ILLINOIS JOURNAL OF MATHEMATICS
Volume 32, Number 3, Fall 1988

SWAN MODULES AND ELLIPTIC FUNCTIONS

BY

ANUPAM SRIVASTAV[1]

Dedicated to the memory of Irving Reiner

1. Introduction

The normal basis theorem for a finite Galois extension N/L states that N as an L-vector space has a basis of the form $\{a^\gamma\}$, where a is a fixed element of N and γ runs over the Galois group $\mathrm{Gal}(N/L) = \Gamma$. In other words, N is a free rank one $L\Gamma$-module. The analogous question for the rings of algebraic integers, $\mathcal{O}_N$ in N and $\mathcal{O}_L$ in L, is the well-known normal integral basis problem. In fact, $\mathcal{O}_N$ is an $\mathcal{A}$-module where

$$\mathcal{A} = \{x \in L\Gamma : \mathcal{O}_N x \subseteq \mathcal{O}_N\},$$

the associated order of the extension N/L in $L\Gamma$. Thus the best possible result would be that $\mathcal{O}_N$ is $\mathcal{A}$-free.

Abelian extensions of $\mathbf{Q}$ are contained in cyclotomic extensions. Leopoldt [4] has shown that in the case that $L = \mathbf{Q}$ and Γ is abelian, $\mathcal{O}_N$ is, indeed, $\mathcal{A}$-free. Furthermore, he has described the order $\mathcal{A}$ explicitly. In the relative case, where both L and N are cyclotomic fields we have the following result [1, Chapter I].

PROPOSITION (1.1). *Let m, r be positive integers such that m divides r. Let $N = \mathbf{Q}(\zeta)$, $L = \mathbf{Q}(\zeta^m)$ where ζ is a primitive mr-th root of unity in $\mathbf{C}$. Let $\Gamma = \mathrm{Gal}(N/L)$ and $\mathcal{A}$ be the associated order of N/L in $L\Gamma$. Then, $\mathcal{O}_N$ is a free rank one $\mathcal{A}$-module.*

Abelian extensions of a quadratic imaginary number field are obtained by adjoining singular values of certain elliptic functions. In [10], M.J. Taylor has obtained elliptic analogues of (1.1) for certain Kummer extensions with respect to an elliptic group law. Taylor showed that the ring of algebraic

Received August 11, 1987.

[1]Based on a part of the author's Ph.D. thesis. Partially supported by a grant from the National Science Foundation.

integers is free over the associated order if, and only if, a certain elliptic analogue of a Swan module is a principal ideal of the associated order. In this paper we use transcendental means to settle the algebraic question of the freeness of this elliptic Swan module. We find an explicit generator for the square of this elliptic Swan module in quite a general case. This generator is a product of elliptic resolvent elements.

For a number field M, we continue to write $\mathcal{O}_M$ for its ring of algebraic integers. Let K be a quadratic imaginary number field with discriminant less than -4. Moreover, assume the prime 2 splits in $K/\mathbf{Q}$. Let $\mathfrak{p} = \lambda\mathcal{O}_K$ denote a non-ramified, principal prime ideal of $\mathcal{O}_K$, where $\lambda \equiv \pm 1 \bmod 4\mathcal{O}_K$. We fix positive integers $r \geq m$ and let N (respectively, L) denote K ray classfield $\bmod 4\mathfrak{p}^{m+r}$ (respectively, $4\mathfrak{p}^r$). As before, we write $\Gamma = \mathrm{Gal}(N/L)$ and $\mathcal{A}$ denotes the associated order of N/L in $L\Gamma$.

We remark at the outset that Γ is an abelian group so that $L\Gamma$ is a commutative L-algebra. The restriction on the discriminant implies that the group of units $\mathcal{O}_K^\times$ of K is $\{\pm 1\}$. Moreover, the restriction on λ implies that $\mathfrak{p}$ is completely split in $K(4)$, the K ray classfield $\bmod 4\mathcal{O}_K$. In [1], Ph. Cassou-Noguès and Taylor have described N as a Kummer extension over L with respect to an elliptic group law.

For any commutative ring R we write $(a, b)R$ for the ideal $aR + bR$. Let $\mathfrak{p} \cap \mathbf{Z} = (p)$ for an odd rational prime p. For $s \in \mathbf{Z}$ with $p \nmid s$, we define a locally free $\mathcal{A}$-ideal, $I_s = (s, \lambda^{-m}\Sigma)\mathcal{A}$, where $\Sigma = \Sigma_{\gamma \in \Gamma}\gamma$. The ideal I_s is called an elliptic Swan module since it is a natural elliptic analogue of the Swan module $(s, \Sigma)\mathbf{Z}\Gamma$ for the integral group ring $\mathbf{Z}\Gamma$. In [10], Taylor has shown that $\mathcal{O}_N$ is $\mathcal{A}$-free if, and only if, the elliptic Swan module I_2 is a principal $\mathcal{A}$-ideal.

In case the prime p splits in $K/\mathbf{Q}$ Taylor showed in [9] that $\mathcal{O}_N$ is a free $\mathcal{A}$-module of rank one. The main result of this paper is:

THEOREM (1.2). *If p is inert in $K/\mathbf{Q}$ and $p \equiv \pm 1 \bmod 8$ then I_2 is a principal ideal of the associated order $\mathcal{A}$.*

Remark (1.3). In general, whether or not I_2 is a principal $\mathcal{A}$-ideal in the case that p is inert and $p \equiv \pm 3 \bmod 8$ remains an open question. The only two cases known to the author for which there is a definite answer are:

(i) $m = 1$.

(ii) $m = 2$, and p^2 is a Wieferich square, i.e., $2^{p-1} \equiv 1 \bmod p^2$. An example of such a prime is $p = 1093$.

In both cases I_2 is a principal $\mathcal{A}$-ideal. Also see (2.3).

Remark (1.4). The author would like to thank M.J. Taylor and S.V. Ullom for their kind help and suggestions. The author is also grateful to D.R. Grayson for pointing out the geometry of the Fueter model (cf. §4).

2. Swan modules

We keep the notation of §1 and view $\mathscr{A}$ as a $\mathbf{Z}$-order in the $\mathbf{Q}$-algebra $L\Gamma$.

For each integer s relatively prime to p, the usual Swan module for the integral group ring $\mathbf{Z}\Gamma$ is defined to be the $\mathbf{Z}\Gamma$-ideal $(s, \Sigma)\mathbf{Z}\Gamma$. Since Γ is a p-group and $(s, \Sigma)\mathbf{Z}_p\Gamma = \mathbf{Z}_p\Gamma$, $(s, \Sigma)\mathbf{Z}\Gamma$ is a locally free $\mathbf{Z}\Gamma$-ideal. Thus $(s, \Sigma)\mathbf{Z}\Gamma$ determines a class $[s, \Sigma]$ in $\mathscr{C}\ell(\mathbf{Z}\Gamma)$, the locally free class group of $\mathbf{Z}\Gamma$. In fact, the Swan classes lie in the kernel group $D(\mathbf{Z}\Gamma)$, and the set of all Swan classes $[s, \Sigma]$ with $p \nmid s$, $s \in \mathbf{Z}$ forms a subgroup $T(\mathbf{Z}\Gamma)$ of $\mathscr{C}\ell(\mathbf{Z}\Gamma)$. We call $T(\mathbf{Z}\Gamma)$ the Swan subgroup of $\mathscr{C}\ell(\mathbf{Z}\Gamma)$. We refer the reader to [13] and [8] for the properties of the Swan subgroup. Swan modules were first considered in [6].

The elliptic Swan module I_s and the usual Swan module $(s, \Sigma)\mathbf{Z}\Gamma$ are related by the following.

LEMMA (2.1). *If $p \nmid s$ for $s \in \mathbf{Z}$, then $I_s = (s, \Sigma)\mathscr{A}$.*

Proof. Since $I_s \supseteq (s, \Sigma)\mathscr{A}$, it suffices to show the equality locally at each prime $\mathfrak{q}$ of $\mathcal{O}_L$. Let $\mathfrak{q}$ be a prime of $\mathcal{O}_L$. Then

$$(I_s)_{\mathfrak{q}} = \begin{cases} \mathscr{A}_{\mathfrak{q}} & \text{if } \mathfrak{q} \nmid s, \\ (s, \Sigma)\mathscr{A}_{\mathfrak{q}} & \text{if } \mathfrak{q} \mid s. \end{cases}$$

On the other hand, $(s, \Sigma)\mathscr{A}_{\mathfrak{q}} = \mathscr{A}_{\mathfrak{q}}$ if $\mathfrak{q} \nmid s$.

The change of rings $\mathbf{Z}\Gamma \to \mathscr{A}$ induces a group homomorphism $\mathscr{C}\ell(\mathbf{Z}\Gamma) \to \mathscr{C}\ell(\mathscr{A})$. The kernel group $D(\mathbf{Z}\Gamma)$ is mapped into the kernel group $D(\mathscr{A})$ under this homomorphism. We set $T(\mathscr{A}, \mathbf{Z})$ to be the image of the Swan subgroup under this map. We call $T(\mathscr{A}, \mathbf{Z})$ the elliptic Swan subgroup of $\mathscr{C}\ell(\mathscr{A})$. Let us denote by $[I_s]$ the class determined by the elliptic Swan module I_s in $\mathscr{C}\ell(\mathscr{A})$. By (2.1) we see that $T(\mathscr{A}, \mathbf{Z})$ is the subgroup of all elliptic Swan classes in $\mathscr{C}\ell(\mathscr{A})$. The addition in $T(\mathbf{Z}\Gamma)$ is given by $[s_1, \Sigma] + [s_2, \Sigma] = [s_1 s_2, \Sigma]$ for $s_1, s_2 \in \mathbf{Z}$ with $p \nmid s_1 s_2$. Therefore, $[I_{s_1}] + [I_{s_2}] = [I_{s_1 s_2}]$ in $T(\mathscr{A}, \mathbf{Z})$. We note that since $\mathscr{A}$ is a commutative order an $\mathscr{A}$-ideal I_s is principal if, and only if, $[I_s] = 0$ in $T(\mathscr{A}, \mathbf{Z})$.

PROPOSITION (2.2). (i) *If p splits in $K/\mathbf{Q}$, then $T(\mathscr{A}, \mathbf{Z}) = 0$. In particular, I_2 is a principal $\mathscr{A}$-ideal.*

(ii) *If p is inert in $K/\mathbf{Q}$, then $T(\mathscr{A}, \mathbf{Z})$ is a p-group and $|T(\mathscr{A}, \mathbf{Z})| \leq p^{2m-1}$.*

Proof. (i) In this case Γ is a cyclic group and by [6] we obtain $T(\mathscr{A}, \mathbf{Z}) = 0$.

(ii) In this case Γ is a non-cyclic p-group of order p^{2m}; by Taylor's theorem (cf. [9]) we obtain $|T(\mathbf{Z}\Gamma)| = p^{2m-1}$.

Remark (2.3). In fact, in case p is inert in $K/\mathbf{Q}$ it can be shown that $|T(\mathscr{A}, \mathbf{Z})| \leq p^{m-1}$. This is the basis for (1.3).

3. Galois module structure

We continue to keep the notation of §1. From (26.3) in [2] we know that an order in an algebra is determined by all its localizations (completions). In [10] Taylor has described all the localizations of the $\mathcal{O}_L$-order $\mathscr{A}$ in $L\Gamma$. For any non-zero prime ideal ℓ of $\mathcal{O}_L$ with $\ell \cap \mathbf{Z} = (l)$, we fix an embedding of $\overline{\mathbf{Q}}$, a fixed algebraic closure of $\mathbf{Q}$, in $\overline{\mathbf{Q}}_l$, a fixed algebraic closure of $\mathbf{Q}_l$, so that it corresponds to ℓ for L. For a fixed $M \subset \overline{\mathbf{Q}}$ we write M' for its closure in $\overline{\mathbf{Q}}_l$.

In case $\ell | \mathfrak{p}$, the local associated order has been shown by Taylor to be amenable to the description in [11] by a Lubin-Tate formal group law. To be precise, there is a Lubin-Tate formal group law F over $\mathcal{O}_{K'}$ so that $L' = K'(\omega_r)$, $N' = K'(\omega_{m+r})$, where ω_n denotes a primitive $\mathfrak{p}^n$-division point of F for each $n \geq 0$.

The Artin map of global class field theory induces a group homomorphism

$$\Gamma \cong \frac{1 + \mathfrak{p}^r \mathcal{O}_{K'}}{1 + \mathfrak{p}^{m+r} \mathcal{O}_{K'}} \cong \left[\frac{\mathfrak{p}^r}{\mathfrak{p}^{m+r}} \right]^+ . \tag{3.1}$$

Let G be the group of $\mathfrak{p}^m$-division points of F. Then there is a group isomorphism

$$G \cong \mathfrak{p}^{-m} / \mathcal{O}_K . \tag{3.2}$$

We set $E = \mathcal{O}_K / \mathfrak{p}^m$, a finite ring. We view Γ and G as E-modules via (3.1) and (3.2). Both are free E-modules of rank one. We write the E-actions on Γ and G exponentially as $\gamma^{[e]}$, $g^{[e]}$ for $\gamma \in \Gamma$, $g \in G$ and $e \in E$. Let γ be an E-generator of Γ and $\omega = \omega_m$ a primitive $\mathfrak{p}^m$-division point of F, i.e., an E-generator of G. From [11] and [12] we see that $\mathscr{A}_{N'/L'}$, the associated order of N'/L', can be described as an $\mathcal{O}_{L'}$-module by

$$\mathscr{A}_{N'/L'} = O_{L'} \cdot 1_\Gamma + \sum_{i=0}^{q^m - 2} \mathcal{O}_{L'} \cdot \sigma_i \tag{3.3}$$

where

$$\sigma_i = \lambda^{-m} \sum_{e \in E} (\omega^{[e]})^i (\gamma^{[e]} - 1_\Gamma) \in \mathscr{A}_{N'/L'} \text{ for } i \geq 0, \tag{3.4}$$

and $q = |\mathcal{O}_K / \mathfrak{p}|$.

We obtain the following characterisation of $\mathscr{A}$ from [10].

PROPOSITION (3.5). *The associated order $\mathscr{A}$ is described locally for each prime ℓ of $\mathcal{O}_L$ as follows*:

$$\mathscr{A}_\ell = \begin{cases} \mathcal{O}_{L'}\Gamma & \text{if } \ell \nmid p, \\ \mathscr{A}_{N'/L'} & \text{if } \ell \mid p \end{cases}$$

where $\mathscr{A}_{N'/L'}$ is as in (3.3).

As a corollary, in [10] it is shown that $\mathcal{O}_N$ is a locally free $\mathscr{A}$-module. Moreover, it is easy to see that $\lambda^{-m}\Sigma \in \mathscr{A}$ so that the elliptic Swan module I_s is an $\mathscr{A}$-ideal for each $s \in \mathbf{Z}$, $p \nmid s$.

For an element $x = \sum_{\delta \in \Gamma} a_\delta \delta \in L\Gamma$ we define its antipode by $\bar{x} = \sum_{\delta \in \Gamma} a_\delta \delta^{-1}$. From (3.5) we obtain as in [12]:

COROLLARY (3.6). *If $x \in \mathscr{A}$, then $\bar{x} \in \mathscr{A}$.*

Next, we set $\mathscr{R}_N = \mathcal{O}_L + 2\mathcal{O}_N$, an $\mathcal{O}_L$-order in N. From [10] we obtain that $\mathscr{R}_N$ is a free $\mathscr{A}$-module of rank one. In addition, $\mathscr{R}_N = \mathcal{O}_L \cdot I_2$. Therefore, we have the following (cf. [10]).

PROPOSITION (3.7). *The ring of algebraic integers $\mathcal{O}_N$ is a free $\mathscr{A}$-module if, and only if, I_2 is a principal $\mathscr{A}$-ideal.*

4. Fueter's elliptic functions

Let $\Omega = \mathbf{Z}\omega_1 + \mathbf{Z}\omega_2$ be a lattice in the complex plane with $\operatorname{im}(\omega_1/\omega_2) > 0$. Let us denote by $\mathscr{P}_\Omega$ the usual Weierstrass $\mathscr{P}$-function (for Ω):

$$\mathscr{P}_\Omega(z) = z^{-2} + \sum_{\omega \in \Omega \setminus 0} \left\{ (z - \omega)^{-2} - w^{-2} \right\}. \tag{4.1}$$

We shall simply write $\mathscr{P}$ for $\mathscr{P}_\Omega$ whenever Ω is clear from the context. Let us fix Ω.

The Weierstrass $\mathscr{P}$-function and its derivative $\mathscr{P}'$ are elliptic functions (for Ω) and there is an isomorphism called the Weierstrass model

$$\mathbf{C}/\Omega \tilde{\to} \mathscr{E} \tag{4.2}$$

where $\mathscr{E}$: $y^2 = 4x^3 - g_2 x - g_3$ is an elliptic curve and the above isomor-

phism is given by

$$z \mapsto \begin{cases} (\mathscr{P}(z) : \mathscr{P}'(z) : 1), & z \notin \Omega, \\ (0:1:0), & z \in \Omega, \end{cases}$$

and $g_2 = g_2(\Omega)$, $g_3 = g_3(\Omega)$ are defined as usual.

Let c, d be two constants satisfying

$$4d^3 - g_2 d - g_3 = 0, \quad 4c^4 = 12d^2 - g_2. \tag{4.3}$$

Then $c \neq 0$ and we set $f = 12dc^{-2}$. The change of variables

$$(x, y) \mapsto (c^2 x + d, c^3 y)$$

on the affine equation of $\mathscr{E}$ gives an elliptic curve $\mathscr{E}_1$: $y^2 = 4x^3 + fx^2 + 4x$, and there is an isomorphism

$$\mathbf{C}/\Omega \xrightarrow{\sim} \mathscr{E}_1 \tag{4.4}$$

given by

$$z \mapsto \begin{cases} (c^{-2}(\mathscr{P}(z) - d) : c^{-3}\mathscr{P}'(z) : 1), & z \notin \Omega, \\ (0:1:0), & z \in \Omega. \end{cases}$$

The addition formula on the elliptic curve $\mathscr{E}_1$ (cf. [5]), shows that there is a non-zero point Q of order 4 in $\mathscr{E}_1$ such that

$$x(Q) = 1, \quad x(2[Q]) = 0. \tag{4.5}$$

Moreover, for any point P in $\mathscr{E}_1$, $P \neq 0, 2[Q]$,

$$\begin{aligned} x(P + 2[Q]) &= (x(P))^{-1}, \\ y(P + 2[Q]) &= -y(P)(x(P))^{-2}. \end{aligned} \tag{4.6}$$

We let $P \mapsto P + 2[Q]$ on $\mathscr{E}_1$. This induces a change of variables

$$(x, y) \mapsto (x^{-1}, -yx^{-2}).$$

Therefore, we obtain an isomorphism

$$\mathbf{C}/\Omega \xrightarrow{\sim} \mathscr{E}(f) \tag{4.7}$$

given by

$$z \mapsto \begin{cases} \left(c^2(\mathscr{P}(z)-d)^{-1} : -c\mathscr{P}'(z)(\mathscr{P}(z)-d)^{-2} : 1\right), & \mathscr{P}(z) \neq d, \\ (0:1:0), & \mathscr{P}(z) = d, \end{cases}$$

where $\mathscr{E}(f)$: $y^2 = 4x^3 + fx^2 + 4x$ is an elliptic curve with the identity of the group law at the origin $\mathbf{0} = (0:0:1)$.

Let ψ be a primitive 4-division point of $\mathbf{C}/\Omega$ that corresponds to Q in $\mathscr{E}_1$. Then from (4.4) and (4.5) we obtain

$$d = \mathscr{P}(2\psi), \quad c^2 = \mathscr{P}(\psi) - \mathscr{P}(2\psi). \tag{4.8}$$

Conversely, let ψ be any primitive 4-division point of $\mathbf{C}/\Omega$. We set c and d to be constants given by (4.8), then c and d satisfy (4.3).

Let us now fix a primitive 4-division point ψ of $\mathbf{C}/\Omega$. Let c and d be given by (4.8). We set a complex number $\ell_\psi = f$. We define the Fueter elliptic functions T_ψ, $T_{1,\psi}$ by

$$T_\psi(z) = \frac{\mathscr{P}(\psi) - \mathscr{P}(2\psi)}{\mathscr{P}(z) - \mathscr{P}(2\psi)}, \tag{4.9}$$

$$T_{1,\psi} = (\mathscr{P}(\psi) - \mathscr{P}(2\psi))^{-1/2} T_\psi'(z).$$

Fueter first defined these functions in [3].

Let $\mathscr{E}_\psi : y^2 = 4x^3 + \ell_\psi x^2 + 4x$ be an elliptic curve with identity of the group law at the origin $\mathbf{0} = (0:0:1)$. From (4.7) and (4.8) we obtain an isomorphism called the Fueter model,

$$\xi: \mathbf{C}/\Omega \tilde{\to} \mathscr{E}_\psi, \tag{4.10}$$

given by

$$\xi(z) = \begin{cases} \left(T_\psi(z) : T_{1,\psi}(z) : 1\right), & z \neq 2\psi, \\ (0:1:0), & z = 2\psi. \end{cases}$$

We also note the j-invariant,

$$j(\mathscr{E}_\psi) = \frac{\left(\Delta(\mathscr{E}_\psi) + 16\right)^3}{\Delta(\mathscr{E}_\psi)}$$

where $\Delta(\mathscr{E}_\psi) = \ell_\psi^2 - 2^6$. Moreover, the discriminant is $4\Delta(\xi_\psi)$. In the sequel we shall write $\ell = \ell_\psi$, $T = T_\psi$ etc. whenever ψ is clear from the context. We

now fix ψ. We set

$$D(z) = \frac{T(z)}{T_1(z)}.$$

We note the following properties of Fueter functions.

First, from (4.6) we obtain

(4.11) (inversion formula) $T(z)T(z + 2\psi) = 1$.

Second, we note from [1, Chapter IV] that

(4.12) (addition formula)

$$T(u + v) = \frac{\left[D^{-1}(u) + D^{-1}(v)\right]^2 T(u)T(v)}{4\left[1 - T(u)T(v)\right]^2}$$

and

(4.13) (difference formula)

$$\left[T(u) - T(v)\right]^2\left[T(u + v) - T(u - v)\right] = T(u + v)T(u - v)T_1(u)T_1(v).$$

From now on we shall take $\Omega = \mathcal{O}_K$. Then $\mathscr{E}_\psi$ has complex multiplication by $\mathcal{O}_K$. From [1] we know that $\mathscr{l}$ is an algebraic integer. Since 2 splits in $K/\mathbf{Q}$, there is a primitive 4-division point ψ on $\mathbf{C}/\mathcal{O}_K$ such that 2ψ has annihilator $2\mathcal{O}_K$. We shall take this particular 4-division point ψ in defining $\mathscr{E}_\psi$, $\mathscr{l}_\psi$, T_ψ etc.. In this case from [1, Chapter IX] we know that $\mathscr{l}^2 - 2^6$ is a unit in $K(4)$, the K ray classfield mod $4\mathcal{O}_K$ and $K(\mathscr{l}) = K(4)$.

We next note the following result on the singular values of T and T_1 (cf. [1, Chapter IX]).

PROPOSITION (4.14). *Let β be a primitive $\mathfrak{p}^s$-division point of $\mathbf{C}/\Omega$, where s is a positive integer. Then*:

(i) $T(\beta) \in \mathcal{O}_{K(4\mathfrak{p}^s)}$.

(ii) $T_1(\beta) \in K(8\mathfrak{p}^s)$.

(iii) $\mathcal{O}_{K(4\mathfrak{p}^s)} = \mathcal{O}_{K(4)}[T(\beta + \psi)]$. *Moreover, $T(\beta + \psi)$ is a unit in $K(4\mathfrak{p}^s)$.*

(iv) $T_1(\beta + \psi)$ *is a unit in* $\overline{\mathbf{Q}}$.

Remark (4.15). For (4.14) (iv) we need the fact that $\mathscr{l}^2 - 2^6$ is a unit.

5. The resolvent element

We keep the earlier notation. From now on we shall also assume that $\mathfrak{p}$ is inert in $K/\mathbf{Q}$, so that we may take $\lambda = p$. The group of p^m-division points of

$\mathbf{C}/\Omega$ is a rank one free E-module. We again write the E-action on this group exponentially. Let us denote by σ_1, σ_2 the non-zero 2-division points of $\mathbf{C}/\Omega$ distinct from 2ψ.

We define a group homomorphism Ψ given by the composite

$$E^+ \xrightarrow{\mathrm{Tr}_{K/\mathbf{Q}}} (\mathbf{Z}/p^m\mathbf{Z})^+ \xrightarrow{\exp} \mathbf{C}^\times, \tag{5.1}$$

where $\exp(k \bmod p^m) = e^{2\pi i(k/p^m)}$ for $k \in \mathbf{Z}$.

Abel's resolvent function R_μ for $\mu \in E$ is defined by

$$R_\mu(z) = \sum_{e \in E} D(z + \alpha^e)\Psi(2\mu e) \quad \text{for } z \in \mathbf{C}. \tag{5.2}$$

We set $\Lambda = p^{-m}\Omega$ and view ψ (respectively, σ_1, σ_2) as a 4-division point (respectively, 2-division points) of $\mathbf{C}/\Lambda$. There is an elliptic analogue of the Gauss sum conductor formula (cf. [1, Chapter VI]):

PROPOSITION (5.3). *Let* $\mu \in E$.

(i) *If* $\mu = 0$, *then* $R_0(z) = p^m D(p^m z)$.

(ii) *If* $\mu \neq 0$, *then*

$$R_\mu(z)R_{-\mu}(z) = p^{2m}D^2(p^m z)\prod_{k=1}^{2}\frac{\mathscr{P}_\Lambda(z + 2k\psi) - \mathscr{P}_\Lambda(\theta)}{\mathscr{P}_\Lambda(\sigma_k) - \mathscr{P}_\Lambda(\theta)}$$

where θ *is a non-zero* p^m*-division point of* $\mathbf{C}/\Lambda$ *and depends on* μ.

Let γ be an E-generator of Γ.

DEFINITION (5.4). We define the resolvent element ρ associated with α and γ by

$$\rho = p^{-m}\sum_{e \in E}\frac{D(\alpha^e + \psi)}{D(p^m\psi)}\gamma^{[e]}.$$

We shall call the element $\rho\bar{\rho}$ the conductor element (associated with α and γ).

We note the following instance of Shimura's reciprocity law (cf. [10]).

PROPOSITION (5.5). *Let* $(-, K)$ *denote the Artin map of the global class field theory. Let* β_1, β_2 *be points of finite order of* $\mathbf{C}/\Omega$ *which are not 2-division points. Then for a unit idele* $u \in K$ *with* $u \equiv 1 \bmod 4\mathcal{O}_k$,

$$\left[\frac{D(\beta_1)}{D(\beta_2)}\right]^{(u^{-1}, K)} = \frac{D(u \cdot \beta_1)}{D(u \cdot \beta_2)}$$

with the natural action of unit ideles of K *on points of finite order of* $\mathbf{C}/\Omega$.

COROLLARY (5.6). *With the above notation, for each* $e \in E$,

$$\frac{D(\alpha^e)}{D(\psi)}, \frac{D(\alpha^e + \psi)}{D(p^m\psi)} \in K(4\mathfrak{p}^m).$$

From (4.14) we deduce that $D(\alpha^e + \psi)$ is a unit in $\overline{\mathbf{Q}}$ for each $e \in E$. Moreover, since

$$D^2(p^m\psi) = D^2(\psi) = (\ell + 8)^{-1} \in \mathcal{O}_{K(4)}^{\times},$$

in view of the above corollary we obtain:

LEMMA (5.7). *The resolvent element* ρ *is such that* $p^m\rho \in \mathcal{O}_L\Gamma$.

We shall now define an irreducible character of the abelian group Γ for each $\mu \in E$. Let $\mu \in E$. We define a group homomorphism

$$\chi_\mu \colon \Gamma \to \mathbf{C}^{\times} \tag{5.8}$$

by

$$\chi_\mu(\gamma^{[e]}) = \Psi(2\mu e) \quad \text{for } e \in E.$$

Since $K_{\mathfrak{p}}/\mathbf{Q}_p$ is unramified, it follows that the irreducible characters of Γ are precisely χ_μ, $\mu \in E$. Next, we note that for any $x \in \overline{\mathbf{Q}}\Gamma$, we have

$$x = \sum_{\mu \in E} \chi_\mu(x) e_{\chi_\mu} \tag{5.9}$$

where e_{χ_μ} is the idempotent associated to χ_μ given by

$$e_{\chi_\mu} = p^{-2m} \sum_{\delta \in \Gamma} \chi_\mu(\delta^{-1})\delta.$$

By class field theory, L is a splitting field for Γ, i.e.,

$$L\Gamma = \sum_{\mu \in E} L \cdot e_{\chi_\mu}.$$

We now observe that

$$\chi_\mu(\rho) = p^{-m} \frac{R_\mu(\psi)}{D(p^m\psi)}, \quad \chi_\mu(\bar{\rho}) = p^{-m} \frac{R_{-\mu}(\psi)}{D(p^m\psi)}. \tag{5.10}$$

Therefore, from (5.3) we deduce

$$\chi_\mu(\rho\bar{\rho}) = \begin{cases} \prod_{k=1}^{2} \dfrac{\mathscr{P}_\Lambda(\psi + 2k\psi) - \mathscr{P}_\Lambda(\theta)}{\mathscr{P}_\Lambda(\sigma_k) - \mathscr{P}_\Lambda(\theta)} & \text{if } \mu \neq 0 \\ 1 & \text{if } \mu = 0 \end{cases} \tag{5.11}$$

where θ is a non-zero p^m-division point of $\mathbf{C}/\Omega$ which depends on μ.

In §6, using q-expansions, we shall show that

$$a_\mu = \frac{1}{4} \prod_{k=1}^{2} \frac{\mathscr{P}_\Lambda(\psi + 2k\psi) - \mathscr{P}_\Lambda(\theta)}{\mathscr{P}_\Lambda(\sigma_k) - \mathscr{P}_\Lambda(\theta)} \quad \text{is a unit in } \overline{\mathbf{Q}}. \tag{5.12}$$

This implies that

$$\rho\bar{\rho} = e_{\chi_0} + 4 \sum_{\mu \in E \setminus 0} a_\mu e_{\chi_\mu} \tag{5.13}$$

where a_μ is a unit in L.

Let $\mathscr{M}$ be the unique maximal $\mathcal{O}_L$-order in $L\Gamma$. Then

$$\mathscr{M} = \sum_{\mu \in E} \mathcal{O}_L \cdot e_{\chi_\mu}. \tag{5.14}$$

PROPOSITION (5.15). *For the maximal order $\mathscr{M}$ in $L\Gamma$, we have*

$$(4, p^{-m}\Sigma)\mathscr{M} = \rho\bar{\rho}\mathscr{M}.$$

Proof. From (5.13) and (5.14) we see that

$$\rho\bar{\rho}\mathscr{M} = \mathcal{O}_L \cdot e_{\chi_0} + 4 \sum_{\mu \in E \setminus 0} \mathcal{O}_L \cdot e_{\chi_\mu}.$$

On the other hand,

$$(4, p^{-m}\Sigma)\mathscr{M} = (4\mathcal{O}_L + p^m\mathcal{O}_L) \cdot e_{\chi_0} + 4 \sum_{\mu \in E \setminus 0} \mathcal{O}_L \cdot e_{\chi_\mu}$$

and $4\mathcal{O}_L + p^m\mathcal{O}_L = \mathcal{O}_L$.

For the next proposition let $J_\wp$ denote the localization (not completion) of an ideal J of $\mathscr{A}$ at prime $\wp$ of $\mathcal{O}_L$.

PROPOSITION (5.16). *If the conductor element $\rho\bar{\rho}$ lies in $\mathscr{A}$ then $I_4 = \rho\bar{\rho}\mathscr{A}$.*

Proof. Let $\rho\bar{\rho} \in \mathscr{A}$. Since I_4, $\rho\bar{\rho}\mathscr{A}$ are both ideals of $\mathscr{A}$ it suffices to show equality locally.

Let $\mathfrak{q}$ be a prime of $\mathcal{O}_L$. If $\mathfrak{q} \nmid \mathfrak{p}$ then $\mathcal{O}_{L_\mathfrak{q}}\Gamma = \mathscr{M}_\mathfrak{q}$ so that $\mathscr{A}_\mathfrak{q} = \mathscr{M}_\mathfrak{q}$, and the equality follows from (5.15).

Now assume that $\mathfrak{q} | \mathfrak{p}$. In this case, $(I_4)_\mathfrak{q} = \mathscr{A}_\mathfrak{q}$, and from (5.15) we obtain $\mathscr{M}_\mathfrak{q} = \rho\bar{\rho}\mathscr{M}_\mathfrak{q}$. Therefore, $\rho\bar{\rho} \in \mathscr{A}_\mathfrak{q} \cap \mathscr{M}_\mathfrak{q}^\times = \mathscr{A}_\mathfrak{q}^\times$ implying that $\rho\bar{\rho}\mathscr{A}_\mathfrak{q} = \mathscr{A}_\mathfrak{q}$.

COROLLARY (5.17). *If the conductor element $\rho\bar{\rho}$ lies in $\mathscr{A}$, then I_2 is a principal $\mathscr{A}$-ideal.*

Proof. From (5.16) we see that the elliptic Swan class $[I_4]$ is trivial in the elliptic Swan subgroup $T(\mathscr{A}, \mathbf{Z})$. Thus, the order of the Swan class $[I_2]$ is either 1 or 2. By (2.2) $|T(\mathscr{A}, \mathbf{Z})|$ is odd, hence $[I_2] = 0$ in $T(\mathscr{A}, \mathbf{Z})$.

In §8 we look at the question of the conductor element $\rho\bar{\rho}$ being in the associated order $\mathscr{A}$.

6. q-expansions

Let $\mathfrak{h}$ be the upper half plane of complex numbers. We let $\mathfrak{h}^* = \mathfrak{h} \cup \mathbf{Q} \cup \{\infty\}$, the completion of $\mathfrak{h}$. Set $\Gamma = SL_2(\mathbf{Z})$. We remark that in this section only, Γ does not denote a Galois group. We view each $\gamma \in \Gamma$ as a linear fractional transformation on $\mathfrak{h}^*$ given by

$$\gamma(z) = \frac{az + b}{cz + d} \quad \text{where } \gamma = \begin{bmatrix} a & b \\ c & d \end{bmatrix}.$$

For a complex valued function f, $\gamma \in \Gamma$, $z \in \mathbf{C}$ we write

$$f|_\gamma(z) = f(\gamma(z)).$$

DEFINITION (6.1). Let Δ be subgroup of Γ of finite index. Let f be a meromorphic function on $\mathfrak{h}$. We call f a modular function for Δ if

(i) $f|_\delta = f$ for $\delta \in \Delta$, and

(ii) f is meromorphic at every cusp of Δ.

For a fixed positive integer n we set

$$\Gamma(n) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \Gamma : a \equiv d \equiv 1 \bmod n;\ b \equiv c \equiv 0 \bmod n \right\},$$

the principal congruence subgroup of level n. A meromorphic function f is a

modular function for $\Gamma(n)$ if, and only if,

(6.2) $f|_\gamma$ is meromorphic at the standard cusp ∞ for each $\gamma \in \Gamma$, and (6.1)(i) holds.

Moreover, by standard theory, f is meromorphic at the cusp ∞ if, and only if, f has a Laurent series expansion with finitely many polar terms in $q_z^{1/n}$ where $q_z = e^{2\pi i z}$. We call this Laurent series the q-expansion of f at the standard cusp ∞. In general, the q-expansion of a modular function f for $\Gamma(n)$ at a cusp s is defined to be the q-expansion of $f|_\gamma$ at ∞ where $\gamma \in \Gamma$ is such that $\gamma(s) = \infty$.

Let ζ_n be a primitive n-th root of unity in some fixed algebraic closure $\overline{\mathbf{Q}}$ of $\mathbf{Q}$. We define the ring S_n by

$$S_n = \mathbf{Z}[\zeta_n]\left(\left(q_z^{1/n}\right)\right).$$

We have the following q-expansion principle from [1, (5.5), Chapter VII].

PROPOSITION (6.3). *Let $\tau \in \mathcal{H}$ and $\Omega_\tau = \mathbf{Z}\tau + \mathbf{Z}$ be a lattice with complex multiplication. Let f be a modular function for $\Gamma(n)$ which is finite on $\mathcal{H}$.*

(i) *If the q-expansions of f at all cusps of $\Gamma(n)$ lie in S_n, then $f(\tau)$ is an algebraic integer.*

(ii) *Moreover, if the q-expansions of f at all cusps lie in $S_n^\times$ and f is non-zero on $\mathcal{H}$, then $f(\tau)$ is a unit in $\overline{\mathbf{Q}}$.*

For $f, g \in S_n$, we write $f \sim g$ whenever $f = gh$, $h \in S_n^\times$. Moreover, for two modular functions f, g for $\Gamma(n)$, we write $f \approx g$ whenever their q-expansions at each cusp of $\Gamma(n)$ are $\sim$ -equivalent. We note that both $\sim$ and $\approx$ are equivalence relations on S_n and modular functions for $\Gamma(n)$ respectively. Furthermore, if $f \approx g$ for $\Gamma(n)$, then $f \approx g$ for $\Gamma(nk)$, $k > 0$.

We fix some notation. Let $\mathbf{x} \in (\mathbf{Q}/\mathbf{Z})^{(2)}$. We view $\mathbf{x}$ as $\mathbf{x} = (x_1, x_2)$ where $x_i \in [0, 1)$ for $i = 1, 2$. For non-zero $n\mathbf{Z}$-division points $\mathbf{a}_i \in (\mathbf{Q}/\mathbf{Z})^{(2)}$, with $1 \le i \le 4$ and $\mathbf{a}_1 \neq \pm\mathbf{a}_2$, $\mathbf{a}_3 \neq \pm\mathbf{a}_4$, we define a modular function for $\Gamma(n)$ which is non-zero and finite on $\mathcal{H}$ by

$$F_{\mathbf{a}_1,\mathbf{a}_2,\mathbf{a}_3,\mathbf{a}_4}(z) = \frac{\mathcal{P}_z\left(\mathbf{a}_1\begin{bmatrix}\omega_1\\ \omega_2\end{bmatrix}\right) - \mathcal{P}_z\left(\mathbf{a}_3\begin{bmatrix}\omega_1\\ \omega_2\end{bmatrix}\right)}{\mathcal{P}_z\left(\mathbf{a}_2\begin{bmatrix}\omega_1\\ \omega_2\end{bmatrix}\right) - \mathcal{P}_z\left(\mathbf{a}_4\begin{bmatrix}\omega_1\\ \omega_2\end{bmatrix}\right)}, \tag{6.4}$$

where $z = \omega_1/\omega_2 \in \mathcal{H}$, $\mathcal{P}_z = \mathcal{P}_{\Omega_z}$ and $\Omega_z = \mathbf{Z}\omega_1 + \mathbf{Z}\omega_2$ is a lattice in $\mathbf{C}$. Often the function $F(z)$ is called a Weierstrass modular unit.

Next, let $\mathbf{d} \in (\mathbf{Q}/\mathbf{Z})^{(2)}$ be a primitive $4\mathbf{Z}$-division point. We set

$$t_{\mathbf{d}}(z) = \frac{12\mathscr{P}_z\left(2\mathbf{d}\begin{bmatrix}\omega_1\\ \omega_2\end{bmatrix}\right)}{\mathscr{P}_z\left(\mathbf{d}\begin{bmatrix}\omega_1\\ \omega_2\end{bmatrix}\right) - \mathscr{P}_z\left(2\mathbf{d}\begin{bmatrix}\omega_1\\ \omega_2\end{bmatrix}\right)}. \tag{6.5}$$

Then we define

$$\phi_{\mathbf{d}}(z) = t_{\mathbf{d}}^2(z) - 2^6. \tag{6.6}$$

From (1.2), (1.7) of Chapter VIII of [1] we obtain:

PROPOSITION (6.7). *Let* $\mathbf{d}$ *be a primitive* $4\mathbf{Z}$*-division point in* $(\mathbf{Q}/\mathbf{Z})^{(2)}$. *Then* $\phi_{\mathbf{d}}$ *is a modular function for* $\Gamma(4)$. *Moreover, the q-expansion of* $\phi_{\mathbf{d}}$ *at* ∞ *is* $\sim$ *-equivalent to*

$$\begin{array}{ll} 1 & \text{if } 2d_1 \neq 0, \\ 2^{12} & \text{if } 2d_1 = 0. \end{array}$$

Now we note the following result on the q-expansion of the Weierstrass $\mathscr{P}$-function (cf. (3.2), Chapter VIII [1]).

PROPOSITION (6.8). *Let* $\mathbf{a}$ *be a primitive* $n\mathbf{Z}$*-division point in* $(\mathbf{Q}/\mathbf{Z})^{(2)}$. *We set* $\zeta_n = e^{2\pi i/n}$. *Then in the q-expansion of* $(2\pi i)^{-2}\mathscr{P}_z(\mathbf{a}) - 1/12$, *the leading term is*

$$\begin{array}{ll} \zeta_n^{na_2}(1-\zeta_n^{na_2})^{-2} & \text{if } a_1 = 0, \\ \zeta_n^{na_2} q^{a_1} & \text{if } 0 < a_1 < 1/2, \\ \zeta_n^{-na_2} q^{1-a_1} & \text{if } 1/2 < a_1 < 1, \\ (\zeta_n^{-na_2} + \zeta_n^{na_2}) q^{1/2} & \text{if } a_1 = 1/2 \text{ and } n \neq 4, \\ -6q & \text{if } a_1 = 1/2 \text{ and } n = 4. \end{array}$$

Moreover, all subsequent coefficients in this q-expansion lie in $\mathbf{Z}[\zeta_n]$.

Let $m > 0$ be a fixed integer. Let $\mathbf{b}$ be a non-zero $p^m\mathbf{Z}$-division point of $(\mathbf{Q}/\mathbf{Z})^{(2)}$. Let $\mathbf{d}$ be a primitive $4\mathbf{Z}$-division point of $(\mathbf{Q}/\mathbf{Z})^{(2)}$. Let $\mathbf{c}(1), \mathbf{c}(2)$ be non-zero $2\mathbf{Z}$-division points of $(\mathbf{Q}/\mathbf{Z})^{(2)}$ distinct from $2\mathbf{d}$. We define a modular function $E_{\mathbf{d},\mathbf{b}}$ for $\Gamma(4p^m)$ as follows:

$$E_{\mathbf{d},\mathbf{b}} = \prod_{k=1}^{2} F_{\mathbf{d}+2k\mathbf{d},\mathbf{b},\mathbf{c}(k),\mathbf{b}} \prod_{k=1}^{2} F_{\mathbf{d}+\mathbf{c}(k),\mathbf{b},\mathbf{c}(k),\mathbf{b}}. \tag{6.9}$$

We now use (6.8) to show the following.

PROPOSITION (6.10). *Let* $\mathbf{b}$ *be a non-zero* $p^m\mathbf{Z}$*-division point of* $(\mathbf{Q}/\mathbf{Z})^{(2)}$ *and let* $\mathbf{d}$ *be a primitive* $4\mathbf{Z}$*-division point of* $(\mathbf{Q}/\mathbf{Z})^{(2)}$. *Then* $E_{\mathbf{d},\mathbf{b}}^2 \approx 2^8\phi_{\mathbf{d}}^{-1}$.

Proof. By abuse of notation, we shall write f for the q-expansion of a modular function f at a given cusp. We must show that $E_{\mathbf{d},\mathbf{b}}^2 \sim 2^8\phi_{\mathbf{d}}^{-1}$ at each cusp. For $\gamma \in \Gamma$,

$$E_{\mathbf{d},\mathbf{b}}|_\gamma = E_{\mathbf{d}\gamma,\mathbf{b}\gamma}, \quad \phi_{\mathbf{d}}|_\gamma = \phi_{\mathbf{d}\gamma}.$$

Moreover, $\mathbf{d}\gamma$ is a primitive $4\mathbf{Z}$-division point and $\mathbf{b}\gamma$ is a non-zero $p^m\mathbf{Z}$-division point in $(\mathbf{Q}/\mathbf{Z})^{(2)}$. Therefore, in view of (6.2), it suffices to show that for all choices of primitive $4\mathbf{Z}$-division points $\mathbf{d}'$ and non-zero $p^m\mathbf{Z}$-division points $\mathbf{b}'$ in $(\mathbf{Q}/\mathbf{Z})^{(2)}$,

$$E_{\mathbf{d}',\mathbf{b}'} \sim 2^8\phi_{\mathbf{d}'}^{-1} \quad \text{at the standard cusp } \infty. \tag{6.11}$$

For convenience we write $\mathbf{d}$ for $\mathbf{d}'$ and $\mathbf{b}$ for $\mathbf{b}'$. From now on a q-expansion means a q-expansion at the cusp ∞. From (6.8) we find the leading coefficient in the q-expansion of $(2\pi i)^{-2}(\mathscr{P}_z(\mathbf{d}) - \mathscr{P}_z(\mathbf{b}))$ to be

$$\begin{cases} -\frac{1}{2} - \eta(1-\eta)^{-2} & \text{if } b_1 = 0,\ d_1 = 0, \\ -\frac{1}{2} & \text{if } b_1 \neq 0,\ d_1 = 0, \\ -\eta(1-\eta)^{-2} & \text{if } b_1 = 0,\ d_1 \neq 0, \\ \text{root of unity in } \mathbf{Z}[i,\eta] & \text{if } b_1 \neq 0,\ d_1 \neq 0, \end{cases} \tag{6.12}$$

where $\eta \neq 1$ is a p^m-th root of unity. Furthermore, all subsequent coefficients are in $\mathbf{Z}[i,\eta]$.

Similarly the leading coefficient in the q-expansion of $(2\pi i)^{-2}(\mathscr{P}_z(\mathbf{f}) - \mathscr{P}_z(\mathbf{b}))$ for a non-zero $2\mathbf{Z}$-division point $\mathbf{f}$ in $(\mathbf{Q}/\mathbf{Z})^{(2)}$ (cf. (3.6), Chapter VIII [1]) is

$$\begin{cases} -\frac{1}{4} - \eta(1-\eta)^{-2} & \text{if } b_1 = 0,\ f_1 = 0, \\ -\frac{1}{4} & \text{if } b_1 \neq 0,\ f_1 = 0, \\ -\eta(1-\eta)^{-2} & \text{if } b_1 = 0,\ f_1 \neq 0, \\ \text{root of unity in } \mathbf{Z}[\eta] & \text{if } b_1 \neq 0,\ f_1 \neq 0. \end{cases} \tag{6.13}$$

We also note that all other coefficients are in $\mathbf{Z}[\eta]$.

From (6.12) and (6.13) we obtain

$$\prod_{k=1}^{2} F_{\mathbf{d}+2k\mathbf{d},\mathbf{b},\mathbf{c}(k),\mathbf{b}} \sim \begin{cases} 4 & \text{if } 2d_1 \neq 0, \\ \frac{1}{4} & \text{if } d_1 = 0, \\ 1 & \text{if } d_1 = \frac{1}{2}. \end{cases} \tag{6.14}$$

Now let $\mathbf{e}$ be a non-zero $2\mathbf{Z}$-division point in $(\mathbf{Q}/\mathbf{Z})^{(2)}$ distinct from $2\mathbf{d}$. We write $\mathbf{h} = \mathbf{d} + \mathbf{e}$. Then $2h_1 \neq 0$ if, and only if, $2d_1 \neq 0$. Moreover, $h_1 = 0$ if, and only if, $d_1 = 1/2$. We also observe that the set $\{\mathbf{h}, \mathbf{h} + 2\mathbf{h}\}$ equals the set $\{\mathbf{d} + \mathbf{c}(1), \mathbf{d} + \mathbf{c}(2)\}$. Therefore, using (6.14), we see that

$$\prod_{k=1}^{2} F_{\mathbf{d}+\mathbf{c}(k),\mathbf{b},\mathbf{c}(k),\mathbf{b}} \sim \begin{cases} 4 & \text{if } 2d_1 \neq 0, \\ \frac{1}{4} & \text{if } d_1 = \frac{1}{2}, \\ 1 & \text{if } d_1 = 0. \end{cases} \tag{6.15}$$

Combining (6.14) and (6.15), we obtain

$$E_{\mathbf{d},\mathbf{b}} \sim \begin{cases} 2^4 & \text{if } 2d_1 \neq 0, \\ 2^{-2} & \text{if } 2d_1 = 0. \end{cases} \tag{6.16}$$

From (6.16) and (6.7), we immediately see that $E_{\mathbf{d},\mathbf{b}}^2 \sim 2^8 \phi_{\mathbf{d}}^{-1}$. This proves (6.11).

COROLLARY (6.17). *With the notation above, the q-expansions of*

$$2^{-12}\left(\prod_{k=1}^{2} F_{\mathbf{d}+2k\mathbf{d},\mathbf{b},\mathbf{c}(k),\mathbf{b}}\right)^6 \phi_{\mathbf{d}}^2$$

at all cusps of $\Gamma(4p^m)$ *lie in* S_{4p^m}.

Proof. This follows from (6.14) and (6.7).

The purpose of q-expansion results (6.10) and (6.17) is to show (5.12).

THEOREM (6.18). *With the notation of* §5, *we have*

$$\prod_{k=1}^{2} \frac{\mathscr{P}_\Lambda(\psi + 2k\psi) - \mathscr{P}_\Lambda(\theta)}{\mathscr{P}_\Lambda(\sigma_k) - \mathscr{P}_\Lambda(\theta)} \in 4\bar{\mathcal{O}}^\times$$

where $\bar{\mathcal{O}}$ *is the ring of integers of* $\bar{\mathbf{Q}}$.

Proof. Let $\Omega = \mathcal{O}_K = \mathbf{Z}\omega_1 + \mathbf{Z}\omega_2$. Then $\Lambda = p^{-m}\mathcal{O}_K = \mathbf{Z}\lambda_1 + \mathbf{Z}\lambda_2$, where $\lambda_k = p^{-m}\omega_k$ for $k = 1, 2$. We make the following specialization in applying the q-expansion principle (6.3) to (6.10) and (6.17):

$$\tau = \lambda_1/\lambda_2, \quad \mathbf{d}\begin{bmatrix}\lambda_1\\ \lambda_2\end{bmatrix} = \psi, \quad \mathbf{b}\begin{bmatrix}\lambda_1\\ \lambda_2\end{bmatrix} = \theta.$$

Then

$$\mathbf{c}(k)\begin{bmatrix}\lambda_1\\ \lambda_2\end{bmatrix} = \sigma_k \quad \text{for } k = 1, 2;$$

this may require rearranging the ordering of $\{\sigma_1, \sigma_2\}$. Let $\mathbf{h} = \mathbf{d} + \mathbf{c}(1)$. Then

$$\phi_{\mathbf{h}}(\tau) = \phi_{\mathbf{d}}(\tau) = \ell^2 - 2^6. \tag{6.19}$$

We recall from §4 that since 2 splits in $K/\mathbf{Q}$, the choice of ψ implies that $\phi_{\mathbf{d}}(\tau)$ is a unit in $\overline{\mathbf{Q}}$.

Now, applying the q-expansion principle (6.3)(i) to (6.17) with 4-division points $\mathbf{d}, \mathbf{h}$, we obtain

$$\prod_{k=1}^{2} \frac{\mathscr{P}_\Lambda(\psi + 2k\psi) - \mathscr{P}_\Lambda(\theta)}{\mathscr{P}_\Lambda(\sigma_k) - \mathscr{P}_\Lambda(\theta)}, \quad \prod_{k=1}^{2} \frac{\mathscr{P}_\Lambda(\psi + \sigma_k) - \mathscr{P}_\Lambda(\theta)}{\mathscr{P}_\Lambda(\sigma_k) - \mathscr{P}_\Lambda(\theta)} \in 4\bar{\mathcal{O}}. \tag{6.20}$$

Similarly, applying the q-expansion principle (6.3)(ii) to (6.10) with the above specializations, we obtain

$$\prod_{k=1}^{2} \frac{\mathscr{P}_\Lambda(\psi + 2k\psi) - \mathscr{P}_\Lambda(\theta)}{\mathscr{P}_\Lambda(\sigma_k) - \mathscr{P}_\Lambda(\theta)} \prod_{k=1}^{2} \frac{\mathscr{P}_\Lambda(\psi + \sigma_k) - \mathscr{P}_\Lambda(\theta)}{\mathscr{P}_\Lambda(\sigma_k) - \mathscr{P}_\Lambda(\theta)} \in 16\bar{\mathcal{O}}^\times. \tag{6.21}$$

We combine (6.20) and (6.21) to get the desired result.

7. The formal group associated with the Fueter model

We keep the notation of §3 and §4. Let us consider the elliptic curve of the Fueter model (4.10):

$$\mathscr{E}_\psi\colon\ y^2 = 4x^3 + \ell x^2 + 4x \tag{7.1}$$

where the identity on $\mathscr{E}_\psi$ is taken to be the point at the origin $\mathbf{0} = (0:0:1)$. We look at $\mathscr{E}_\psi$ locally at $\mathfrak{p}$ and denote this elliptic curve by $\mathscr{E}'$. We fix an embedding of $\overline{\mathbf{Q}}$ in $\overline{\mathbf{Q}}_p$ so that it corresponds to $\mathfrak{p}$ for K. For a field $M \subseteq \overline{\mathbf{Q}}$

we write M' for its closure in $\overline{\mathbf{Q}}_p$. We observe that $K' = K(4)'$, since $\mathfrak{p}$ is completely split in $K(4)$. We also recall that $\iota \in K(4)$. Now $\mathscr{E}'$ admits complex multiplication and has good reduction modulo $\mathfrak{p}$.

We shall simply write (x, y) for a point on $\mathscr{E}'$ with projective coordinates $(x : y : 1)$. Let us denote by $\mathscr{E}_0'$ the kernel of reduction of $\mathscr{E}'$ modulo $\mathfrak{p}$. We know from [7] that there is a formal group law F on $\mathscr{E}_0'$ with the parameter

$$t = \frac{2x}{y} \tag{7.2}$$

on F associated with the point (x, y) of $\mathscr{E}_0'$. Moreover,

$$x = t^2 a(t^2), \quad y = 2ta(t^2) \tag{7.3}$$

where $a(t) \in \mathcal{O}_{K'}[[t]]$ and $a(0) = 1$. In [1] it is also shown that F is, in fact, a Lubin-Tate formal group law defined over $\mathcal{O}_{K'}$ for a uniformizing parameter $p' \in \{\pm p\}$.

Let s be a positive integer and let β be a primitive p^s-division point of $\mathbf{C}/\mathcal{O}_K$. Then:

(7.4) $(T(\beta), T_1(\beta)) \in \mathscr{E}_0'$ and the parameter $2D(\beta)$ on F associated with this point is a primitive p^s-division point of F.

We recall from (4.14) that $D(\beta) \in K(8\mathfrak{p}^s)$.

LEMMA (7.5). *If $p \equiv \pm 1 \bmod 8$ and β is a primitive p^s-division point of $\mathbf{C}/\Omega$ for a positive integer s, then $K'(D(\beta)) = K(4\mathfrak{p}^s)'$.*

Proof. We know that

$$\big(K'(D(\beta)) : K'\big) = \big(p^2 - 1\big)p^{2(s-1)} = \big(K(4\mathfrak{p}^s)' : K'\big).$$

Furthermore, $D(\beta) \in K(8\mathfrak{p}^s)' = K(4\mathfrak{p}^s)'$, since $p \equiv \pm 1 \bmod 8$.

Remark (7.6). This lemma shows that for $p \equiv \pm 1 \bmod 8$ we can use the Lubin-Tate formal group law associated with the Fueter model to describe the local Galois module structure by (3.3). Moreover, for a primitive p^m-division point α of $\mathbf{C}/\mathcal{O}_K$, $\omega = 2D(\alpha)$ is a primitive p^m-division point of F.

PROPOSITION (7.7). *Let α be a primitive p^m-division point of $\mathbf{C}/\mathcal{O}_K$. Then, there exists $b(X) \in \mathcal{O}_{K'}[[X]]$ such that*

$$\frac{D(\alpha^e + \psi)}{D(\psi)} = b\left(\frac{D(\alpha^e)}{D(\psi)}\right) \quad \text{for } e \in E.$$

Moreover, $b(0) = 1$.

Proof. Let $z \in \mathbf{C}/\Omega$ be such that $(T(z), T_1(z)) \in \mathscr{E}_0'$. We consider

$$\frac{D(z+\psi)}{D(\psi)}$$

and use the difference formula (4.13) with $u = z + \psi$ and $v = \psi$ to obtain

$$\frac{D(z+\psi)}{D(\psi)} = \frac{T(z+\psi)T(z)T_1^2(\psi)}{[T(z+\psi)-1]^2[1-T^2(z)]}. \tag{7.8}$$

Expanding $T(z+\psi)$ by the addition formula (4.12), and in view of (7.2), (7.3) writing

$$t(z) = 2D(z), \quad T(z) = t^2(z)a(t^2(z)) \tag{7.9}$$

where $a(X) \in \mathcal{O}_{K'}[[X]]$ with $a(0) = 1$, we obtain

$$\frac{D(z+\psi)}{D(\psi)} = \frac{f(t(z))}{g(t(z))} \tag{7.10}$$

where

$$f(X) = 4T_1^2(\psi)X^2a^2(X^2)[2 + T_1(\psi)X]^2[1 - X^2a(X^2)],$$

$$g(X) = \left[\{2 + T_1(\psi)X\}^2 - 4\{1 - X^2a(X^2)\}^2\right]^2[1 + X^2a(X^2)].$$

We now write

$$t' = \frac{T_1(\psi)}{2}t.$$

Then

$$t'(z) = \frac{D(z)}{D(\psi)} \quad \text{and} \quad (t')^2 = \frac{(\ell+8)}{4}t^2.$$

Since $\ell^2 - 2^6 \in \mathcal{O}_{K(4)}^{\times}$ and p is odd we see that $(\ell+8)/4 \in \mathcal{O}_{K'}^{\times}$. Therefore,

$$f(t) = 16(t')^2f_1(t'), \quad g(t) = 64(t')^2g_1(t') \tag{7.11}$$

where $f_1(X), g_1(X) \in \mathcal{O}_{K'}[[X]]$ with $f_1(0) = 4$, $g_1(0) = 1$.

Taking the inverse of the formal power series $g_1(X)$ in $\mathcal{O}_{K'}[[X]]$ and noting that $4 \in \mathcal{O}_{K'}^{\times}$, we have shown

$$\frac{D(z+\psi)}{D(\psi)} = b\left(\frac{D(z)}{D(\psi)}\right) \tag{7.12}$$

where $b(X) \in \mathcal{O}_{K'}[[X]]$ and $b(0) = 1$.

The proof is now completed on taking $z = \alpha^e$ for each $e \in E$.

8. $p \equiv \pm 1 \bmod 8$

We keep the notation of earlier sections.

THEOREM (8.1). *If $p \equiv \pm 1 \bmod 8$, then the resolvent element ρ lies in the associated order $\mathcal{A}$.*

Proof. From (5.7) it suffices to show that $\rho \in \mathcal{A}_{\mathfrak{p}}$ whenever $\mathfrak{p}$ is a prime of $\mathcal{O}_L$ such that $\mathfrak{p}|\mathfrak{P}$.

Let $\mathfrak{p}$ be a prime of $\mathcal{O}_L$ such that $\mathfrak{p}|\mathfrak{P}$. We fix an embedding of $\overline{\mathbf{Q}}$ in $\overline{\mathbf{Q}}_p$ so that it corresponds to $\mathfrak{p}_N$ over N where $\mathfrak{p}_N$ is the unique prime of $\mathcal{O}_N$ with $\mathfrak{p}_N \cap \mathcal{O}_L = \mathfrak{p}$. We see that this embedding corresponds to $\mathfrak{p}$ over L and $\mathfrak{P}$ over K. With the notation of §7 we have that $N' = N_{\mathfrak{p}_N}$, $L' = L_{\mathfrak{p}}$ and $K' = K_{\mathfrak{P}}$. Since $p \equiv \pm 1 \bmod 8$ we note from (7.6) that the local Galois module structure of N'/L' can be described by the Lubin-Tate formal group law associated with the Fueter model (4.10).

Let α be the primitive p^m-division point of $\mathbf{C}/\mathcal{O}_K$ and let γ be the E-generator of Γ for which the resolvent element ρ is defined in (5.4). We write

$$\omega = 2D(\alpha). \tag{8.2}$$

Then $\omega^{[e]} = 2D(\alpha^e)$ for $e \in E$ and ω is a primitive p^m-division point in F. From (3.3) and (3.5) we obtain

$$\mathcal{A}_{N'/L'} = O_{L'} \cdot 1_\Gamma + \sum_{i=0}^{p^{2m}-2} \mathcal{O}_{L'} \cdot \sigma_i \tag{8.3}$$

where

$$\sigma_i = p^{-m} \sum_{e \in E} \left(\omega^{[e]}\right)^i \left(\gamma^{[e]} - 1_\Gamma\right) \in \mathcal{A}_{N'/L'} \quad \text{for } i \geq 0.$$

Now

$$p^{-m}\sum_{e\in E}\frac{D(\alpha^e+\psi)}{D(p^m\psi)}=p^{-m}\frac{R_0(\psi)}{D(p^m\psi)}=1.$$

Therefore,

$$\rho-1_\Gamma=p^{-m}\sum_{e\in E}\frac{D(\alpha^e+\psi)}{D(p^m\psi)}(\gamma^{[e]}-1_\Gamma).$$

Since D is an odd function and $p^m\psi=\varepsilon(p^m)\psi$ in $\mathbf{C}/\Omega$ where $\varepsilon(p^m)=\pm 1$, we obtain

$$\rho-1_\Gamma=\varepsilon(p^m)p^{-m}\sum_{e\in E}\frac{D(\alpha^e+\psi)}{D(\psi)}(\gamma^{[e]}-1_\Gamma).$$

Using (7.7), we see that

$$\rho-1_\Gamma=\varepsilon(p^m)p^{-m}\sum_{e\in E}b\left(\frac{\omega^{[e]}}{2D(\psi)}\right)(\gamma^{[e]}-1_\Gamma) \tag{8.4}$$

where $b(X)\in\mathcal{O}_{K'}[[X]]$ and $b(0)=1$.

Since $D(\alpha)/D(\psi)\in K(4\sqrt{p^m})\subseteq L$, $D(\alpha)\in L'$ and $D^2(\psi)=(\zeta+8)^{-1}\in\mathcal{O}_{K(4)}^\times$ we see that $2D(\psi)\in\mathcal{O}_{L'}^\times$. Thus, we may rewrite (8.4) as

$$\rho-1_\Gamma=\varepsilon(p^m)\sum_{e\in E}p^{-m}\left(\sum_{i\geq 0}s_i(\omega^{[e]})^i\right)(\gamma^{[e]}-1_\Gamma) \tag{8.5}$$

where $s_i\in\mathcal{O}_{L'}$ for $i\geq 0$. Rearranging terms, we obtain

$$\rho-1_\Gamma=\varepsilon(p^m)\sum_{i\geq 0}s_i\sigma_i \tag{8.6}$$

where $s_i\in\mathcal{O}_{L'}$ for $i\geq 0$. Since $\sigma_i\in\mathscr{A}_\varphi$ for $i\geq 0$ and $\lim_{n\to\infty}\sigma_n=0$ in $L\Gamma$, we see that $\rho\in\mathscr{A}_\varphi$.

Finally, we obtain the main result (1.2).

Proof of (1.2). In view of our previous results, in particular, (5.17) it suffices to show that $\rho\bar{\rho}\in\mathscr{A}$. In (8.1) we proved that $\rho\in\mathscr{A}$ for $p\equiv\pm 1 \bmod 8$. From (3.6) we deduce that in that case $\bar{\rho}\in\mathscr{A}$. This completes the proof of (1.2).

References

1. Ph. Cassou-Noguès and M.J. Taylor, *Elliptic functions and rings of integers*, Birkhäuser, Boston, 1987.
2. C.W. Curtis and Irving Reiner, *Methods of representation theory with applications to finite groups and orders*, Vol. I, Wiley, New York, 1981.
3. R. Fueter, *Vorlesungen über die singulären Moduln und die komplexe Multiplikation der elliptischen Funktionen*, 1 und 2, Teubner, Leipzig, 1924.
4. H.W. Leopoldt, Über die Hauptordnung der ganzen Elemente eines abelschen Zahlkörpers, J. Reine Angew. Math., vol. 209 (1962), pp. 54–71.
5. J. Silverman, *The arithmetic of elliptic curves*, Graduate Text, no. 106, Springer-Verlag, New York, 1985.
6. R.G. Swan, *Periodic resolutions for finite groups*, Ann. of Math., vol. 72 (1960), pp. 267–291.
7. J. Tate, *Algorithm for determining the type of a singular fiber in an elliptic pencil*, Lecture Notes in Mathematics, no. 476, Springer-Verlag, New York, 1975, pp. 33–52.
8. M.J. Taylor, *Class groups of group rings*, London Math. Soc. Lecture Note Series, no. 91, Cambridge University Press, Cambridge, 1984.
9. _____, *Relative Galois module structure of rings of integers and elliptic functions II*, Ann. of Math., vol. 121 (1985), pp. 519–535.
10. _____, *Relative Galois module structure of rings of integers and elliptic functions III*, Proc. London Math. Soc. (3), vol. 51 (1985), pp. 415–431.
11. _____, *Formal groups and the Galois module structure of local rings of integers*, J. Reine Angew. Math., vol. 358 (1985), pp. 97–103.
12. _____, *Hopf structure and the Kummer theory of formal groups*, J. Reine Angew. Math., vol. 375/376 (1987), pp. 1–11.
13. S.V. Ullom, *Nontrivial lower bounds for class groups of integral group rings*, Illinois J. Math., vol. 20 (1976), pp. 361–371.

University of Illinois
Urbana, Illinois