Journal de Théorie des Nombres
de Bordeaux ***9*** *(1997), 383–394*

Construction of Ray Class Fields by Elliptic Units

par Reinhard SCHERTZ*

Résumé. En multiplication complexe, il est démontré que les unités elliptiques sont contenues dans certains corps de classes de rayon sur un corps quadratique imaginaire K, et Ramachandra [3] a démontré que ces corps peuvent être engendrés sur K par des unités elliptiques. Pourtant les générateurs construits par Ramachandra impliquent des produits assez compliqués de grandes puissances de valeurs singulières de la fonction de Felix Klein définie plus bas, ainsi que des produits de valeurs du discriminant Δ. Nous démontrons dans cet article que dans la plupart des cas un générateur est donné par une puissance d'une valeur singulière de la fonction de Felix Klein ou bien par le quotient de deux de ces valeurs. Ces dernières sont trés utiles pour des raisons numériques, car les coefficients de leurs polynômes minimaux sont relativement petits, ce qui est mis en évidence par des exemples en fin d'article.

Abstract. From complex multiplication we know that elliptic units are contained in certain ray class fields over a quadratic imaginary number field K, and Ramachandra [3] has shown that these ray class fields can even be generated by elliptic units. However the generators constructed by Ramachandra involve very complicated products of high powers of singular values of the Klein form defined below and singular values of the discriminant Δ. It is the aim of this paper to show, that in many cases a generator over K can be constructed as a power of one singular value of the Klein form or as a quotient of two such values. The latter are very suitable for numerical puposes because it turns out that the coefficients of their minimal polynomials are rather small, as it can be seen in the numerical examples at the end of this article.

* The results of this paper were obtained during an invited stay at the University of Bordeaux. They were favoured by the warm hospitality of the Institute for Mathematics.
Manuscrit reçu le 18 avril 1997.

1. Introduction and Results

We let L be a lattice in $\mathbb{C}$ and ω_1, ω_2 a $\mathbb{Z}$-basis of L with $\Im(\frac{\omega_1}{\omega_2}) > 0$. The normalized Klein form is then defined by

$$\varphi\left(z \left| \begin{matrix} \omega_1 \\ \omega_2 \end{matrix} \right.\right) = 2\pi i \; e^{-\frac{zz^*}{2}} \sigma(z|L) \eta(\frac{\omega_1}{\omega_2})^2 \omega_2^{-1}. \tag{1}$$

Here σ denotes the σ-function of L and η the Dedekind eta-function. z^* is defined by

$$z^* = z_1 \eta_1 + z_2 \eta_2 \tag{2}$$

with the real coordinates z_1, z_2 of $z = z_1\omega_1 + z_2\omega_2$ and the quasi-periods η_1, η_2 of the elliptic Weierstrass ζ-function of L belonging to ω_1, ω_2.

In what follows let K be a quadratic imaginary number field of discriminant d, $\mathfrak{O}$ the ring of integers in K and $\mathfrak{f}$ an integral Ideal of $\mathfrak{O}$. We denote by $K(\mathfrak{f})$ the ray class field modulo $\mathfrak{f}$ over K, and we assume that $\mathfrak{f}$ is also the conductor of $K(\mathfrak{f})/K$. We fix a basis ω_1, ω_2 of $\mathfrak{f}$ with $\Im(\frac{\omega_1}{\omega_2}) > 0$. Then for $\nu \in \mathfrak{O}$ we have

$$\varphi\left(\nu \left| \begin{matrix} \omega_1 \\ \omega_2 \end{matrix} \right.\right) \in K(12f^2) \tag{3}$$

where $f = \min(\mathbb{N} \cap \mathfrak{f})$ is the smallest integer in $\mathfrak{f}$. It follows from the transformation formula of the eta-function, that the 12-th powers of the values in (3) or their quotients are independent of the choice of basis in $\mathfrak{f}$. So we can write more elegantly

$$\begin{aligned} \varphi(\nu|\mathfrak{f})^{12} &= \varphi\left(\nu \left| \begin{matrix} \omega_1 \\ \omega_2 \end{matrix} \right.\right)^{12}, \\ \frac{\varphi(\lambda\nu|\mathfrak{f})}{\varphi(\nu|\mathfrak{f})} &= \frac{\varphi\left(\lambda\nu \left| \begin{smallmatrix} \omega_1 \\ \omega_2 \end{smallmatrix} \right.\right)}{\varphi\left(\nu \left| \begin{smallmatrix} \omega_1 \\ \omega_2 \end{smallmatrix} \right.\right)}. \end{aligned} \tag{4}$$

Using this notation we collect some known facts in Theorem 1 and 2.

THEOREM 1. *1)* $\varphi(\nu|\mathfrak{f})^{12f} \in K(\mathfrak{f})$ *for every* $\nu \in \mathfrak{O} \setminus \mathfrak{f}$.
2) The action of a Frobenius map $\sigma(\mathfrak{c})$ *of* $K(\mathfrak{f})/K$ *belonging to an integral ideal* $\mathfrak{c}$ *prime to* $\mathfrak{f}$ *is given by*

$$\left[\varphi(\nu|\mathfrak{f})^{12f}\right]^{\sigma(\mathfrak{c})} = \varphi(\nu|\mathfrak{f}\mathfrak{c}^{-1})^{12f}.$$

THEOREM 2. *1) If* $\gcd(\mathfrak{f}, \bar{\mathfrak{f}}) = 1$, *then for* $\nu \in \mathfrak{O} \setminus \mathfrak{f}$ *the value* $\varphi(\nu|\mathfrak{f})^{12f}$ *is the* f*-th power of an element of* $K(\mathfrak{f})$.
2) Let λ *be in* $\mathfrak{O}$ *and* $\mathfrak{b}, \mathfrak{c}$ *primitive ideals of norm* b, c, *such that* $\mathfrak{b}\mathfrak{c}$ *is primitive and prime to* $N(\mathfrak{f})$. *We decompose*

$$f = f^* f^{**},$$

where $f^* \in \mathbb{N}$ *is the non split part of* f *and* $f^{**} \in \mathbb{N}$ *the split part of* f. *Further we assume* $N(\mathfrak{b}) \equiv 1 \mod 12$ *and* $N(\lambda\mathfrak{b}) \equiv 1 \mod 2f^*$. *Now using the notation* $[\omega_1, \omega_2] := \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$, *we can find an element* $\beta \in K$, $\Im\beta > 0$, *such that*

$$\mathfrak{f} = f[\beta, 1], \quad \mathfrak{f}\mathfrak{b}^{-1} = f[\frac{\beta}{b}, 1],$$

$$\mathfrak{f}\mathfrak{c}^{-1} = f[\frac{\beta}{c}, 1], \quad \mathfrak{f}\mathfrak{b}^{-1}\mathfrak{c}^{-1} = f[\frac{\beta}{bc}, 1].$$

With this choice of basis we define

$$\theta := \frac{\varphi\left(\lambda \left| \mathfrak{f}\mathfrak{b}^{-1}\right.\right)}{\varphi\left(1\left|\mathfrak{f}\right.\right)} := \frac{\varphi^*\left(\lambda \left| \mathfrak{f}\mathfrak{b}^{-1}\right.\right)}{\varphi^*\left(1\left|\mathfrak{f}\right.\right)} \left(\frac{\eta(\frac{\beta}{b})}{\eta\left(\beta\right)}\right)^2$$

putting $\varphi^*(z|L) := e^{-\frac{zz^*}{2}}\sigma(z|L)$. *The trace of* $f\beta$ *being prime to* f^{**} *there is a solution* $a \in \mathbb{Z}$ *of the congruence* $a \cdot trace(f\beta) \equiv \frac{N(\lambda\mathfrak{b})-1}{2f^*} \mod f^{**}$. *We set* $\zeta := e^{\frac{2\pi i a}{f^{**}}}$.
Then

$$\zeta\theta \in K(\mathfrak{f}) \text{ and } \left(\tfrac{\eta(\frac{\beta}{b})}{\eta(\beta)}\right)^2 \in K(1).$$

Further we have the Galois actions

$$\zeta^{\sigma(\mathfrak{c})} = \zeta^c, \qquad \left(\frac{\varphi^*\left(\lambda\left|\mathfrak{f}\mathfrak{b}^{-1}\right.\right)}{\varphi^*\left(1\left|\mathfrak{f}\right.\right)}\right)^{\sigma(\mathfrak{c})} = \frac{\varphi^*\left(\lambda\left|\mathfrak{f}\mathfrak{b}^{-1}\mathfrak{c}^{-1}\right.\right)}{\varphi^*\left(1\left|\mathfrak{f}\mathfrak{c}^{-1}\right.\right)},$$

$$\left(\frac{\eta(\frac{\beta}{b})}{\eta\left(\beta\right)}\right)^{2\sigma(\mathfrak{c})} = \left(\frac{\eta(\frac{\beta}{bc})}{\eta\left(\frac{\beta}{c}\right)}\right)^2$$

In the following let

(5) $$\mathfrak{f} = \mathfrak{p}_1^{m_1} \cdot \ldots \cdot \mathfrak{p}_s^{m_s}$$

be the decomposition of $\mathfrak{f}$ into powers of prime ideals. We define

(6) $$e_j := \text{ the exponent of } \left(\mathfrak{O}/\mathfrak{p}_j^{m_j}\right)^*.$$

By W we denote the subgroup of roots of unity in K, and we set

(7) $$w = |W|.$$

Using this notation we can now state the main results of this article in the following two Theorems:

THEOREM 3. *Let $\mathfrak{f}$ be the conductor of $K(\mathfrak{f})/K$. We assume that either $\mathfrak{f}$ is the power of a prime ideal or satisfies the condition*

$$e_j \not| 2 \text{ for } j=1,\ldots,s\text{-}1 \text{ and } e_s \not| 2w, \quad \mathfrak{p}_s^{m_s} \not| \gcd(6,w).$$

We let $\mathfrak{b}$ be an integral ideal of K prime to $\mathfrak{f}$, whose ideal class in the ray class group $\mathfrak{K}_{\mathfrak{f}}$ mod $\mathfrak{f}$ has an order different from 1 and 3. Then the numbers

$$\varphi(1\,|\mathfrak{f})^{12fn} \quad and \quad \left(\frac{\varphi\left(1\,\middle|\mathfrak{f}\mathfrak{b}^{-1}\right)}{\varphi(1\,|\mathfrak{f})}\right)^{12fn}, \qquad n=1,2,\ldots,$$

are generators for the extension $K(\mathfrak{f})/K$. Of course, the same is true for all roots of these numbers that, according to Theorem 2 are in $K(\mathfrak{f})$.

If the hypothesis of Theorem 3 about the $\mathfrak{p}_j$'s is not satisfied we can prove a somewhat weaker result. An arbitrary integral ideal $\mathfrak{f}$ can always be decomposed in the form

$$\mathfrak{f} = \mathfrak{f}_1\mathfrak{f}_2, \tag{8}$$

where $\mathfrak{f}_2$ equals $\mathfrak{O}$ or satisfies the hypothesis of Theorem 3. $\mathfrak{f}_1$ is the product of low powers of certain prime ideals above 2,3,5 in the case $d \leq -4$ and also above 7 in the case $d=-3$. Given such a decomposition we set

$$P_{\mathfrak{f}} := \text{ the set of prime ideals dividing } \mathfrak{f}_1. \tag{9}$$

and we state the hypothesis

(10) *For any given complex numbers $\xi_{\mathfrak{p}}$, $\mathfrak{p} \in P_{\mathfrak{f}}$, there exists a character χ of $\mathfrak{K}_1$ such that $\chi(\mathfrak{p}) \neq \xi_{\mathfrak{p}}$ for all $\mathfrak{p} \in P_{\mathfrak{f}}$.*

THEOREM 4. *Let H denote the Hilbert class field of K and let $\mathfrak{b} = (\lambda)$ be a principal ideal in $\mathfrak{O}$ prime to $\mathfrak{f}$, whose ideal class in $\mathfrak{K}_{\mathfrak{f}}$ has an order different from 1 and 3. Then under the hypothesis (10) about $\mathfrak{f}$ the numbers*

$$\varphi(1\,|\mathfrak{f})^{12fn} \quad and \quad \left(\frac{\varphi(\lambda\,|\mathfrak{f})}{\varphi(1\,|\mathfrak{f})}\right)^{12fn}, \qquad n=1,2,\ldots,$$

are generators for the extension $K(\mathfrak{f})/H$.

However numerical examples computed so far suggest the

CONJECTURE. *The assertions of Theorem 3 and 4 hold for an arbitrary conductor $\mathfrak{f}$ and for every ideal $\mathfrak{b}$ prime to $\mathfrak{f}$, whose ideal class in $\mathfrak{K}_{\mathfrak{f}}$ is of order different from 1.*

We will explain later, why our method of proof does not carry over to a full proof of the conjecture.

In view of Theorem 4 one would like to have also a generator for H that is numerically usable. For this pupose we quote from [5] the

THEOREM 5. *Let Δ be the discriminant from the theory of elliptic functions and let $\mathfrak{a}$ and $\mathfrak{b}$ be non principal integral ideals of K. We assume further $\mathfrak{a} = \mathfrak{b}$ if $\mathfrak{a}^2$ and $\mathfrak{b}^2$ are principal. Then*

$$H = K\left(\frac{\Delta(\mathfrak{a})\Delta(\mathfrak{b})}{\Delta(\mathfrak{a}\mathfrak{b})\Delta(\mathfrak{O})}\right).$$

The condition "$\mathfrak{a} = \mathfrak{b}$ if $\mathfrak{a}^2$ and $\mathfrak{b}^2$ are principal" is missing in [5]. It is in fact necessary, because otherwise the element in Theorem 5 is a relative norm to a proper subfield.

It has been worked out in [6] that in many cases the generators in Theorem 5 are even 24^{th} powers of elements in H. This is for example true if $\mathfrak{a}$ and $\mathfrak{b}$ are non principal prime ideals of norm $\equiv 1 \mod 12$ or if the discriminant is prime to 6. In fact one can show using [6] that apart from trivial exceptions the ideals $\mathfrak{a}$ and $\mathfrak{b}$ can always be chosen so that the generator in Theorem 5 is a 24^{th} power of an element in H.

2. Proofs

Theorem 1 and 2 contain known facts that can easily be derived from Stark's reciprocity law [7] and the method described in [6], as it is explained in [4], [6] and [7].

To prove the assertions of Theorems 3 and 4, we let

$$\sigma : \mathfrak{K}_{\mathfrak{f}} \to G(K(\mathfrak{f})/K) \tag{11}$$

be the Artin map between the ray class group $\mathfrak{K}_{\mathfrak{f}}$ and the Galois group of $K(\mathfrak{f})/K$. For a character χ of $\mathfrak{K}_{\mathfrak{f}}$ we consider the sum

$$A_{\mathfrak{f}}(\chi) := \frac{1}{12f} \sum_{\mathfrak{k} \in \mathfrak{K}_{\mathfrak{f}}} \bar{\chi}(\mathfrak{k}) \log \left| \varphi(1|\mathfrak{f})^{12f\sigma(\mathfrak{k})} \right|. \tag{12}$$

Let $\mathfrak{f}_\chi$ denote the conductor of χ, and for every integral ideal $\mathfrak{t}$ satisfying $\mathfrak{f}_\chi | \mathfrak{t} | \mathfrak{f}$ we denote by the same letter the corresponding character of $\mathfrak{K}_{\mathfrak{t}}$. For $\mathfrak{f} = \mathfrak{f}_\chi$ and $\chi \neq 1$ we know from Curt Meyer [2] that the above sum appears as a factor in the value of the L-function of K belonging to χ at $s = 1$. Hence

$$A_{\mathfrak{f}_\chi}(\chi) \neq 0 \quad \text{for} \quad \chi \neq 1. \tag{13}$$

Moreover, we find in [3] the relation

$$A_{\mathfrak{f}}(\chi) = \frac{w_{\mathfrak{f}_\chi}}{w_{\mathfrak{f}}} \Big(\prod_{\mathfrak{p} | \frac{\mathfrak{f}}{\mathfrak{f}_\chi}} (1 - \bar{\chi}(\mathfrak{p})) \Big) A_{\mathfrak{f}_\chi}(\chi), \tag{14}$$

where $w_{\mathfrak{f}}$ and $w_{\mathfrak{f}_\chi}$ denote the number of roots of unity in K congruent to 1 mod $\mathfrak{f}$ resp. mod $\mathfrak{f}_\chi$. Of course, on the right hand side in (14) χ must be understood as a character of $\mathfrak{K}_{\mathfrak{f}_\chi}$. We give a sketch of the proof of (14), which is easily deduced from the following relation between Klein-forms [1]: For any two complex lattices $L \subset L'$ and for any torsion point $t \in \frac{1}{M}L \setminus L$, $M \in \mathbb{N}$, $t \notin L'$, we have

$$\prod_{\substack{\xi \in L' \\ \xi \bmod L}} \varphi(t+\xi|L)^{12m} = \varphi(t|L')^{12m} \tag{15}$$

where $m = \operatorname{lcm}(M, N)$ and N an integer such that $NL' \subset L$. By the exponent 12 the factors in (15) become independent of the choice of basis in L and L', and, due to the exponent m, the values of φ are the same when t is changed modulo L'. We set $t = 1, L' = \mathfrak{f}, L = \mathfrak{f}\mathfrak{p}$ with an integral ideal $\mathfrak{f}$ and a prime ideal $\mathfrak{p}$ of K. Then (15) can be rewritten in the form

$$\prod_{\substack{\mathfrak{k}_{\mathfrak{f}\mathfrak{p}} \in \mathfrak{K}_{\mathfrak{f}\mathfrak{p}} \\ \mathfrak{k}_{\mathfrak{f}\mathfrak{p}} \subset \mathfrak{e}_{\mathfrak{f}}}} \varphi(1|\mathfrak{f}\mathfrak{p})^{m\frac{w_{\mathfrak{f}}}{w_{\mathfrak{f}\mathfrak{p}}}\sigma(\mathfrak{k}_{\mathfrak{f}\mathfrak{p}})} = \begin{cases} \varphi(1|\mathfrak{f})^m, \text{ if } \mathfrak{p}|\mathfrak{f}, \\ \dfrac{\varphi(1|\mathfrak{f})^m}{\varphi(1|\mathfrak{f})^{m\sigma(\mathfrak{p}^{-1}\mathfrak{e}_{\mathfrak{f}})}}, \text{ if } \mathfrak{p} \nmid \mathfrak{f}, \end{cases} \tag{16}$$

where $m = 12fN(\mathfrak{p})$ and $\mathfrak{e}_{\mathfrak{f}}$ denotes the unit class in $\mathfrak{K}_{\mathfrak{f}}$. Now, taking conjugates and logarithms of (16), we find the relation

$$A_{\mathfrak{f}\mathfrak{p}}(\chi) = \frac{w_{\mathfrak{f}}}{w_{\mathfrak{f}\mathfrak{p}}}(1 - \bar{\chi}(\mathfrak{p}))A_{\mathfrak{f}}(\chi), \tag{17}$$

which implies (14). We observe that $A_{\mathfrak{f}}(\chi)$ may vanish if $\mathfrak{f} \neq \mathfrak{f}_\chi$. This is in fact the obstacle for the proof of the above conjecture. However $A_{\mathfrak{f}}(\chi)$ is non zero for enough $\mathfrak{f}$'s and χ's to prove the following lemma, which yields the proof of the Theorems 3 and 4.

The proof of Theorem 4 is obtained in the same way. We observe that the subgroup $\mathfrak{U}$ in (19) corresponding to the intermediate field L generated by ϵ over H consists of principal ideals, thus making the application of Lemma 1 possible.

LEMMA 1. *Let $\mathfrak{a}$ and $\mathfrak{b}$ be ideals in K, prime to $\mathfrak{f}$ and not contained in the unit class of $\mathfrak{K}_{\mathfrak{f}}$. Then under the hypothesis of Theorem 3 about $\mathfrak{f}$ and d there exists a character χ of $\mathfrak{K}_{\mathfrak{f}}$ satisfying*

$$A_{\mathfrak{f}}(\chi) \neq 0,$$
$$\chi(\mathfrak{a}) \neq 1 \text{ and } \chi(\mathfrak{b}) \neq 1.$$

The same assertion holds under the hypothesis of Theorem 4, if $\mathfrak{a}$ and $\mathfrak{b}$ are principal.

We postpone the proof of lemma 1 and begin by showing how the assertions of Theorems 3 and 4 follow from it:

Proof of Theorem 3: Assume that

$$\epsilon := \varphi(1|\mathfrak{f})^{12fn} \tag{18}$$

generates over K an intermediate field L of $K(\mathfrak{f})/K$. We consider the diagram of the fields in play and corresponding subgroups of $\mathfrak{K}_\mathfrak{f}$:

$$\begin{array}{ccc} K(\mathfrak{f}) & \longleftrightarrow & \{1\} \\ | & & | \\ L & \longleftrightarrow & \mathfrak{U} \\ | & & | \\ K & \longleftrightarrow & \mathfrak{K}_\mathfrak{f} \end{array} \tag{19}$$

We assume now that $L \neq K(\mathfrak{f})$. Then $\mathfrak{U} \neq \{1\}$, and by lemma 1 there exists a character χ of $\mathfrak{K}_\mathfrak{f}$ with the property

$$\chi|\mathfrak{U} \neq 1 \text{ and } A_\mathfrak{f}(\chi) \neq 0. \tag{20}$$

This leads to a contradiction for, appealing to $\epsilon^{\sigma(\mathfrak{h})} = \epsilon$ for $\mathfrak{h} \in \mathfrak{U}$, we can rewrite $A_\mathfrak{f}(\chi)$ in the form

$$\begin{aligned} A_\mathfrak{f}(\chi) &= \tfrac{1}{12fn} \sum_{\mathfrak{k}\in\mathfrak{K}_\mathfrak{f}} \bar{\chi}(\mathfrak{k}) \log \left|\epsilon^{\sigma(\mathfrak{k})}\right| \\ &= \tfrac{1}{12fn} \sum_{\substack{\mathfrak{k}\in\mathfrak{K}_\mathfrak{f} \\ \mathfrak{k} \bmod \mathfrak{U}}} \bar{\chi}(\mathfrak{k}) \left(\sum_{\mathfrak{h}\in\mathfrak{U}} \bar{\chi}(\mathfrak{h}) \right) \log \left|\epsilon^{\sigma(\mathfrak{k})}\right|, \end{aligned} \tag{21}$$

where the inside sum of the right hand side must be zero because of $\chi|\mathfrak{U} \neq 1$. Hence $L = K(\mathfrak{f})$. This proves the first assertion of Theorem 3. The second assertion is obtained in the same way. Setting

$$\epsilon = \frac{\varphi(1|\mathfrak{f}\mathfrak{b}^{-1})^{12fn}}{\varphi(1|\mathfrak{f})^{12fn}} \text{ and } L = K(\epsilon), \tag{22}$$

we have

$$\epsilon = \varphi(1|\mathfrak{f})^{12fn(\sigma(\mathfrak{b})-1)}. \tag{23}$$

We assume that $L \neq K(\mathfrak{f})$, and as in (21) we find

$$(\chi(\mathfrak{b}) - 1)A_\mathfrak{f}(\chi) = \frac{1}{12fn} \sum_{\substack{\mathfrak{k}\in\mathfrak{K}_\mathfrak{f} \\ \mathfrak{k} \bmod \mathfrak{U}}} \bar{\chi}(\mathfrak{k}) \left(\sum_{\mathfrak{h}\in\mathfrak{U}} \bar{\chi}(\mathfrak{h}) \right) \log \left|\epsilon^{\sigma(\mathfrak{k})}\right|, \tag{24}$$

where $\mathfrak{U}$ denotes the subgroup of $\mathfrak{K}_\mathfrak{f}$ corresponding to L. The assumption $L \neq K(\mathfrak{f})$ implies $\mathfrak{U} \neq \{1\}$, and we get a contradiction if, according to the lemma, we choose χ so that

$$\chi|\mathfrak{U} \neq 1, \chi(\mathfrak{b}) \neq 1 \text{ and } A_\mathfrak{f}(\chi) \neq 0. \tag{25}$$

This completes the proof of Theorem 3.

Proof of lemma 1:

It suffices to prove the Lemma when the orders of $\mathfrak{a}$ and $\mathfrak{b}$ are prime numbers.

$$o(\mathfrak{a}) = p, \quad o(\mathfrak{b}) = q \neq 3. \tag{26}$$

It is an elementary fact about a finite abelian group G, that for two elements in G different from the unit element there exists a character whose value at the two elements is different from 1. So for $\mathfrak{a}$ and $\mathfrak{b}$ satisfying the hypothesis of lemma 1 we can find a character χ of $\mathfrak{K}_\mathfrak{f}$ so that

$$\chi(\mathfrak{a}) \neq 1, \chi(\mathfrak{b}) \neq 1. \tag{27}$$

We will now change χ so that in addition to (27) we have $A_\mathfrak{f}(\chi) \neq 0$. If $\mathfrak{f}$ is the power of a prime ideal $\mathfrak{p}$, this is not necessary, because then $\chi \neq 1$ implies $\mathfrak{p}|\mathfrak{f}_\chi$. Otherwise we must look at the prime ideals dividing the conductor of χ. So we consider the character $\hat{\chi}$ of $(\mathfrak{O}/\mathfrak{f})^*$ defined by χ via the homomorphism

$$\begin{array}{ccc} (\mathfrak{O}/\mathfrak{f})^* & \rightarrow & \mathfrak{K}_\mathfrak{f} \\ \xi + \mathfrak{f} & \mapsto & \xi \mathfrak{e}_\mathfrak{f} \end{array} \tag{28}$$

with kernel $(W + \mathfrak{f})/\mathfrak{f}$, $e_\mathfrak{f}$ denoting the unit class in $\mathfrak{K}_\mathfrak{f}$. According to the decomposition

$$(\mathfrak{O}/\mathfrak{f})^* \cong (\mathfrak{O}/\mathfrak{p}_1^{m_1})^* \times ... \times (\mathfrak{O}/\mathfrak{p}_s^{m_s})^*, \tag{29}$$

we can write $\hat{\chi}$ as a product

$$\hat{\chi} = \chi_1 \cdot .. \cdot \chi_s \tag{30}$$

of characters χ_i of $(\mathfrak{O}/\mathfrak{p}_i^{m_i})^*$, and we have the implication

$$\chi_i \neq 1 \Longrightarrow \mathfrak{p}_i|\mathfrak{f}_\chi. \tag{31}$$

Thus if all the χ_j are non trivial, we can conclude from (14) that $A_\mathfrak{f}(\chi) \neq 0$. Otherwise we change χ so that in addition to (27) all the χ_j are non trivial. We assume that $\chi_1 = 1$. By definition of e_1 and e_s there exist characters ψ_1, ψ_s of $(\mathfrak{O}/\mathfrak{p}_1^{m_1})^*$ and $(\mathfrak{O}/\mathfrak{p}_s^{m_s})^*$ of order e_1 and e_s. Furthermore by the hypothesis "$\mathfrak{p}_s^{m_s} \not| \gcd(6,w)$" we can choose ψ_s so that viewing ψ_s as a character of $(\mathfrak{O}/\mathfrak{f})^*$ we have

$$\psi_s\left((W+\mathfrak{f})/\mathfrak{f}\right) = W. \tag{32}$$

This implies that we can find $\kappa \in \mathbb{N}$ such that

$$\psi = \psi_1 \psi_s^{\kappa} \tag{33}$$

is trivial on $(W+\mathfrak{f})/\mathfrak{f}$. Thus ψ can be viewed as a character of the image in (28). Using the same letter we extend ψ to a character of $\mathfrak{K}_{\mathfrak{f}}$ and set

$$\tilde{\chi} = \chi\psi^{2\mu},\ \mu \in \mathbb{Z},\ gcd(\mu, e_1) = 1. \tag{34}$$

Then because of $e_1 \not| 2$ the conductor of $\tilde{\chi}$ must be divisible by $\mathfrak{p}_1$, whereas the powers of $\mathfrak{p}_2, ..., \mathfrak{p}_{s-1}$ dividing $\mathfrak{f}_{\tilde{\chi}}$ are the same as those dividing $\mathfrak{f}_{\chi}$. By a suitable choice of μ in (34) we must now achieve, that (27) ist satisfied also for $\tilde{\chi}$. This means

$$\psi^{2\mu}(\mathfrak{a}) \neq \chi^{-1}(\mathfrak{a}),\quad \psi^{2\mu}(\mathfrak{b}) \neq \chi^{-1}(\mathfrak{b}). \tag{35}$$

Now recalling $q \neq 3$ we distinguish the cases $p = q = 2$, $p = q \geq 5$, and $p \neq q$. If $p = q = 2$ we have $\psi^2(\mathfrak{a}) = \psi^2(\mathfrak{b}) = 1$ and (35) holds because of $\chi^{-1}(\mathfrak{a}), \chi^{-1}(\mathfrak{b}) \neq 1$. If $p = q \geq 5$ and $p \not| e_1$ we can conclude in the same way. Otherwise at most two prime residues μ mod p are forbidden by (35) hence at least two are left to satisfy (35). In the case $p \neq q$ at most one prime residue μ mod p is forbidden by (35) if $p \neq 2$ and at most one prime residue μ mod q, if $q \neq 2$. So we can find μ by solving simultaneous congruences.
Proceeding in this way for $j = 2, ..., s-1$ we end up with a character $\tilde{\chi}$, whose conductor is divisible by $\mathfrak{p}_1 \cdot ... \cdot \mathfrak{p}_{s-1}$. If now $\mathfrak{p}_s \not| \mathfrak{f}_{\tilde{\chi}}$, we set

$$\tilde{\tilde{\chi}} = \tilde{\chi}\tilde{\psi}^{2\mu},\quad \mu \in \mathbb{Z},\ \gcd(\mu, e_s) = 1,\quad \tilde{\psi} = \psi_s^{w}, \tag{36}$$

We observe that $\tilde{\psi}^{2\mu}$ is non trivial because of $e_s \not| 2w$. Hence the conductor of $\tilde{\tilde{\chi}}$ equals the conductor of $\tilde{\chi}$ times a power of $\mathfrak{p}_s$. Furthermore μ can be chosen so that (27) is satisfied by $\tilde{\tilde{\chi}}$. So $\tilde{\tilde{\chi}}$ has the desired properties, and Lemma 1 is proved under the hypothesis of Theorem 3.

We now let $\mathfrak{f}$ satisfy the hypothesis of Theorem 4. Applying the above construction, we find a character $\tilde{\chi}$ with the property (27), whose conductor is divisible by all the $\mathfrak{p}_j$'s that are not in the set $P_{\mathfrak{f}}$ defined in (9). $\tilde{\chi}$ can be viewed as a character of $\mathfrak{K}_{\mathfrak{f}_0}$ where $\mathfrak{f}_0$ is defined by

$$\mathfrak{f}_0 = \prod_{\mathfrak{p}_j | \mathfrak{f}_{\tilde{\chi}}} \mathfrak{p}_j^{m_j} \tag{37}$$

We set

$$Q_{\tilde{\chi}} = \{\mathfrak{p} \mid \mathfrak{p}|\mathfrak{f} \text{ and } \mathfrak{p} \not| \mathfrak{f}_{\tilde{\chi}}\}. \tag{38}$$

Then $Q_{\tilde{\chi}}$ is a subset of $P_{\mathfrak{f}}$ and thus by (10) for

$$\xi_{\mathfrak{p}} = \tilde{\chi}(\mathfrak{p}),\ \mathfrak{p} \in Q_{\tilde{\chi}}, \tag{39}$$

there exists a character χ' of $\mathfrak{K}_1$ such that

$$\chi'(\mathfrak{p}) \neq \xi_{\mathfrak{p}},\ \mathfrak{p} \in Q_{\tilde{\chi}}. \tag{40}$$

So by setting

$$\tilde{\tilde{\chi}} = \tilde{\chi}\chi' \tag{41}$$

we have constructed a character satisfying

$$\begin{array}{l} \mathfrak{p}_j|\mathfrak{f}_{\tilde{\tilde{\chi}}} \text{ for } \mathfrak{p}_j|\mathfrak{f},\ \mathfrak{p}_j \notin Q_{\tilde{\chi}}, \\ \tilde{\tilde{\chi}}(\mathfrak{p}_j) \neq 1 \text{ for } \mathfrak{p}_j \in Q_{\tilde{\chi}}, \end{array} \tag{42}$$

and, appealing to (14), we have

$$A_{\mathfrak{f}}(\tilde{\tilde{\chi}}) \neq 0. \tag{43}$$

Furthermore remembering that $\mathfrak{a}$ and $\mathfrak{b}$ are principal ideals, we see that $\chi'(\mathfrak{a}) = \chi'(\mathfrak{b}) = 1$. So $\tilde{\tilde{\chi}}$ satisfies (27), because $\tilde{\chi}$ does. This completes the proof of Lemma 1 under the assumptions of Theorem 4.

Examples:

In the following examples we consider elliptic units of the form

$$\epsilon := \frac{\varphi(\lambda\,|\mathfrak{f})}{\varphi(1\,|\mathfrak{f})}. \tag{44}$$

Computing their conjugates by Theorem 1 we determine their minimal polynomial with respect to K.

Example 1: We set $d = -19$, $\mathfrak{f} = (2\sqrt{-19})$ and $\lambda = \frac{17+\sqrt{-19})}{2}$. Then (λ) has order 3 in $\mathfrak{K}_{\mathfrak{f}}$. So this is a case excepted in Theorem 3. But, confirming our conjecture, the computation shows that the number ϵ is a generator of $K(2\sqrt{-19})/K$. The minimal polynomial is given by

$$
\begin{aligned}
X^{27} & +\left(\tfrac{-9-\sqrt{-19}}{2}\right)X^{26}+\left(\tfrac{-11-9\sqrt{-19}}{2}\right)X^{25}+\left(\tfrac{-113+5\sqrt{-19}}{2}\right)X^{24}\\
& +\left(\tfrac{-197-\sqrt{-19}}{2}\right)X^{23}+\left(\tfrac{497+77\sqrt{-19}}{2}\right)X^{22}+\left(14-219\sqrt{-19}\right)X^{21}\\
& +\left(\tfrac{-1507-121\sqrt{-19}}{2}\right)X^{20}+\left(\tfrac{-3853-313\sqrt{-19}}{2}\right)X^{19}\\
& +\left(908+839\sqrt{-19}\right)X^{18}+\left(\tfrac{-1019-1582\sqrt{-19}}{2}\right)X^{17}\\
& +\left(\tfrac{-10159+5715\sqrt{-19}}{2}\right)X^{16}+\left(13307-2428\sqrt{-19}\right)X^{15}\\
& +\left(\tfrac{-38379+2225\sqrt{-19}}{2}\right)X^{14}+\left(\tfrac{38379+2225\sqrt{-19}}{2}\right)X^{13}\\
& +\left(-13307-2428\sqrt{-19}\right)X^{12}+\left(\tfrac{10159+5715\sqrt{-19}}{2}\right)X^{11}\\
& +\left(1019-1582\sqrt{-19}\right)X^{10}+\left(-908+839\sqrt{-19}\right)X^{9}\\
& +\left(\tfrac{3853-313\sqrt{-19}}{2}\right)X^{8}+\left(\tfrac{1507-121\sqrt{-19}}{2}\right)X^{7}+\left(-14-219\sqrt{-19}\right)X^{6}\\
& +\left(\tfrac{-497+77\sqrt{-19}}{2}\right)X^{5}+\left(\tfrac{197-\sqrt{-19}}{2}\right)X^{4}+\left(\tfrac{113+5\sqrt{-19}}{2}\right)X^{3}\\
& +\left(\tfrac{11-9\sqrt{-19}}{2}\right)X^{2}+\left(\tfrac{9-\sqrt{-19}}{2}\right)X-1
\end{aligned}
$$

Example 2: We set $d=-7$, $\mathfrak{f}=\mathfrak{p}_2^2(\sqrt{-7})$, $\mathfrak{p}_2=\left(\frac{-1+\sqrt{-7})}{2}\right)$, which is one of the cases excepted in Theorem 3 and 4. We choose $\lambda=13$. Then, confirming the conjecture, ϵ is a generator of $K(\mathfrak{f})/K$ with the minimal polynomial

$$
\begin{aligned}
X^{6} & +(-1+\sqrt{-7})X^{5}-\left(\tfrac{5+\sqrt{-7}}{2}\right)X^{4}+\left(\tfrac{5-\sqrt{-7}}{2}\right)X^{3}\\
& -\left(\tfrac{5+\sqrt{-7}}{2}\right)X^{2}-(1-\sqrt{-7})X+1.
\end{aligned}
$$

Example 3: We set $d=-88$, $\mathfrak{f}=(4)$ and $\lambda=1+2\sqrt{-22}$. Then, according to Theorem 3 the number ϵ is a generator of $K(4)/K$ with the minimal polynomial

$$
\begin{aligned}
X^{8} & +(-12-6\sqrt{-22})X^{7}+(-44+12\sqrt{-22})X^{6}+(48+6\sqrt{-22})X^{5}+32X^{4}\\
& +(48-6\sqrt{-22})X^{3}+(-44-12\sqrt{-22})X^{2}+(12+\sqrt{-22})X+1.
\end{aligned}
$$

We include also an example for Theorem 5: Let $K=\mathbb{Q}(\sqrt{-523})$ and $\mathfrak{a}=\mathfrak{b}=\mathbb{Z}7+\mathbb{Z}\frac{3+\sqrt{-523}}{2}$. Then a 24^{th} root of the number in Theorem 5 is a generator for H/K. Its minimal polynomial is

$$X^5+6X^4+59X^3-X^2+64X-1.$$

References

[1] D. Kubert, S. Lang, *Modular Units*, Grundlehren Math. Wiss., Vol. 244, Springer-Verlag, New-York/Berlin, (1981).

[2] C. Meyer, *Die Berechnung der Klassenzahl abelscher Körper über quadratischen Zahlkörpern*, Akademie-Verlag, Berlin (1957).

[3] K. Ramachandra, Some Applications of Kronecker's limit formula, *Ann. Math.* 80 (1964), 104-148.

[4] R. Schertz, Galoismodulstruktur und elliptische Funktionen, *Journal of Number Theory*, Vol. 39, No. 3, (1991.

[5] R. Schertz, Problèmes de construction en multiplication complexe, *Séminaire de Théorie des Nombres de Bordeaux* 4 (1992), 239-262.
[6] R. Schertz, Zur expliziten Berechnung von Ganzheitsbasen in Strahlklassenkörpern über einem imaginär-quadratischen Zahlkörper, *Journal of Number Theory*, Vol. 34, No. 1 (1990), 41-53.
[7] H. Stark, L-functions at $s = 1$, IV, *Advances in Math.* 35 (1980), 197-235.

Reinhard SCHERTZ
Institut für Mathematik der Universität Augsburg
Universitätsstraße 8, 86159 Augsburg
Germany
e-mail: schertz@uni-augsburg.de