) = 0$, but the nonvanishing of $L'(0, \psi)$ is well known and can be seen, for instance, from $\zeta_H(s) = \prod_{\psi} L(s, \psi)$. ■

COROLLARY 27. *If $C \in \mathrm{Cl}(\mathfrak{o})$ is nontrivial, then $\mathbb{Q}(v_C) = H^+$.*

Proof. The proof is clear. ■

For the three 4-types of $\mathfrak{o}$ which are maximal at 2 but for which 2 is not inert, namely, $2_+^0, 2_+^2$, and 2^3, there is a proper primitive ideal $\mathscr{P}_2 \subset \mathfrak{o}$ of norm 2 whose corresponding unit $u_{\mathscr{P}_2}$ is related via a simple formula to the j-invariant of $\mathfrak{o}$. This formula facilitates the computation of the minimal polynomial of j for large discriminants by lowering the required numerical precision as follows: one may first calculate $u_{\mathscr{P}_2}$ (and its conjugates) using Lemma 23(v), then use the explicit expression of j in terms of $u_{\mathscr{P}_2}$ to compute the conjugates of j, which are much larger and hence would require higher accuracy to compute directly. To explain the exact connection, we introduce the Weber functions (see [We])

$$\mathfrak{f}(z) = e_{48}(-1)\frac{\eta((z+1)/2)}{\eta(z)}, \qquad \mathfrak{f}_1(z) = \frac{\eta(z/2)}{\eta(z)}, \qquad \mathfrak{f}_2(z) = \sqrt{2}\frac{\eta(2z)}{\eta(z)},$$

which satisfy

$$\mathfrak{f}\mathfrak{f}_1\mathfrak{f}_2 = \sqrt{2} \tag{9}$$

and are related to $j = \gamma_2^3$ via

$$\gamma_2 = \frac{\mathfrak{f}^{24} - 16}{\mathfrak{f}^8} = \frac{\mathfrak{f}_1^{24} + 16}{\mathfrak{f}_1^8} = \frac{\mathfrak{f}_2^{24} + 16}{\mathfrak{f}_2^8}. \tag{10}$$

The determination of the following "class invariants" (elements of H) was made by Weber [We, p. 473].

THEOREM 28. *For each of the 4-types of* $\mathfrak{o}$ *listed in Table 5,* $\mathscr{P}_2$ *is a proper primitive ideal of* $\mathfrak{o}$, *whose corresponding unit* $u = u_{\mathscr{P}_2}$ *has the indicated expression in terms of* $\mathfrak{f}$ *or* $\mathfrak{f}_1$, *giving rise to a class invariant that is a unit generator of* H^+; *the last column gives an expression for* $j(\sqrt{-d_0})$ *in terms of* u. *Moreover, for the 4-type* 2_+^2, *if* $d_0 \equiv 1 \pmod 8$, *then* $(\mathfrak{f}^2(\sqrt{-d_0})/\sqrt{2})^{w_3}$ *is a class invariant.*

Proof. All claims follow easily from Lemma 23, with the help of (1), (9), and (10). For the last statement of (ii), we use the fact that there is an ideal of norm $(d_0+1)/2 \equiv 1 \pmod 4$ in the class of $\mathscr{P}_2$. We leave the remaining details to the reader. ■

TABLE 5

4-type	$\mathscr{P}_2$	$u = u_{\mathscr{P}_2}$	class invariant	$j(\sqrt{-d_0})$
2_+^0	$[(1+\sqrt{-d_0})/2, 2]$	$\mathfrak{f}(\sqrt{-d_0})/\sqrt{2}$	$(\mathfrak{f}(\sqrt{-d_0})/2)^{w_3}$	$(256u^{24}-1)^3/u^{24}$
2_+^2	$[1+\sqrt{-d_0}), 2]$	$\mathfrak{f}^2(\sqrt{-d_0})/\sqrt{2}$	$(\mathfrak{f}^4(\sqrt{-d_0})/2)^{w_3}$	$64(4u^{12}-1)^3/u^{12}$
2^3	$[\sqrt{-d_0}), 2]$	$\mathfrak{f}_1^2(\sqrt{-d_0})/\sqrt{2}$	$(\mathfrak{f}_1^2(\sqrt{-d_0})/2)^{w_3}$	$64(4u^{12}+1)^3/u^{12}$

Remark. For an order $\mathfrak{o}$ of 4-type 2_+^0, $j(\sqrt{-d})$ is the j-invariant of the lattice $\mathfrak{o}' = [1, \sqrt{-d}]$ (a suborder of index 2 and type 2_-^2) whose ring class field coincides with that of $\mathfrak{o}$. We may express the j-invariant of $\mathfrak{o}$ itself as

$$j((1+\sqrt{-d})/2) = -(16u^{24}-1)^3/u^{48},$$

because $u = e_{48}(1)\mathfrak{f}_2^{-1}((1+\sqrt{-d})/2)$. For the orders of discriminant $-7, -28, -4$, and -8 with class number 1, the unit $u = u_{\mathscr{P}_2}$ is a rational integer; hence $u^2 = 1$, and the above theorem gives the well-known values

$$j\left(\frac{1+\sqrt{-7}}{2}\right) = -3^3 \cdot 5^3, \qquad j(\sqrt{-7}) = 3^3 \cdot 5^3 \cdot 17^3,$$

$$j(\sqrt{-1}) = 2^6 \cdot 3^3, \qquad j(\sqrt{-2}) = 2^6 \cdot 5^3.$$

Our results give an efficient method for calculating a defining polynomial for $H/\mathbb{Q}$ of reasonably small height. One can choose an ideal $\mathscr{A} \in I^*(6d)$ that is not principal, and set $\alpha_1 = \eta(\mathscr{A})/\eta(\mathfrak{o})$; if $m \in \mathbb{Z}$ satisfies $m(\mathbb{N}\mathscr{A}-1)/2 \equiv 0 \pmod{w_{12}}$, then α_1^m generates H over $\mathbb{Q}$. If $\mathscr{A}^2$ is not principal (only finitely many $\mathfrak{o}$ have exponent-2 class group), upon setting $\alpha_2 = \eta(\mathscr{A}^2)/\eta(\mathfrak{o})$, another generator for $H/\mathbb{Q}$ is α_2^n whenever $n(\mathbb{N}\mathscr{A}^2-1)/2 \equiv 0 \pmod{w_{12}}$, and this ele-

ment sometimes has smaller height. The minimal polynomial of α_2^n over $\mathbb{Q}$ is computed easily as $g(x)\bar{g}(x)$, where

$$g(x) = \prod_{\mathscr{B}} \left(x - \frac{\eta(\mathscr{A}^2\mathscr{B})^n}{\eta(\mathscr{B})^n} \right),$$

the product being over ideals $\mathscr{B} \in I^*(6ad)$ representing $\mathrm{Cl}(\mathfrak{o})$. We mention in passing that α_2/α_1^2 is a very useful unit (cf. [H1] and [H2] for numerical examples).

For many purposes, a defining polynomial for $H^+/\mathbb{Q}$ suffices and is more desirable, having half the degree and (usually) much smaller height. For this, one may compute the minimal polynomial of v_C for some nonprincipal class C using Lemma 23(ii), (v). It helps to choose C with n_C as small as possible; by the remarks following Definition 24, we can usually find a class C with $n_C = 1$. As a simple example, the order $\mathfrak{o}$ with discriminant $-336 = -2^4 \cdot 3 \cdot 7$ has class number 8; the values of n_C are $1, 2, 3, 6$, each with multiplicity 2. For the unique nontrivial class C with $n_C = 1$ (represented by a prime ideal of norm 37, for instance), u_C has palindromic minimal polynomial

$$x^8 - 20x^7 + 32x^6 - 12x^5 + 14x^4 - 12x^3 + 32x^2 - 20x + 1.$$

Next we will compute the minimal polynomial of $\gamma_2(\mathfrak{o})$ for the order $\mathfrak{o}$ with discriminant $-728 = -2^3 \cdot 3 \cdot 7$, which has class number 12. The ideal $\mathscr{P}_2$ is in the same class as a prime ideal $\mathscr{P}_{109}$ of norm $109 \equiv 1 \pmod{12}$; hence $u_{\mathscr{P}_2} = u_{\mathscr{P}_{109}} \in H^+$, and we compute its minimal polynomial to be

$$x^{12} - 28x^{11} + 96x^{10} - 84x^9 - 24x^8 - 28x^7 - 46x^6$$

$$+ 28x^5 - 24x^4 + 84x^3 + 96x^2 + 28x + 1. \tag{11}$$

Theorem 28 and (10) give the formula $\gamma_2(\mathfrak{o}) = 4(4u_{\mathscr{P}_2}^{12} + 1)/u_{\mathscr{P}_2}^4$; the minimal polynomial of this number is easily calculated from (11); we list its coefficients in Table 6.

The constant coefficient, in accordance with Gross-Zagier [GZ], factors as

$$2^{24} \cdot 5^{12} \cdot 17^2 \cdot 29^2 \cdot 71^2 \cdot 107^2 \cdot 179^2 \cdot 257 \cdot 521.$$

Finally, consider the order $\mathfrak{o}$ of discriminant $-2^4 \cdot 5$, whose class number is 4. If C is the unique class of order 2, then $n_C = 1$ and u_C has minimal polynomial $x^4 - 2x^3 - 2x^2 - 2x + 1$; indeed, u_C is none other than the elliptic unit first computed by Abel in 1828.

TABLE 6

n	coefficient of x^n
12	1
11	−1866218673280
10	2506323872824179200
9	5860775115793209494400 0
8	384135771128265194122240000
7	−1475847761157625761617920000 0
6	389328264798027989151782400000 0
5	700066934399943089328128000000 00
4	−101619221893541101488447488000000 00
3	−23850774789854573678077747200000000 0
2	−22359123274848856456396800000000000 0
1	33882930912781849064026931200000000000
0	24649887862510135421279027200000000000 0

REFERENCES

[Ab] N. H. ABEL, *Recherches sur les fonctions elliptiques*, J. Reine Angew. Math. **2** (1828), 160–190; reprinted in *Oeuvres completes de Niels Henrik Abel, Vol. 1*, Gröndahl, Oslo, 1881, 380–382.

[AM] A. O. L. ATKIN AND F. MORAIN, *Elliptic curves and primality proving*, Math. Comp. **61** (1993), 29–68.

[De] M. DEURING, *Die Klassenkörper der komplexen Multiplikation*, Enzyklopädie der mathematischen Wissenschaften: Mit Einschluss ihrer Anwendungen, Band I 2, Heft 10, Teil II (Article I 2, 23), B. G. Teubner, Stuttgart, 1958.

[Gr] B. H. GROSS, *Minimal models for elliptic curves with complex multiplication*, Compositio Math. **45** (1982), 155–164.

[GZ] B. H. GROSS AND D. ZAGIER, *On singular moduli*, J. Reine Angew. Math. **355** (1985), 191–220.

[H1] F. HAJIR, *Elliptic units of cyclic unramified extensions of complex quadratic fields*, Acta Arith. **64** (1993), 69–85.

[H2] ———, *Unramified elliptic units*, thesis, Massachusetts Inst. of Technology, 1993.

[He] G. HERGLOTZ, *Über das quadratische Reziprozitätsgesetz in imaginären quadratischen Zahlkörpern*, Leipziger Ber. **73** (1921), 303–310; *Gesammelte Schriften*, §20, Vandenhoeck and Ruprecht, Göttingen, 1979.

[Hu] A. HURWITZ, *Grundlagen einer independenten Theorie der elliptischen Modulfunktionen und Theorie der Multiplikator-Gleichungen erster Stufe*, Math. Ann. **18** (1881), 528–592.

[Kr] L. KRONECKER, "Zur Theorie der Elliptischen Funktionen" in *Leopold Kronecker's Werke, Vol. 4*, 347–495; *Vol. 5*, 1–132, Teubner, Leipzig, 1929.

[KL] D. S. KUBERT AND S. LANG, *Modular Units*, Springer-Verlag, New York, 1981.
[Ro] G. ROBERT, *Unités Elliptiques*, Bull. Soc. Math. France **36**, Soc. Math. France, Paris, 1973.
[Sc] R. SCHERTZ, *Zur Theorie der Ringklassenkörper über imaginär-quadratischen Zalhkörpern*, J. Number Theory **10** (1978), 70–82.
[Sh] G. SHIMURA, *Introduction to the Arithmetic Theory of Automorphic Functions*, Publ. Math. Soc. Japan **11**, Iwanami Shoten, Tokyo, 1971.
[Si] C. L. SIEGEL, *Advanced Analytic Number Theory, 2d ed.*, Tata Inst. Fund. Res. Stud. Math. **9**, Tata Inst. Fund. Res., Bombay, 1980.
[St] H. M. STARK, *L-functions at $s = 1$, IV: First derivatives at $s = 0$*, Adv. Math. **35** (1980), 197–235.
[Wa] G. N. WATSON, *Singular Moduli, III*, Proc. London Math. Soc. (3) **40** (1936), 83–142.
[We] H. WEBER, *Lehrbuch der Algebra, Vol. 3*, Chelsea, New York, 1961.

HAJIR: DEPARTMENT OF MATHEMATICS, CALIFORNIA INSTITUTE OF TECHNOLOGY, PASADENA, CALIFORNIA 91125, USA; fhajir@cco.caltech.edu

VILLEGAS: DEPARTMENT OF MATHEMATICS, PRINCETON UNIVERSITY, PRINCETON, NEW JERSEY 08544; USA; CURRENT: UNIVERSITY OF TEXAS AT AUSTIN, AUSTIN, TEXAS 78712, USA; villegas@math.utexas.edu