Elliptic curves and module structure over Hopf orders

and

The conjecture of Chinburg-Stark for abelian extensions of a quadratic imaginary field

Werner Bley
Institut für Mathematik
Universität Augsburg
86135 Augsburg
Germany
email: bley@math.uni-augsburg.de

December 22, 1997

Preface

This habilitation thesis consists of two parts, both originating in the field of Galois module structure.

The first part is concerned with the study of the module structure of rings of integers. My investigations are on the one hand based on methods and results of M. J. Taylor, Ph. Cassou-Noguès and R. Schertz concerning classical Galois module structure of rings of integers over associated orders in the spirit of H. W. Leopoldt, and on the other hand on a more recent approach of M. J. Taylor dealing with the module structure of so-called Kummer orders over explicitly given Hopf orders. It was one of my main motivations to illuminate the relation between both approaches.

The second part is in the first place a contribution to the theory of Artin L-series. More precisely, we consider a strong version of Stark's conjecture, due to T. Chinburg, for abelian extensions of a quadratic imaginary number field. The relation to Galois module theory stems from the fact that the validity of this conjecture provides important information about an invariant attached to the Galois structure of the group of S-units, the so-called third Chinburg invariant.

There is still another common feature which connects both parts: the source of the main results is always the analytic theory of elliptic units. Only the interplay between algebraic and analytic methods leads to nice theories with valuable results.

The first part is not written in the style of a research paper. On the contrary, the subject is introduced in a very detailed and essentially self-contained way. For many results, although already in the literature, I give complete proofs; hopefully always with appropriate references. The second part is still detailed, but not nearly as self-contained as the first.

I gratefully acknowledge the help of many people in producing this habilitation thesis. First I wish to thank J. Ritter and R. Schertz for their constant support during the last seven years. I am also grateful to J. Ritter and A. Weiss for suggesting to me to work on the conjecture of Chinburg-Stark. Special thanks go to R. Boltje for many fruitful discussions and also for his consent to include a joint paper in the first part.

Contents

Part I

Elliptic curves and module structure over Hopf orders

1 Introduction

In [T2], M. J. Taylor initiated the study of the Galois module structure of certain Kummer orders associated to torsion points on an abelian variety. In [BB] we axiomatized the situation considered by Taylor and applied our results to investigate the module structure of the full ring of integers of certain algebras obtained by dividing torsion points with respect to the group law of a relative Lubin-Tate formal group.

Besides the examples arising from Lubin-Tate theory, there is a variety of natural examples for the general situation considered in [BB]. These notes are intended to discuss some of them, in particular we will deal with examples associated to elliptic curves.

This paper is also an attempt to understand the connections between earlier work of M. J. Taylor and Ph. Cassou-Noguès [CT], R. Schertz [Sch2] and others concerning the Galois module structure of rings of integers over their associated orders for certain wildly ramified relative ray class field extensions of a quadratic imaginary number field, and the more recent work of M. J. Taylor and A. Srivastav [T2], [ST] on the module structure of Kummer orders over certain explicitly given Hopf orders.

We assume the following situation:

- $\mathcal{O}$ is a Dedekind domain of characteristic 0, K its field of fractions, $\bar{K}$ an algebraic closure of K, and $\Omega := \mathrm{Gal}(\bar{K}/K)$ the absolute Galois group of K.
- G is a finite group on which Ω acts from the left.
- Γ is a finite set on which G and Ω act from the left such that G acts simply transitively (thus $|G| = |\Gamma|$) and ${}^{\omega}({}^{g}\gamma) = {}^{({}^{\omega}g)}({}^{\omega}\gamma)$ for all $\omega \in \Omega$, $g \in G$, and $\gamma \in \Gamma$ (the last condition just means that the semidirect product $G \rtimes \Omega$ acts on Γ).

We always write the action of $\omega \in \Omega$ on G and Γ exponentially from the left (as in ${}^{\omega}g$ and ${}^{\omega}\gamma$ for $g \in G$ and $\gamma \in \Gamma$) and its action on $\bar{K}$ as $\omega(x)$ for $x \in \bar{K}$. For any intermediate field $K \subseteq L \subseteq \bar{K}$, we set $\Omega_L := \mathrm{Gal}(\bar{K}/L) \leqslant \Omega$, and denote by $\mathcal{O}_L$ the integral closure of $\mathcal{O}$ in L.

The motivation for considering this general algebraic context stems from the observation that many natural examples, which are already discussed in the literature, fit into this framework.

Examples 1.1 For any field of characteristic 0 let μ_n, $n \in \mathbb{N}$, denote the multiplicative group of n-th roots of unity in its algebraic closure.

(a) Let $r, m \in \mathbb{N}$ and set $K := \mathbb{Q}(\mu_r)$, $G := \mu_m$. Fix a primitive r-th root of unity $\beta \in \mu_r$, and set $\Gamma := \{x \in \bar{K} \mid x^m = \beta\}$. Then $\Gamma \subseteq \mu_{r+m}$ and G acts on Γ by multiplication. This very explicit example will be discussed in detail in Section 3. It will serve as motivation and guideline for the more involved applications to elliptic curves.

(b) More generally, let K be a number field, let $m \in \mathbb{N}$ and $G := \mu_m$. For $\beta \in K^\times$ set $\Gamma := \{x \in \bar{K} \mid x^m = \beta\}$. Then G acts on Γ by multiplication.

(c) For arbitrary K let L/K be a finite Galois extension with Galois group G, and let Ω act on G by conjugation. Moreover, let $\gamma_0 \in L$ be a primitive element ($L = K(\gamma_0)$), and let Γ be the set of Galois conjugates of γ_0.

(d) Let E/F be an elliptic curve with complex multiplication by $\mathcal{O}_k$, where F is a finite extension of a quadratic imaginary number field k. For any integral ideal $\mathfrak{a} \subseteq \mathcal{O}_k$ write $E[\mathfrak{a}]$ for the subgroup of points of $E(\bar{F})$ that are annihilated by all elements $a \in \mathfrak{a}$. For $x \in \mathcal{O}_k$ let $[x] \in \mathrm{End}(E)$ be the corresponding endomorphism of E. Let, for simplicity, $(a) = \mathfrak{a} \subseteq \mathcal{O}_k$ be a principal ideal and set $G := E[\mathfrak{a}]$. For $P \in E(\bar{F})$ define $K := F(P)$ and $\Gamma := \{Q \in E(\bar{F}) \mid [a](Q) = P\}$. Then G acts on Γ by translation.

This kind of example is extensively studied in [Ag], [ST] and [T2]. It is also the main topic of this part (see Section 5).

(e) Let $\mathbb{Q}_p \subseteq F$ be a finite field extension of the field of p-adic numbers, and let $\mathfrak{p}_F = (\pi)$ be the maximal ideal of the ring $\mathcal{O}_F$ of integers in F. Let $\mathcal{F}$ be a Lubin-Tate formal group attached to a Lubin-Tate power series $f(X) \in \mathcal{O}_F[[X]]$. Let $[-]\colon \mathcal{O}_F \to \mathrm{End}(\mathcal{F})$ be the usual ring isomorphism with $[\pi](X) = f(X)$. For $n \in \mathbb{N}$ set $G_n := \{x \in \mathfrak{p}_{\bar{F}} \mid [\pi^n](x) = 0\}$, the subgroup of π^n-torsion points in the $\mathcal{O}_F$-module $\mathfrak{p}_{\bar{F}}$ endowed with the $\mathcal{F}$-group law and the $\mathcal{O}_F$-action $ax := [a](x)$ for $a \in \mathcal{O}_F$ and $x \in \mathfrak{p}_{\bar{F}}$, and let $F_n := F(G_n)$ denote the field obtained by adjoining the elements of G_n. For fixed $r, m \in \mathbb{N}_0$, $m \geq 1$, set $K := F_r$, $G := G_m$, choose $\beta \in G_r$, and set $\Gamma := \{x \in \mathfrak{p}_{\bar{F}} \mid [\pi^m](x) = \beta\} \subseteq G_{m+r}$. Then G acts on Γ by translation.

For more details about this example in the case $m \leq r$ see [CT, Ch. X] and [T1]. The general case is dealt with in [BB].

We return to the situation described at the beginning and define

$$\mathbf{A} := \bar{K}G\,, \quad \mathbf{B} := \mathrm{Map}(G, \bar{K})\,, \quad \mathbf{C} := \mathrm{Map}(\Gamma, \bar{K})\,,$$

the group algebra of G over $\bar{K}$, the set of maps from G and from Γ to $\bar{K}$, respectively. Then $\mathbf{A}$ is a $\bar{K}$-Hopf algebra, B is its $\bar{K}$-dual Hopf algebra, $\mathbf{C}$ is a $\bar{K}$-algebra and a right $\mathbf{A}$-module by the $\bar{K}$-linear extension of the action $(f \cdot g)(\gamma) := f({}^g\gamma)$ of G on $\mathbf{C}$, where $g \in G$, $f \in \mathbf{C}$, and $\gamma \in \Gamma$.

Note that Ω acts on $\mathbf{A}$, $\mathbf{B}$, and $\mathbf{C}$ by

$$^{\omega}(\sum_{g\in G}\lambda_g g) := \sum_{g\in G}\omega(\lambda_g)\,^{\omega}g\,, \quad (^{\omega}b)(g) := \omega(b(^{\omega^{-1}}g))\,, \quad (^{\omega}f)(\gamma) := \omega(f(^{\omega^{-1}}\gamma))\,,$$

for $\omega \in \Omega$, $\lambda_g \in \bar{K}$, $b \in \mathbf{B}$, $g \in G$, $f \in C$, and $\gamma \in \Gamma$. This is an action via K-Hopf algebra automorphisms on A and B, and via K-algebra automorphisms on C. Hence, we may take fixed points with respect to the subgroup $\Omega_L = \mathrm{Gal}(\bar{K}/L)$ for any intermediate field $K \subseteq L \subseteq \bar{K}$:

$$A_L := (\bar{K}G)^{\Omega_L}\,, \quad B_L := \mathrm{Map}(G, \bar{K})^{\Omega_L}\,, \quad C_L := \mathrm{Map}(\Gamma, \bar{K})^{\Omega_L}\,.$$

We omit the index L for $L = K$. Then A_L and B_L are L-Hopf subalgebras of $\mathbf{A}$ and $\mathbf{B}$, and they are L-dual to each other. Moreover, C_L is an L-algebra and an A_L-module by restriction of the $\mathbf{A}$-action on $\mathbf{C}$. In Proposition 2.12 we show that C_L together with its A_L-module structure is a Galois object in the sense of [CS], and, if G is abelian, that C_L is a free A_L-module of rank 1. In the abelian case, we also define a resolvent $(f,\chi) \in \bar{K}$, for $f \in \mathbf{C}$ and $\chi \in \hat{G} := \mathrm{Hom}(G, \bar{K}^{\times})$, and show that, for given $f \in C_L$, one has $f \cdot A_L = C_L$ if and only if $(f,\chi) \neq 0$ for all $\chi \in \hat{G}$, see Proposition 2.13.

For any intermediate field $K \subseteq L \subseteq \bar{K}$, the L-algebras B_L and C_L are commutative. Let us assume that G is abelian. Then also A_L is commutative, and we may define the maximal $\mathcal{O}_L$-orders

$$\mathcal{A}_L\,, \quad \mathcal{B}_L = \mathrm{Map}(G, \mathcal{O}_{\bar{K}})^{\Omega_L}, \quad \mathcal{C}_L := \mathrm{Map}(\Gamma, \mathcal{O}_{\bar{K}})^{\Omega_L}\,,$$

of A_L, B_L, and C_L, respectively. Moreover, for arbitrary G, set

$$\mathcal{A}_L^{\circ} := (\mathcal{O}_{\bar{K}}G)^{\Omega_L}\,,$$

which is an $\mathcal{O}_L$-order of A_L. Then, $\mathcal{C}_L$ is an $\mathcal{A}_L^{\circ}$-module and we may define the associated order

$$\mathcal{A}_L^{\mathrm{ass}} := \{a \in A_L \mid \mathcal{C}_L \cdot a \subseteq \mathcal{C}_L\}$$

of $\mathcal{C}_L$ in A_L, which contains $\mathcal{A}_L^{\circ}$. If G is abelian, then we have inclusions

$$\mathcal{A}_L^{\circ} \subseteq \mathcal{A}_L^{\mathrm{ass}} \subseteq \mathcal{A}_L\,.$$

Again , we omit the index L in $\mathcal{A}_L$, $\mathcal{B}_L$, $\mathcal{C}_L$, $\mathcal{A}_L^{\circ}$, $\mathcal{A}_L^{\mathrm{ass}}$, if $L = K$.

We henceforth assume that G is abelian. Then C_L is a free A_L-module of rank one (see Proposition 2.12). This can be viewed as the analogue of the classical Normal Basis Theorem, which states that for a Galois extension N/M the $M\mathrm{Gal}(N/M)$-module N is free of rank one. As in the classical situation we may then ask for an integral analogue of the Normal Basis Theorem. As already mentioned, $\mathcal{A}_L^{\circ}$ acts on $\mathcal{C}_L$; but if our aim is to prove that $\mathcal{C}_L$ is free (or at least locally free) over some order $\tilde{\mathcal{A}}_L$ in A_L, then we have to study $\mathcal{C}_L$ as a module over $\mathcal{A}_L^{\mathrm{ass}}$. In fact, if $\mathcal{C}_L = f \cdot \tilde{\mathcal{A}}_L$ for $f \in \mathcal{C}_L$, then the definition of the associated order immediately implies $\mathcal{A}_L^{\mathrm{ass}} = \tilde{\mathcal{A}}_L$. Since associated orders are determined locally, we can only hope for local freeness, if we consider $\mathcal{C}_L$ over $\mathcal{A}_L^{\mathrm{ass}}$.

To emphasize the analogy to classical Galois module structure theory we recall some well-known results in this context. Let, for the moment, N/M be a Galois extension of number fields with group G. The Normal Basis Theorem suggests one seek an integral normal basis. But by a theorem of E. Noether we know that $\mathcal{O}_N$ is locally free over $\mathcal{O}_M G$, if and only if N/M is at most tamely ramified. If $M = \mathbb{Q}$ and N/M is abelian and tame, then the Theorem of Hilbert-Speiser asserts that $\mathcal{O}_N$ is free of rank one over $\mathbb{Z}G$. By work of Leopoldt [Leo] the following generalization of the Hilbert-Speiser Theorem holds: for an abelian extension $N/\mathbb{Q}$ the ring of integers $\mathcal{O}_N$ is free over its associated order in $\mathbb{Q}G$.

In the relative case, when $\mathbb{Q}$ is replaced by some number field M, there is a beautiful theory due to A. Fröhlich and M. J. Taylor for tamely ramified extensions N/M (see [Fr2]). If we allow wild ramification the situation is very different. Even the local situation is far from being well understood. In particular there is no analogue of E. Noether's theorem and there are very few criteria for determining whether $\mathcal{O}_N$ is locally free over its associated order.

It is therefore important to look for interesting classes of wildly ramified extensions with known Galois structure. Some of the most interesting examples in this context are certain relative ray class field extensions N/M of a quadratic imaginary number field k. There are results due to Cassou-Noguès, Schertz, Taylor and others, stating that $\mathcal{O}_N$ is free over its associated order in MG, see e.g. [CT, Ch. XI], [Sch2]. We shall see that these examples are essentially special cases of Example 1.1(d).

In order to sketch the connection of our approach and classical Galois module theory we return to the situation described at the beginning.

Remarks 1.2 (a) Suppose that the action of Ω on Γ is transitive. Fix an element γ_0 and denote its stabilizer by Ω_L, corresponding to an intermediate field $K \subseteq L \subseteq \bar{K}$. Then one has a bijection $\Omega/\Omega_L \simeq G$, where $\omega\Omega_L$ is mapped to $g \in G$, if ${}^{\omega}\gamma_0 = {}^{g}\gamma_0$. Moreover, associating to $f \in C$ the value $f(\gamma_0) \in \bar{K}$, defines isomorphisms $C \simeq L$ and $\mathcal{C} \simeq \mathcal{O}_L$ of L- (resp. $\mathcal{O}_L$-) algebras.

(b) The absolute Galois group Ω acts trivially on G if and only if $A = KG$.

If one assumes suitable Kummer conditions in Examples 1.1 (a), (d) and (e), then $A = KG$. Moreover, in many interesting examples Ω acts transitively on Γ and, in the notation of Remark 1.2 (a), the fixed field L of the stabilizer $\mathrm{stab}_\Omega(\gamma_0)$ is an abelian Galois extension of K such that the bijection $\mathrm{Gal}(L/K) = \Omega/\Omega_L \simeq G$ is a group isomorphism (see e.g. Lemma 4.1). In this case, the A-module structure of C corresponds to the KG-module structure of L, and we are in the classical situation of Galois module structure theory.

To conclude this introductory section we outline how the rest of this part is arranged and we describe the main results. Section 2 is taken almost unchanged from [BB]. Since it describes the basic algebraic set-up and develops results which are needed in all of the applications, it had to be included for the reader's convenience. The sections 2.1 and 2.2 summarize properties of the Hopf algebras A_L and B_L, respectively, for intermediate fields $K \subseteq L \subseteq \bar{K}$. Most of these properties can already be found in [T2] without proofs. For the reader's convenience and for later use we provide proofs of all assertions. In Section 2.3 we show that $\mathcal{A}_L^\circ$ (resp. $\mathcal{A}_L$ if G is abelian) is an $\mathcal{O}_L$-Hopf order in A_L if and only if the discriminant ideals d_{B_L} of $\mathcal{B}_L$ (resp. d_{A_L} of $\mathcal{A}_L$) over $\mathcal{O}_L$ are trivial, see Proposition 2.8 (resp.Proposition 2.10). Thus, the structural information of being a Hopf order is completely described by an arithmetic invariant, the discriminant. Moreover, we compute the index ideal $[\mathcal{A}_L : \mathcal{A}_L^\circ]_{\mathcal{O}_L}$ in terms of d_{A_L} and d_{B_L}, see Lemma 2.6. Section 2.4 is concerned with the L-algebra structure and the A_L-module structure of C_L. If G is abelian we determine, for any $f \in C_L$ with $f \cdot A_L = C_L$, the index ideal $[\mathcal{C}_L : f \cdot \mathcal{A}_L^\circ]_{\mathcal{O}_L}$ in terms of d_{B_L}, d_{C_L}, and the resolvents (f, χ), $\chi \in \hat{G}$, see Proposition 2.13.

In Section 3 we discuss the cyclotomic example of 1.1(a) in some detail. We show that $\mathcal{C}$ is free of rank one over its associated order (see Theorem 3.6). The proof is achieved prime by prime, and so the main work has to be done in the case $K = \mathbb{Q}(\zeta_{p^r})$, $G = \mu_{p^r}$, with a rational prime p and $m, r \in \mathbb{N}_0$, $m \geq 1$. For $r = 0$ the associated order is given by $\mathcal{A}^\circ$ and the proof of Theorem 3.6 is more or less trivial. In the more interesting case $r \geq 1$ the associated order $\mathcal{A}^{\text{ass}}$ is equal to the unique maximal order $\mathcal{A}$ in A (Theorem 3.1), but with regard to further applications it is more important to note that $\mathcal{A}^{\text{ass}} = \mathcal{A}$ also coincides with the Cartier dual $\mathcal{A}^{\text{gs}}$ of the Hopf order which represents the group scheme of p^m-th roots of unity (Theorem 3.5).

In Section 4 we study a slight generalization of Example 1.1(e), namely relative Lubin-Tate extensions. This section is also part of [BB] (except for the trivial case $r = 0$) and only included for the sake of completeness. These local results will be needed for our treatment of the elliptic curve examples 1.1(d). As in the cyclotomic example we show that for $r \geq 1$ one has $\mathcal{A}^{\text{ass}} = \mathcal{A}^{\text{gs}}$ (Corollary 4.10), where here $\mathcal{A}^{\text{gs}}$ denotes the Cartier dual of the $\mathcal{O}_K$-Hopf algebra which represents the $\mathcal{O}_K$-group scheme of $\mathfrak{p}_F^m$-torsion on $\mathcal{F}$. Furthermore we prove that $\mathcal{C} \simeq \mathcal{A}^{\text{ass}}$ (see Theorem 4.12). The main tool for our proof of Theorem 4.12 will be the factorization of a suitable resolvent function which takes values in $\mathcal{O}_{\bar{F}}[[X]]$ (see Theorem 4.11).

Finally Section 5 contains the main results of these notes. We apply the results of the previous sections to derive analogous results for Example 1.1(d). To that end we introduce in Section 5.1 a special class of elliptic curves. Let k be a quadratic imaginary number field. For an integral ideal $\mathfrak{f}$ of k we denote the ray class field of conductor $\mathfrak{f}$ by $k(\mathfrak{f})$. Let F/k be an abelian number field extension and E/F an elliptic curve with complex multiplication by $\mathcal{O}_k$. In addition we assume that $F(E_{\text{tor}})/k$ is abelian. This is equivalent to the existence of a Groessencharacter φ of k such that $\psi_{E/F} = \varphi \circ N_{F/k}$, where $\psi_{E/F}$ denotes the Groessencharacter associated to E/F and $N_{F/k}$ the norm map from F to k. We fix φ and set $\mathfrak{f} = \operatorname{lcm}(\mathfrak{f}_\varphi, \mathfrak{f}_{F/k})$, where $\mathfrak{f}_\varphi$ and $\mathfrak{f}_{F/k}$ denote the conductors of φ

and F/k, respectively. Note that $\mathfrak{f}$ is an invariant of E/F and does not depend on the choice of φ.

As in the cyclotomic example the major problem is to derive a result in the prime power case. Let $\mathfrak{p}$ be a prime ideal of k such that $(\mathfrak{f}, \mathfrak{p}) = 1$. We set $G = E[\mathfrak{p}^m]$ and fix a primitive $\mathfrak{p}^{r+m}$-torsion point $Q_0 \in E(\bar{F})$, where $r, m \in \mathbb{N}_0$, $m \geq 1$. We set $K = k(\mathfrak{f}\mathfrak{p}^r)$ and $\Gamma = \{Q_0 +_E P \mid P \in G\}$. Then $K(Q_0) = k(\mathfrak{f}\mathfrak{p}^{r+m})$ and $\Omega = \Omega_K$ acts on Γ (Lemma 5.9). Again the case $r = 0$ is easily established (Theorem 5.20). Hence we assume $r \geq 1$ in the following. In this case we obtain a K-algebra isomorphism

$$\begin{array}{rcl} \tau : C & \longrightarrow & L := k(\mathfrak{f}\mathfrak{p}^{r+m}), \\ f & \longmapsto & f(Q_0) \end{array}$$

and a bijection $\varphi : G \to \mathrm{Gal}(L/K)$ by Remark 1.2. Via τ we endow L with the structure of an A-module. We remark that under the Kummer condition $r \geq m \geq 1$ one has $A = KG$, φ is a group isomorphism, and identifying G and $\mathrm{Gal}(L/K)$ the map τ is actually an isomorphism of $A = KG$-modules. In other words, we are in the classical situation of Galois module structure, studying the Galois structure of the ring of integers in the wildly ramified extension $k(\mathfrak{f}\mathfrak{p}^{r+m})/k(\mathfrak{f}\mathfrak{p}^r)$.

In [Sch2], R. Schertz constructed certain Galois resolvents for extensions of the form $k(\mathfrak{f}\mathfrak{p}^{r+m})/k(\mathfrak{f}\mathfrak{p}^r)$, $r \geq m \geq 1$, and computed under some restrictions on $\mathfrak{f}$ and $\mathfrak{p}$ their prime ideal factorization. Via τ^{-1} his resolvents are mapped to the kind of resolvents we define in (12) and we can use his techniques and results to obtain useful resolvents for $r, m \geq 1$. This is the content of Sections 5.3, 5.4 and 5.5.

For a prime $\mathfrak{P}$ of F above $\mathfrak{p}$ the formal group $\hat{E}$ associated with the kernel of reduction modulo $\mathfrak{P}$ is a relative Lubin-Tate formal group (Lemma 5.8).This fact provides the link from the global theory to the local Lubin-Tate theory of Section 4. Section 5.6 is devoted to the investigation of this connection.

In Section 5.7 we derive our main results on the module structure of $\mathcal{C}$. Again the case $r = 0$ is easily established. The associated order $\mathcal{A}^{\text{ass}}$ is in this case given by $\mathcal{A}^\circ$ and $\mathcal{C}$ is free of rank one over $\mathcal{A}^{\text{ass}}$. The case $r \geq 1$ is much more interesting. In order to control the ramification of primes $\mathfrak{Q}$ of K not dividing $\mathfrak{p}$ we impose the following hypothesis:

$$E \text{ attains good reduction over } K = k(\mathfrak{f}\mathfrak{p}^r).$$

This is in fact a very mild condition, since for a fixed elliptic curve E/F this hypothesis is satisfied for all but a finite number of pairs $\mathfrak{p}, r$ (see Lemma 5.26).

We will then prove that the associated order $\mathcal{A}^{\text{ass}}$ coincides with the Cartier dual $\mathcal{A}^{\text{gs}}$ of the $\mathcal{O}_K$-Hopf order which represents the $\mathcal{O}_K$-group scheme of $\mathfrak{p}^m$-torsion points on E. Furthermore we show that $\mathcal{C}$ is a locally free, rank one $\mathcal{A}^{\text{ass}}$-module (Theorem 5.24).

Due to the lack of appropriate resolvents we are not able to prove a complete result for the question of global freeness of $\mathcal{C}$ over $\mathcal{A}^{\text{ass}}$. However, if $\mathfrak{f}$ is composite and $(\mathfrak{f}, \mathfrak{p}\bar{\mathfrak{p}}) = 1$ we can show that $\mathcal{C}$ is free over its associated order

(Theorem 5.27). If $\mathfrak{f}$ is the power of an $\mathcal{O}_k$-prime ideal we make use of the fact that the associated orders behave well under a change of the base field. This provides restriction homomorphisms between the relevant locally free classgroups. Using this tool we prove that $\mathcal{C}$ is free over its associated order if $(\mathfrak{f}, \mathfrak{p}\bar{\mathfrak{p}}) = 1$ and $(\mathfrak{p}, w_k) = 1$, where w_k denotes the number of roots of unity in k (Theorem 5.29). As a corollary we obtain results for the classical Galois module structure of rings of integers: let $r, m \geq 1$ be integers with $1 \leq m \leq r$, let $\mathfrak{f}$ be an integral $\mathcal{O}_k$-ideal with $|\{\varepsilon \in \mathcal{O}_k{}^* \mid \varepsilon \equiv 1 \pmod{\mathfrak{f}}\}| = 1$ and let $\mathfrak{p}$ be a prime with $(\mathfrak{f}, \mathfrak{p}\bar{\mathfrak{p}}) = 1$ and $(\mathfrak{p}, w_k) = 1$. Set $K = k(\mathfrak{f}\mathfrak{p}^r)$ and $L = k(\mathfrak{f}\mathfrak{p}^{r+m})$. Then $\mathcal{O}_L$ is free over its associated order in $K\mathrm{Gal}(L/K)$ (Corollary 5.30). Finally we use the results of the prime power case to derive results in the composite case (Theorem 5.32).

In the last Section 6 we relate our results to the theory of Kummer orders introduced by M.J. Taylor in [T2]. In particular, our results imply that for the special class of elliptic curves described in Section 5.1 the Kummer order $\tilde{\mathcal{O}}_P$ is essentially the full ring of integers (Theorem 6.2). Our approach also provides infinitely many examples of elliptic curves defined over a number field M with complex multiplication by $\mathcal{O}_k$ and everywhere good reduction for which a conjecture of M. J. Taylor [T2, §1] holds in full generality (Theorem 6.4).

2 Algebra

2.1 Forms of group algebras

In this section we study the properties of the $\bar{K}$-Hopf algebra $\mathbf{A}$ and its subalgebras $A_L = \mathbf{A}^{\Omega_L}$, for intermediate fields $K \subseteq L \subseteq \bar{K}$.

For a K-Hopf algebra we write as usual $\Delta_H : H \to H \otimes_K H$ for the diagonal, $S_H : H \to H$ for the antipode and $\varepsilon_H : H \to K$ for the augmentation. If there is no danger of confusion we omit the index.

We view $\mathbf{A}$ as a Hopf algebra with $\Delta(g) = g \otimes g$, $S(g) = g^{-1}$ and $\varepsilon(g) = 1$ for $g \in G$.

Lemma 2.1 *Let $K \subseteq L \subseteq \bar{K}$ be an intermediate field, and let $g_1, \ldots, g_r \in G$ be a set of representatives for the Ω_L-orbits of G. For each $i \in \{1, \ldots, r\}$ let L_i be the fixed field of $\mathrm{stab}_{\Omega_L}(g_i) \leqslant \Omega_L$, and let $x_{i,1}, \ldots, x_{i,r_i}$ be an L-basis of L_i. Finally, for $1 \leqslant i \leqslant r$ and $1 \leqslant j \leqslant r_i$, set*

$$a_{i,j} := \sum_{\omega \in \Omega_L / \mathrm{stab}_{\Omega_L}(g_i)} \omega(x_{i,j})\, {}^{\omega}g_i \in \mathbf{A}\,,$$

and assume that $L \subseteq M \subseteq N \subseteq \bar{K}$ are further intermediate fields. Then the following assertions hold:

(i) *The elements $a_{i,j}$, $1 \leqslant i \leqslant r$, $1 \leqslant j \leqslant r_i$, form an L-basis of A_L. If, for each $i \in \{1, \ldots, r\}$ the elements $x_{i,1}, \ldots, x_{i,r_i}$ form an $\mathcal{O}_L$-basis of $\mathcal{O}_{L_i}$ then the elements $a_{i,j}$, $1 \leqslant i \leqslant r$, $1 \leqslant j \leqslant r_i$, form an $\mathcal{O}_L$-basis of $\mathcal{A}_L^0$.*

(ii) *One has $\dim_L(A_L) = |G|$.*

(iii) *The elements $a_{i,j}$, $1 \leqslant i \leqslant r$, $1 \leqslant j \leqslant r_i$, form also an M-basis of A_M; in particular, they form a $\bar{K}$-basis of $\mathbf{A}$.*

(iv) *The map*

$$i_L^M : A_L \otimes_L A_L \to A_M \otimes_M A_M\,, \quad a \otimes_L a' \mapsto a \otimes_M a'\,,$$

is an injective L-algebra map such that $i_M^N \circ i_L^M = i_L^N$. In particular, $A_L \otimes_L A_L$ can be regarded as an L-subalgebra of $\mathbf{A} \otimes_{\bar{K}} \mathbf{A}$.

(v) *Under the identification $A_L \otimes_L A_L \subseteq \mathbf{A} \otimes_{\bar{K}} \mathbf{A}$ of (iv), A_L is an L-Hopf subalgebra of $\mathbf{A}$.*

(vi) *The map*

$$\phi_L^M : M \otimes_L A_L \to A_M\,, \quad \lambda \otimes_L a \mapsto \lambda a\,,$$

is an isomorphism of M-Hopf algebras such that the diagrams

$$\begin{array}{ccc} M \otimes_L A_L & \xrightarrow{\phi_L^M} & A_M \\ {\scriptstyle \omega\otimes\omega}\downarrow & & \downarrow{\scriptstyle \omega} \\ \omega(M) \otimes_{\omega(L)} A_{\omega(L)} & \xrightarrow{\phi_{\omega(L)}^{\omega(M)}} & A_{\omega(M)} \end{array} \qquad \begin{array}{ccc} N \otimes_M M \otimes_L A_L & \xrightarrow{N\otimes\phi_L^M} & N \otimes_M A_M \\ {\scriptstyle \mathrm{can}\otimes A_L}\downarrow & & \downarrow{\scriptstyle \phi_M^N} \\ N \otimes_L A_L & \xrightarrow{\phi_L^N} & A_N \end{array}$$

commute for each $\omega \in \Omega$, where can: $N \otimes_M M \to N$ *is the multiplication map.*

Proof (i) It is easy to see that the elements $a_{i,j}$, $1 \leqslant i \leqslant r$, $1 \leqslant j \leqslant r_i$, lie in A_L. On the other hand, for arbitrary $a = \sum_{g\in G} \lambda_g g \in A_L$, the coefficient λ_g is fixed under $\mathrm{stab}_{\Omega_L}(g)$, for each $g \in G$, and so $\lambda_{g_i} \in L_i$ for each $i \in \{1, \ldots, r\}$. Moreover, for each $i \in \{1, \ldots, r\}$ and each $\omega \in \Omega_L$, one has $\lambda_{{}^\omega g_i} = \omega(\lambda_{g_i})$. Now it follows easily that the elements $a_{i,j}$, $1 \leqslant i \leqslant r$, $1 \leqslant j \leqslant r_i$, form an L-basis of A_L. The second assertions is shown in a similar way.

(ii) Indeed, by (i) we have

$$\dim_L(A_L) = \sum_{i=1}^{r} r_i = \sum_{r=1}^{r} [L_i : L] = \sum_{i=1}^{r} [\Omega_L : \mathrm{stab}_{\Omega_L}(g_i)] = |G|\,.$$

(iii) First we show that the elements $a_{i,j}$, $1 \leqslant i \leqslant r$, $1 \leqslant j \leqslant r_i$, form a $\bar{K}$-basis of $\mathbf{A}$. Expressing the elements $a_{i,j}$, $1 \leqslant i \leqslant r$, $1 \leqslant j \leqslant r_i$, by the basis G of $\mathbf{A}$ produces a matrix which is a block diagonal matrix with r blocks indexed by the Ω_L-orbits of G, where the i-th block is given by

$$\Big(\omega(x_{i,j})\Big)_{\substack{j\in\{1,\ldots,r_i\} \\ \omega\in\Omega_L/\mathrm{stab}_{\Omega_L}(g_i)}}$$

whose determinant does not vanish, since L_i/L is separable. This shows the result for $M = \bar{K}$. For arbitrary M, it suffices by (ii) to show that the elements $a_{i,j}$ $(1 \leqslant i \leqslant r, 1 \leqslant j \leqslant r_i)$ are M-linearly independent. But this follows from the case $M = \bar{K}$.

(iv) This follows immediately from (iii), since i_L^M maps an L-basis to an M-basis.

(v) It is easy to see that $S(A_L) \subseteq A_L$, since taking inverses in G commutes with the Ω-action on $\mathbf{A}$. Let $a \in A_L$. Then, by (iii), we may write

$$\Delta(a) = \sum_{i,j,i',j'} \lambda_{i,j,i',j'}\, a_{i,j} \otimes_{\bar{K}} a_{i',j'} \in \mathbf{A} \otimes_{\bar{K}} \mathbf{A}$$

with uniquely determined coefficients $\lambda_{i,j,i',j'} \in \bar{K}$. We apply an arbitrary element $\omega \in \Omega_L$ on both sides. Since Δ respects the Ω-action, we obtain

$$\Delta(a) = \sum_{i,j,i',j'} \omega(\lambda_{i,j,i',j'})\, a_{i,j} \otimes_{\bar{K}} a_{i',j'} \,.$$

Thus, by their uniqueness, the coefficients $\lambda_{i,j,i',j'}$ are contained in L, and $\Delta(a) \in i_L^{\bar{K}}(A_L \otimes_L A_L)$.

(vi) It is easy to see that ϕ_L^M is a homomorphism of M-Hopf algebras and that the two diagrams commute. Moreover, by (iii), ϕ_L^M is an isomorphism. $\square$

For the rest of this section we assume that G is abelian. Let L be a subextension of $\bar{K}/K$. In order to understand the L-algebra structure of A_L we work with the Wedderburn decomposition of $\mathbf{A}$. Let $\hat{G} := \mathrm{Hom}(G, \bar{K}^\times)$ denote the abelian group of $\bar{K}$-characters of G. Then Ω acts on $\hat{G}$ by

$$({}^{\omega}\chi)(g) := \omega\big(\chi({}^{\omega^{-1}}g)\big)$$

for $\chi \in \hat{G}$, $\omega \in \Omega$, and $g \in G$. It is well-known that the map

$$\rho\colon \mathbf{A} = \bar{K}G \to \prod_{\chi \in \hat{G}} \bar{K}\,, \quad \sum_{g \in G} \lambda_g g \mapsto \big(\sum_{g \in G} \lambda_g \chi(g)\big)_{\chi \in \hat{G}}$$

is an isomorphism of $\bar{K}$-algebras. For $\chi \in \hat{G}$, we denote by $e_\chi \in \mathbf{A}$ the element corresponding to the primitive idempotent ε_χ of $\prod_{\chi \in \hat{G}} \bar{K}$ which has entry 1 in the component χ and 0 everywhere else. Then

$$e_\chi = \frac{1}{|G|} \sum_{g \in G} \chi(g^{-1}) g \,.$$

Note that ${}^{\omega}(e_\chi) = e_{({}^{\omega}\chi)}$ for each $\omega \in \Omega$ and $\chi \in \hat{G}$. The Ω-action on $\mathbf{A}$ is transported via ρ to the action

$${}^{\omega}\big((\lambda_\chi)_{\chi \in \hat{G}}\big) = \big(\omega(\lambda_{({}^{\omega^{-1}}\chi)})\big)_{\chi \in \hat{G}}$$

for $(\lambda_\chi)_{\chi \in \hat{G}} \in \prod_{\chi \in \hat{G}} \bar{K}$ and $\omega \in \Omega$. Thus, the application of ω moves the χ-component λ_χ to the ${}^{\omega}\chi$-component while simultaneously applying ω to λ_χ. This implies that ρ restricts to an isomorphism

$$\rho_L\colon A_L \simeq \{(\lambda_\chi) \in \prod_{\chi \in \hat{G}} \bar{K} \mid \omega(\lambda_\chi) = \lambda_{({}^{\omega}\chi)} \text{ for all } \omega \in \Omega_L\}\,. \tag{1}$$

Lemma 2.2 *Assume that G is abelian and let $K \subseteq L \subseteq \bar{K}$ be an intermediate field. Let $\chi_1, \ldots, \chi_s \in \hat{G}$ be a set of representatives for the Ω_L-orbits of $\hat{G}$. For each $k \in \{1, \ldots, s\}$, let $\hat{L}_k$ denote the fixed field of $\mathrm{stab}_{\Omega_L}(\chi_k) \leqslant \Omega_L$, and let $y_{k,1}, \ldots, y_{k,s_k}$ be an L-basis of $\hat{L}_k$. For $1 \leqslant k \leqslant s$ and $1 \leqslant l \leqslant s_k$, set*

$$\hat{a}_{k,l} := \sum_{\omega \in \Omega_L / \mathrm{stab}_{\Omega_L}(\chi_k)} \omega(y_{k,l}) \, {}^{\omega}e_{\chi_k} \in \mathbf{A}\,.$$

Then the following assertions hold:

(i) *The composition*

$$\tilde{\rho}\colon \mathbf{A} \xrightarrow{\rho} \prod_{\chi \in \hat{G}} \bar{K} \xrightarrow{p} \prod_{k=1}^{s} \bar{K}\,,$$

where p denotes the projection to the $\chi_1, \ldots, \chi_s$-components, restricts to an L-algebra isomorphism

$$\tilde{\rho}_L \colon A_L \to \prod_{k=1}^{s} \hat{L}_k\,.$$

In particular, the maximal order $\mathcal{A}_L$ of A_L is given by $\tilde{\rho}_L^{-1}(\prod_{k=1}^{s} \mathcal{O}_{\hat{L}_k})$.

(ii) *The elements $\hat{a}_{k,l}$, $1 \leqslant k \leqslant s$, $1 \leqslant l \leqslant s_k$, form an L-basis of A_L. If, for each $k \in \{1, \ldots, s\}$, the elements $y_{k,1}, \ldots, y_{k,s_k}$ form an $\mathcal{O}_L$-basis of $\mathcal{O}_{\hat{L}_K}$ then the elements $\hat{a}_{k,l}$, $1 \leqslant k \leqslant s$, $1 \leqslant l \leqslant s_k$, form an $\mathcal{O}_L$-basis of $\mathcal{A}_L$.*

Proof (i) This follows immediately from (1).

(ii) The elements $\hat{a}_{k,l}$ are contained in A_L and $\tilde{\rho}_L(\hat{a}_{k,l})$, $1 \leqslant k \leqslant s$, $1 \leqslant l \leqslant s_k$ form an L-basis of $\prod_{k=1}^{s} \hat{L}_k$. Thus (ii) follows from (i). The integral version can be seen in the same way. □

2.2 Duality

It is well-known that the Hopf algebra dual (also called Cartier dual) of $\mathbf{A}$ is the $\bar{K}$-Hopf algebra $\mathbf{B} := \mathrm{Map}(G, \bar{K})$ consisting of all set maps from G to $\bar{K}$. The duality is given by the non-degenerate bilinear form

$$(-,-)\colon \mathbf{A} \otimes_{\bar{K}} \mathbf{B} \to \bar{K}, \quad \Big(\sum_{g \in G} \lambda_g g, f\Big) \mapsto \sum_{g \in G} \lambda_g f(g)\,.$$

The $\bar{K}$-linear structure of $\mathbf{B}$ is obvious. Multiplication is given by $(f_1 f_2)(g) = f_1(g) f_2(g)$, for $f_1, f_2 \in \mathbf{B}$ and $g \in G$, with the constant map with value 1 as unity. The diagonal Δ, augmentation ϵ, and antipode S are given by

$$\begin{aligned} \Delta(f)(g_1, g_2) &= f(g_1 g_2)\,, \\ \epsilon(f) &= f(1)\,, \\ S(f)(g) &= f(g^{-1})\,, \end{aligned}$$

respectively, for $f \in \mathbf{B}$, $g, g_1, g_2 \in G$, where in the definition of Δ we identify $\mathbf{B} \otimes_{\bar{K}} \mathbf{B}$ with $\mathrm{Map}(G \times G, \bar{K})$ in the obvious way. For the $\bar{K}$-basis elements l_g, $g \in G$, with $l_g(h) := \delta_{g,h}$ for $h \in G$, we have

$$\Delta(l_g) = \sum_{\substack{g_1, g_2 \in G \\ g_1 g_2 = g}} l_{g_1} \otimes_{\bar{K}} l_{g_2} .$$

Note that Ω acts on $\mathbf{B}$ by

$$({}^{\omega}f)(g) := \omega\big(f({}^{\omega^{-1}}g)\big)$$

for $\omega \in \Omega$, $f \in \mathbf{B}$, and $g \in G$. This action respects the $\bar{K}$-Hopf algebra structure, as is easily verified. For $a \in \mathbf{A}$, $f \in \mathbf{B}$, and $\omega \in \Omega$ one has

$$({}^{\omega}a, {}^{\omega}f) = \omega\big((a, f)\big) . \tag{2}$$

For each intermediate field $K \subseteq L \subseteq \bar{K}$ we set

$$B_L := \mathbf{B}^{\Omega_L} = \mathrm{Map}(G, \bar{K})^{\Omega_L} = \{f \colon G \to \bar{K} \mid f({}^{\omega}g) = \omega(f(g)) \text{ for all } \omega \in \Omega_L\} .$$

Then B_L is an L-subalgebra of $\mathbf{B}$.

The next lemma shows that B_L is an L-Hopf subalgebra of $\mathbf{B}$ and is the L-dual of A_L with respect to the restricted bilinear form $(-,-)$. By $\mathcal{B}_L$ we denote the maximal order in B_L which is given by

$$\mathcal{B}_L = \mathrm{Map}(G, \mathcal{O}_{\bar{K}})^{\Omega_L} .$$

Lemma 2.3 *Let $K \subseteq L \subseteq \bar{K}$ be an intermediate field, and let $g_1, \ldots, g_r \in G$, $L_1, \ldots, L_r$, and $x_{i,1}, \ldots, x_{i,r_i} \in L_i$ ($1 \leqslant i \leqslant r$) be given as in Lemma 2.1. Moreover, for $1 \leqslant i \leqslant r$ and $1 \leqslant j \leqslant r_i$, let $b_{i,j} \in \mathbf{B}$ be defined by*

$$b_{i,j}(g) := \begin{cases} \omega(x_{i,j}), & \text{if } g = {}^{\omega}g_i \text{ for some } \omega \in \Omega_L, \\ 0, & \text{otherwise.} \end{cases}$$

Assume that $L \subseteq M \subseteq N \subseteq \bar{K}$ are further intermediate fields. Then the following assertions hold:

(i) *The map*

$$\sigma_L \colon B_L \to \prod_{i=1}^{r} L_i , \quad b \mapsto b(g_i) ,$$

is an L-algebra isomorphism. In particular, σ_L restricts to an isomorphism

$$\sigma_L \colon \mathcal{B}_L \to \prod_{i=1}^{r} \mathcal{O}_{L_i} .$$

(ii) *The elements* $b_{i,j}$, $1 \leqslant i \leqslant r$, $1 \leqslant j \leqslant r_i$, *form an* L*-basis of* B_L. *If, for each* $i \in \{1, \ldots, r\}$, *the elements* $x_{i,1}, \ldots, x_{i,r_i}$ *form an* $\mathcal{O}_L$*-basis of* $\mathcal{O}_{L_i}$ *then the elements* $b_{i,j}$, $1 \leqslant i \leqslant r$, $1 \leqslant j \leqslant r_i$, *form an* $\mathcal{O}_L$*-basis of* $\mathcal{B}_L$.

(iii) *One has* $\dim_L(B_L) = |G|$.

(iv) *The elements* $b_{i,j}$, $1 \leqslant i \leqslant r$, $1 \leqslant j \leqslant r_i$, *form also an* M*-basis of* B_M.

(v) *The map*

$$j_L^M : B_L \otimes_L B_L \to B_M \otimes_M B_M \,, \quad b \otimes_L b' \mapsto b \otimes_M b' \,,$$

is an injective L*-algebra homomorphism such that* $j_M^N \circ j_L^M = j_L^N$. *In particular,* $B_L \otimes_L B_L$ *can be regarded as* L*-subalgebra of* $\mathbf{B} \otimes_{\bar{K}} \mathbf{B}$.

(vi) *Under the identification* $B_L \otimes_L B_L \subseteq \mathbf{B} \otimes_{\bar{K}} \mathbf{B}$ *of (v),* B_L *is an* L*-Hopf subalgebra of* $\mathbf{B}$.

(vii) *The map*

$$\psi_L^M : M \otimes_L B_L \to B_M \,, \quad \lambda \otimes_L b \mapsto \lambda b \,,$$

is an isomorphism of M*-Hopf algebras such that the diagrams*

$$\begin{array}{ccc} M \otimes_L B_L & \xrightarrow{\psi_L^M} & B_M \\ {\scriptstyle \omega\otimes\omega}\big\downarrow & & \big\downarrow{\scriptstyle \omega} \\ \omega(M) \otimes_{\omega(L)} B_{\omega(L)} & \xrightarrow{\psi_{\omega(L)}^{\omega(M)}} & B_{\omega(M)} \end{array} \qquad \begin{array}{ccc} N \otimes_M M \otimes_L B_L & \xrightarrow{N\otimes\psi_L^M} & N \otimes_M B_M \\ {\scriptstyle \mathrm{can}\otimes B_L}\big\downarrow & & \big\downarrow{\scriptstyle \psi_M^N} \\ N \otimes_L A_L & \xrightarrow{\psi_L^N} & B_N \end{array}$$

commute for all $\omega \in \Omega$.

(viii) *The map* $A_L \otimes_L B_L \to A_M \otimes_M B_M$, $a \otimes_L b \mapsto a \otimes_M b$, *is injective; in particular,* $A_L \otimes_L B_L$ *can be regarded as an* L*-subspace of* $\mathbf{A} \otimes_{\bar{K}} \mathbf{B}$. *Morover, the restriction of* $(-,-)$ *to* $A_L \otimes_L B_L$ *takes values in* L *and is non-degenerate.*

(ix) *The* L*-Hopf algebras* A_L *and* B_L *are dual to each other with respect to* $(-,-) \colon A_L \otimes_L B_L \to L$.

Proof (i) For $b \in B_L$ and $i \in \{1, \ldots, r\}$, the elements $b({}^{\omega}g_i) = \omega(b(g_i))$, $\omega \in \Omega_L$, are determined by $b(g_i)$. Hence, σ_L is injective. On the other hand, for given elements $\lambda_i \in L_i$, $i = 1, \ldots, r$, the map $b \colon G \to \bar{K}$, defined by $b({}^{\omega}g_i) := \omega(\lambda_i)$, for $i = 1, \ldots, r$ and $\omega \in \Omega_L$, is obviously in B_L.

(ii) This follows immediately from (i).

(iii) This follows from (ii) and the equation $\sum_{i=1}^{r} [\Omega_L : \mathrm{stab}_{\Omega_L}(g_i)] = |G|$.

(iv) This is proved in a similar way as Lemma 2.1 (iii) by reduction to the case $M = \bar{K}$ and using the basis l_g, $g \in G$, of $\mathbf{B}$ which leads to the same transition matrix as in the proof of Lemma 2.1 (iii).

(v) This follows from (iv).

(vi) This is proved in a similar way as Lemma 2.1 (v) using the basis $b_{i,j}$, $1 \leqslant i \leqslant r$, $1 \leqslant j \leqslant r_i$, of B_L.

(vii) By (iv), ψ_L^M is an isomorphism of M-spaces. The remaining assertions are easily verified.

(viii) The injectivity of the map $A_L \otimes_L B_L \to A_M \otimes_M B_M$ follows from Lemma 2.1 (iii) and part (iv). Moreover, $(A_L, B_L) \subseteq L$ by Equation (2). Using the bases $a_{i,j}$ of A_L from Lemma 2.1 and $b_{i,j}$ of B_L, $1 \leqslant i \leqslant r$, $1 \leqslant j \leqslant r_i$, with their property from Lemma 2.1 (iii) and from (iv), we see that $(A_L, B_L) = L$ and that the restricted pairing $A_L \otimes_L B_L \to L$ is non-degenerate.

(ix) This follows from part (viii) and from the existence of bases $a_{i,j}$ of A_L and $b_{i,j}$ of B_L with the properties from Lemma 2.1 (iii) and from (iv). $\square$

2.3 Indices and Hopf structures

Let $K \subseteq L \subseteq \bar{K}$ be an intermediate field. We may take duals of $\mathcal{O}_L$-lattices in A_L and B_L with respect to the non-degenerate pairing

$$A_L \otimes_L B_L \to L\,, \quad \big(\sum_{g\in G} \lambda_g g, f\big) \mapsto \sum_{g\in G} \lambda_g f(g)\,.$$

More precisely, if $\mathcal{R} \subseteq A_L$ and $\mathcal{S} \subseteq B_L$ are $\mathcal{O}_L$-lattices then

$$\mathcal{R}^* := \{f \in B_L \mid (r,f) \in \mathcal{O}_L \text{ for all } r \in \mathcal{R}\}$$

and

$$\mathcal{S}^* := \{a \in A_L \mid (a,s) \in \mathcal{O}_L \text{ for all } s \in \mathcal{S}\}$$

are $\mathcal{O}_L$-lattices in B_L and A_L respectively. Note that $\mathcal{R}$ is an $\mathcal{O}_L$-order (resp. $\mathcal{O}_L$-subcoalgebra) of A_L if and only if $\mathcal{R}^*$ is an $\mathcal{O}_L$-subcoalgebra (resp. $\mathcal{O}_L$-order) in B_L. A similar statement holds for $\mathcal{S}$. Moreover, $\mathcal{R}$ is an $\mathcal{O}_L$-Hopf order in A_L if and only if $\mathcal{R}^*$ is an $\mathcal{O}_L$-Hopf order in B_L, and similarly for $\mathcal{S}$.

Recall that for $\mathcal{O}_L$-lattices $X \subseteq Y$ of equal $\mathcal{O}_L$-rank the *$\mathcal{O}_L$-order ideal* $[Y : X]_{\mathcal{O}_L}$ is defined as the product $\mathfrak{p}_1 \cdots \mathfrak{p}_t$ of non-zero prime ideals $\mathfrak{p}_1, \dots, \mathfrak{p}_t$ of $\mathcal{O}_L$ if $R/\mathfrak{p}_1, \dots, R/\mathfrak{p}_t$ are the $\mathcal{O}_L$-composition factors of Y/X. More generally, for $\mathcal{O}_L$-lattices X and Y in a finite dimensional L-vector space the order ideal $[Y : X]_{\mathcal{O}_L}$ is defined as the fractional ideal $[Y : X \cap Y]_{\mathcal{O}_L}[X : X \cap Y]_{\mathcal{O}_L}^{-1}$. For the following properties of order ideals see for example [R, §4]. If $L \subseteq L' \subseteq \bar{K}$ is a finite extension field of L then

$$\big[\mathcal{O}_{L'} \otimes_{\mathcal{O}_L} Y : \mathcal{O}_{L'} \otimes_{\mathcal{O}_L} X\big]_{\mathcal{O}_{L'}} = [Y : X]_{\mathcal{O}_L}\mathcal{O}_{L'}\,.$$

If $\mathfrak{p}$ is a non-zero prime ideal of $\mathcal{O}_L$ then the following localization property holds:

$$[Y_\mathfrak{p} : X_\mathfrak{p}]_{(\mathcal{O}_L)_\mathfrak{p}} = \big([Y : X]_{\mathcal{O}_L}\big)_\mathfrak{p}\,.$$

If Y and X are free $\mathcal{O}_L$-modules and M is the matrix of coefficients arising from expressing an $\mathcal{O}_L$-basis of X by an $\mathcal{O}_L$-basis of Y, then

$$[Y : X]_{\mathcal{O}_L} = \det(M)\mathcal{O}_L\,.$$

Finally, if $L \subseteq L' \subseteq \bar{K}$ is as above and $X' \subseteq Y'$ are $\mathcal{O}_{L'}$-lattices then

$$[Y' : X']_{\mathcal{O}_L} = N_{L'/L}\big([Y' : X']_{\mathcal{O}_{L'}}\big)\,.$$

If G is abelian we denote by d_{A_L} the discriminant ideal of the maximal order $\mathcal{A}_L$ over $\mathcal{O}_L$, i.e. $d_{A_L} = \prod_{k=1}^{s} d_{\hat{L}_k/L}$ in the notation of Lemma 2.2. Similarly, for arbitrary G, we denote by d_{B_L} the discriminant ideal of the maximal order $\mathcal{B}_L$ over $\mathcal{O}_L$, i.e. $d_{B_L} = \prod_{i=1}^{r} d_{L_i/L}$ in the notation of Lemma 2.1 and Lemma 2.3. If $L \subseteq L' \subseteq \bar{K}$ is as above then we write $\mathcal{D}_{L'/L}$ for the different of $\mathcal{O}_{L'}$ over $\mathcal{O}_L$.

Lemma 2.4 *With the notation of Lemma 2.1 and Lemma 2.3 one has*

$$\mathcal{B}_L^* = \Big\{\sum_{i=1}^{r} \sum_{\omega\in\Omega_L/\mathrm{stab}_{\Omega_L}(g_i)} \omega(\lambda_i)\ {}^{\omega}g_i \mid \lambda_i \in \mathcal{D}_{L_i/L}^{-1} \text{ for } i = 1,\dots,r\Big\}\,.$$

Moreover, $\mathcal{B}_L^*$ is an $\mathcal{O}_L$-order in A_L if and only if $d_{B_L} = \mathcal{O}_L$.

Proof Each element $a \in A_L$ can be written in the form

$$a = \sum_{i=1}^{r} \sum_{\omega\in\Omega_L/\mathrm{stab}_{\Omega_L}(g_i)} \omega(\lambda_i)\ {}^{\omega}g_i$$

with uniquely determined $\lambda_i \in L_i$, $i = 1,\dots,r$, by Lemma 2.1 (i). Then $a \in \mathcal{B}_L^*$ if and only if $(a,f) \in \mathcal{O}_L$ for all $f \in \mathcal{B}_L$. By Lemma 2.3 (i), each $f \in \mathcal{B}_L^*$ is a sum of elements of the form $\sum_\omega \omega(x_i)\, l_{{}^{\omega}g_i}$, $x_i \in \mathcal{O}_{L_i}$, $i = 1,\dots,r$, where the sum runs over coset representatives of $\Omega_L/\mathrm{stab}_{\Omega_L}(g_i)$. Hence, $a \in \mathcal{B}_L^*$ if and only if

$$\sum_{\omega\in\Omega_L/\mathrm{stab}_{\Omega_L}(g_i)} \omega(\lambda_i)\,\omega(x_i) = \mathrm{Tr}_{L_i/L}(\lambda_i x_i) \in \mathcal{O}_L$$

for all $i \in \{1,\dots,r\}$ and all $x_i \in \mathcal{O}_{L_i}$, which is equivalent to $\lambda_i \in \mathcal{D}_{L_i/L}^{-1}$ for all $i \in \{1,\dots,r\}$.

If $d_{B_L} = \mathcal{O}_L$ then $\mathcal{D}_{L_i/L} = \mathcal{O}_{L_i}$ for all $i = 1,\dots,r$, and therefore $\mathcal{B}_L^* = \mathcal{A}_L^\circ$ is an $\mathcal{O}_L$-order. Suppose, conversely, that $\mathcal{B}_L^*$ is an $\mathcal{O}_L$-order and let $i \in \{1,\dots,r\}$ be arbitrary. Let $i' \in \{1,\dots,r\}$ and $\nu \in \Omega_L$ be such that $g_i^{-1} = {}^{\nu}g_{i'}$. Note that $\mathrm{stab}_{\Omega_L}(g_i) = \mathrm{stab}_{\Omega_L}(g_i^{-1})$ and that $\nu : L_{i'} \to L_i$ is a L-isomorphism. Let $\lambda_i \in \mathcal{D}_{L_i/L}^{-1}$ and $\lambda'_{i'} \in \mathcal{D}_{L_{i'}/L}^{-1}$ be arbitrary. Then

$$\sum_{\omega\in\Omega_L/\mathrm{stab}_{\Omega_L}(g_i)} \omega(\lambda_i)\ {}^{\omega}g_i\,, \qquad \sum_{\omega'\in\Omega_L/\mathrm{stab}_{\Omega_L}(g_{i'})} \omega'(\lambda'_{i'})\ {}^{\omega'}g_{i'}$$

are elements of $\mathcal{B}_L^*$. Hence, also their product lies in $\mathcal{B}_L^*$. In particular the coefficient at $1 \in G$ of this product is an element of $\mathcal{O}_L$:

$$\sum_{\omega\in\Omega_L/\mathrm{stab}_{\Omega_L}(g_i)} \omega(\lambda_i)\,\omega\nu(\lambda'_{i'}) = \mathrm{Tr}_{L_i/L}(\lambda_i\nu(\lambda'_{i'})) \in \mathcal{O}_L\,. \tag{3}$$

If $\lambda'_{i'}$ runs through $\mathcal{D}^{-1}_{L_{i'}/L}$ then $\nu(\lambda'_{i'})$ runs through $\mathcal{D}^{-1}_{L_i/L}$ and (3) implies that $\mathrm{Tr}_{L_i/L}(\mathcal{D}^{-2}_{L_i/L}) \subseteq \mathcal{O}_L$. But this is only possible if $d_{L_i/L} = \mathcal{O}_L$. Since this holds for all $i \in \{1, \ldots, r\}$ we obtain $d_{B_L} = \mathcal{O}_L$. □

Corollary 2.5 *One has* $\mathcal{A}^\circ_L \subseteq \mathcal{B}^*_L$ *and* $[\mathcal{B}^*_L : \mathcal{A}^\circ_L]_{\mathcal{O}_L} = d_{B_L}$.

Proof The inclusion $\mathcal{A}^\circ_L \subseteq \mathcal{B}^*_L$ is clear from Lemma 2.4. Applying $\tilde{\rho}_L$ from Lemma 2.2 (i) we have

$$\begin{aligned}[\mathcal{B}^*_L : \mathcal{A}^\circ_L]_{\mathcal{O}_L} &= \Big[\prod_{i=1}^r \mathcal{D}^{-1}_{L_i/L} : \prod_{i=1}^r \mathcal{O}_{L_i}\Big]_{\mathcal{O}_L} = \prod_{i=1}^r [\mathcal{O}_{L_i} : \mathcal{D}_{L_i/L}]_{\mathcal{O}_L} \\ &= \prod_{i=1}^r d_{L_i/L} = d_{B_L} .\end{aligned}$$

□

We remark that, even for G abelian, $\mathcal{B}^*_L$ is not necessarily contained in $\mathcal{A}_L$.

For the following lemma we assume that G is abelian. Let $L \subseteq L' \subseteq \bar{K}$ be a finite extension field of L containing $L_1, \ldots, L_r$ and $\hat{L}_1, \ldots, \hat{L}_s$ in the notation of Lemma 2.1 and Lemma 2.2. Then $A_{L'} = L'G$, $B_{L'} = \mathrm{Map}(G, L')$, and $A_{L'} \cong \prod_{\chi \in \hat{G}} L'$ via $\rho_{L'}$ as L'-algebras. Such a finite extension L' will be called a *splitting field* for A_L and B_L.

Lemma 2.6 *Let G be abelian. Then*

$$[\mathcal{A}_L : \mathcal{A}^\circ_L]^2_{\mathcal{O}_L} = |G|^{|G|} d_{B_L} d^{-1}_{A_L}$$

for each intermediate field $K \subseteq L \subseteq \bar{K}$.

Proof Let $\mathfrak{p}$ be a non-zero prime ideal of $\mathcal{O}_L$. Since $(\mathcal{A}_L)_\mathfrak{p}$ is the maximal $(\mathcal{O}_L)_\mathfrak{p}$-order in A_L and $(\mathcal{A}^\circ_L)_\mathfrak{p}$ is the set of elements in A_L whose coefficients with respect to G are integral over $(\mathcal{O}_L)_\mathfrak{p}$, we may as well assume that $\mathcal{O}_L$ is local with maximal ideal $\mathfrak{p}$. Let L' be a splitting field for A_L and B_L. We determine

$$[\mathcal{A}_L : \mathcal{A}^\circ_L]^2_{\mathcal{O}_L} \mathcal{O}_{L'} = [\mathcal{O}_{L'} \otimes_{\mathcal{O}_L} \mathcal{A}_L : \mathcal{O}_{L'} \otimes_{\mathcal{O}_L} \mathcal{A}^\circ_L]^2_{\mathcal{O}_{L'}}$$

using the isomorphism $\phi^{L'}_L : L' \otimes_L A_L \to A_{L'}$, the maximal $\mathcal{O}_{L'}$-order $\mathcal{A}_{L'}$ of $A_{L'}$, and the isomorphism $\rho_{L'} : A_{L'} \to \prod_{\chi \in \hat{G}} L'$. More precisely, $[\mathcal{A}_L : \mathcal{A}^\circ_L]_{\mathcal{O}_L} \mathcal{O}_{L'}$ is the quotient of the order ideals

$$\big[\rho_{L'}(\mathcal{A}_{L'}) : (\rho_{L'} \circ \phi^{L'}_L)(\mathcal{O}_{L'} \otimes_{\mathcal{O}_L} \mathcal{A}^\circ_L)\big]^2_{\mathcal{O}_{L'}} \tag{4}$$

and

$$[\rho_{L'}(\mathcal{A}_{L'}) : (\rho_{L'} \circ \phi^{L'}_L)(\mathcal{O}_{L'} \otimes_{\mathcal{O}_L} \mathcal{A}_L)]^2_{\mathcal{O}_{L'}} . \tag{5}$$

For the computation of the order ideal (5) let χ_k, $\hat{L}_k$, $y_{k,l}$, and $\hat{a}_{k,l}$, $1 \leqslant k \leqslant s$, $1 \leqslant l \leqslant s_k$, be given as in Lemma 2.2 such that $y_{k,1}, \ldots, y_{k,s_k}$ is an $\mathcal{O}_L$-basis of $\mathcal{O}_{\hat{L}_k}$ for each $k = 1, \ldots, s$. Then the elements

$$\hat{a}_{k,l} = \sum_{\omega \in \Omega_L/\mathrm{stab}_{\Omega_L}(\chi_k)} \omega(y_{k,l})\, e_{{}^{\omega}\chi_k} \qquad (1 \leqslant k \leqslant s,\ 1 \leqslant l \leqslant s_k)$$

form an $\mathcal{O}_L$-basis of $\mathcal{A}_L$ and $(\rho_{L'} \circ \phi_L^{L'})(\mathcal{O}_{L'} \otimes_{\mathcal{O}_L} \mathcal{A}_L)$ has as $\mathcal{O}_{L'}$-basis the elements

$$\big(\chi(\hat{a}_{k,l})\big)_{\chi \in \hat{G}} \qquad (1 \leqslant k \leqslant s,\ 1 \leqslant l \leqslant s_k)\,.$$

Expressing this basis by the $\mathcal{O}_{L'}$-basis ε_χ, $\chi \in \hat{G}$, of $\rho_{L'}(\mathcal{A}_{L'}) = \prod_{\chi \in \hat{G}} \mathcal{O}_{L'}$, we obtain a block diagonal transition matrix with blocks indexed by $\hat{G}/\Omega_L$. The block belonging to χ_k is given by

$$\Big(\omega(y_{k,l})\Big)_{\substack{l \in \{1,\ldots,s_k\} \\ \omega \in \Omega_L/\mathrm{stab}_{\Omega_L}(\chi_k)}}\,.$$

The square of the determinant of this block generates the $\mathcal{O}_L$-ideal $d_{\hat{L}_k/L}$. Thus, the squared order ideal in (5) is given by

$$\prod_{k=1}^{s} d_{\hat{L}_k/L}\mathcal{O}_{L'} = d_{A_L/L}\mathcal{O}_{L'}\,. \tag{6}$$

For the computation of the squared order ideal (4) let g_i, L_i, $x_{i,j}$, and $a_{i,j}$, $1 \leqslant i \leqslant r$, $1 \leqslant j \leqslant r_i$, be given as in Lemma 2.1 such that $x_{i,1}, \ldots, x_{i,r_i}$ is an $\mathcal{O}_L$-basis of $\mathcal{O}_{L_i}$ for each $i \in \{1, \ldots, r\}$. Then, the elements

$$a_{i,j} = \sum_{\omega \in \Omega_L/\mathrm{stab}_{\Omega_L}(g_i)} \omega(x_{i,j})\, {}^{\omega}g_i \qquad (1 \leqslant i \leqslant r,\ 1 \leqslant j \leqslant r_i)$$

form an $\mathcal{O}_L$-basis of $\mathcal{A}_L^\circ$. Thus, the elements

$$\Big(\sum_{\omega \in \Omega_L/\mathrm{stab}_{\Omega_L}(g_i)} \omega(x_{i,j})\, \chi({}^{\omega}g_i)\Big)_{\chi \in \hat{G}} \qquad (1 \leqslant i \leqslant r,\ 1 \leqslant j \leqslant r_i)$$

form an $\mathcal{O}_{L'}$-basis of $(\rho_{L'} \circ \phi_L^{L'})(\mathcal{O}_{L'} \otimes_{\mathcal{O}_L} \mathcal{A}_L^\circ)$. Expressing this basis by the basis ε_χ, $\chi \in \hat{G}$, of $\rho_{L'}(\mathcal{A}_{L'}) = \prod_{\chi \in \hat{G}} \mathcal{O}_{L'}$, we obtain the transition matrix

$$M = \Big(\sum_{\omega \in \Omega_L/\mathrm{stab}_{\Omega_L}(g_i)} \omega(x_{i,j})\, \chi({}^{\omega}g_i)\Big)_{\substack{(i,j) \\ \chi \in \hat{G}}}$$

which is the product $M = M_1 M_2$ of the block diagonal matrix M_1 with blocks indexed by $i = 1, \ldots, r$, the i-th block given by

$$M_{1,i} = \Big(\omega(x_{i,j})\Big)_{\substack{j \in \{1,\ldots,r_i\} \\ \omega \in \Omega_L/\mathrm{stab}_{\Omega_L}(g_i)}}\,,$$

and the matrix

$$M_2 = \Big(\chi(g)\Big)_{\substack{g\in G\\ \chi\in\hat{G}}} .$$

Now, $\det(M_{1,i})^2$ generates the $\mathcal{O}_L$-ideal $d_{L_i/L}$; thus $\det(M_1)^2\mathcal{O}_L = d_{B_L}$. Moreover, since

$$\sum_{g\in G}\chi_1(g)\,\chi_2(g) = \sum_{g\in G}(\chi_1\chi_2)(g) = \begin{cases}|G|, & \text{if } \chi_1 = \chi_2^{-1},\\ 0, & \text{otherwise,}\end{cases}$$

for $\chi_1, \chi_2 \in \hat{G}$, we have

$$\det(M_2)^2 = \det(M_2^t M_2) = \pm|G|^{|G|} . \tag{7}$$

Altogether this yields

$$\det(M)^2\mathcal{O}_{L'} = |G|^{|G|}d_{B_L}\mathcal{O}_{L'} \tag{8}$$

which expresses the squared order ideal in (4). Now, dividing the ideal in (8) by the ideal in (6), the result follows, since extending $\mathcal{O}_L$-ideals to $\mathcal{O}_{L'}$-ideals is injective. □

Next we investigate under which circumstances $\mathcal{A}_L^\circ$ and (in the abelian case) $\mathcal{A}_L$ are Hopf orders over $\mathcal{O}_L$ in A_L. The crucial point is to get hold of the image of the diagonal.

Since the following might be of general interest we place ourselves for the moment in a more general setting. Let H be a finite group, E/F a field extension in characteristic zero, and $R \subseteq F$ a subring such that F is the field of fractions of R. Suppose that $\mathcal{A} \subseteq EH$ is an R-subalgebra of EH with R-basis $a_1, \dots, a_n$ which is also an E-basis of EH. Then the multiplication map $E \otimes_R \mathcal{A} \to EH$, $\lambda\otimes_R a \mapsto \lambda a$, is an E-algebra isomorphism and the map $\mathcal{A}\otimes_R\mathcal{A} \to EH \otimes_E EH$, $a\otimes_R a' \mapsto a\otimes_E a'$, is injective, so that $\mathcal{A}\otimes_R\mathcal{A}$ can be regarded as an R-subalgebra in $EH \otimes_E EH$. We would like to decide whether $\Delta(\mathcal{A}) \subseteq \mathcal{A}\otimes_R\mathcal{A}$ or not. We write

$$a_i = \sum_{h\in H}\alpha_{i,h}h$$

for $i = 1, \dots, n$ with $\alpha_{i,h} \in E$, and we consider the matrix

$$S := \big(\alpha_{i,h}\big)_{\substack{i\in\{1,\dots,n\}\\ h\in H}} \in \mathrm{GL}_n(E) ,$$

together with its inverse

$$T := S^{-1} = \big(\beta_{h,i}\big)_{\substack{h\in H\\ i\in\{1,\dots,n\}}} .$$

Then we have the following criterion:

Lemma 2.7 *Keeping the above notation, the following assertions are equivalent:*

(i) $\Delta(\mathcal{A}) \subseteq \mathcal{A} \otimes_R \mathcal{A}$.

(ii) $\sum_{h\in H} \alpha_{i,h}\beta_{h,j}\beta_{h,j'} \in R$ *for all* $i, j, j' \in \{1, \dots, n\}$.

Proof We write

$$\Delta(a_i) = \sum_{j,j'=1}^{n} \gamma_{j,j'}^{(i)} a_j \otimes_E a_{j'}$$

with uniquely determined coefficients $\gamma_{j,j'}^{(i)} \in E$. Then, for $i \in \{1, \dots, n\}$, we have $\Delta(a_i) \in \mathcal{A} \otimes_R \mathcal{A}$ if and only if $\gamma_{j,j'}^{(i)} \in R$ for all $j, j' \in \{1, \dots, n\}$. Using the expansion $\Delta(a_i) = \sum_{h\in H} \alpha_{i,h} h \otimes h$, we obtain the equivalent equation

$$\sum_{h\in H} \alpha_{i,h} h \otimes h = \sum_{j,j'=1}^{n} \sum_{h_1,h_2\in H} \gamma_{j,j'}^{(i)} \alpha_{j,h_1}\alpha_{j',h_2} h_1 \otimes h_2 \,.$$

Hence, the coefficients $\gamma_{j,j'}^{(i)}$ are uniquely determined by the system of linear equations

$$\sum_{j,j'} \gamma_{j,j'}^{(i)} \alpha_{j,h_1}\alpha_{j',h_2} = \begin{cases} \alpha_{i,h}, & \text{if } h_1 = h_2 =: h, \\ 0, & \text{if } h_1 \neq h_2, \end{cases}$$

one equation for each $i \in \{1, \dots, n\}$ and each pair $(h_1, h_2) \in H \times H$. Now it is easy to verify that these equations are satisfied for $\gamma_{j,j'}^{(i)} = \sum_{h\in H} \alpha_{i,h}\beta_{h,j}\beta_{h,j'}$, and the result follows. □

In the following proposition we apply Lemma 2.7 to the $\mathcal{O}_L$-order $\mathcal{A}_L^\circ$ in A_L.

Proposition 2.8 *The* $\mathcal{O}_L$*-order* $\mathcal{A}_L^\circ$ *is a Hopf order in* A_L *if and only if* $d_{B_L} = \mathcal{O}_L$.

Proof Clearly, $\mathcal{A}_L^\circ$ is stable under the antipode of A_L. The inclusion $\Delta(\mathcal{A}_L^\circ) \subseteq \mathcal{A}_L^\circ \otimes_{\mathcal{O}_L} \mathcal{A}_L^\circ$ can be tested by localization. Thus we may assume that $\mathcal{O}_L$ is a local ring. In this case we choose g_i, L_i, $x_{i,j}$, and $a_{i,j}$ as in Lemma 2.1 such that, for each $i \in \{1, \dots, r\}$, the elements $x_{i,1}, \dots, x_{i,r_i}$, form an $\mathcal{O}_L$-basis of $\mathcal{O}_{L_i}$. Then the elements $a_{i,j}$, $1 \leqslant i \leqslant r$, $1 \leqslant j \leqslant r_i$, form an $\mathcal{O}_L$-basis of $\mathcal{A}_L^\circ$, and, in the notation introduced before Lemma 2.7, the coefficient matrix S is a block diagonal matrix, the blocks indexed by $i = 1, \dots, r$, and the i-th block given by

$$\big(\omega(x_{i,j})\big)_{\substack{i\in\{1,\dots,r_i\} \\ \omega\in\Omega_L/\mathrm{stab}_{\Omega_L}(g_i)}} \,.$$

If $x^*_{i,1}, \ldots, x^*_{i,r_i} \in L_i$ is a dual basis of $x_{i_1}, \ldots, x_{i,r_i}$ with respect to the trace form $\mathrm{Tr}_{L_i/L}$, then the inverse T of S is given by the block diagonal matrix with the i-th block

$$\big(\omega(x^*_{i,j})\big)_{\substack{\omega\in\Omega_L/\mathrm{stab}_{\Omega_L}(g_i)\\ i\in\{1,\ldots,r_i\}}} .$$

Now, taking into account the block diagonal structure of S and T, Lemma 2.7 states that $\Delta(\mathcal{A}^\circ_L) \subseteq \mathcal{A}^\circ_L \otimes_{\mathcal{O}_L} \mathcal{A}^\circ_L$ if and only if

$$\sum_{\omega\in\Omega_L/\mathrm{stab}_{\Omega_L}(g_i)} \omega(x_{i,j})\,\omega(x^*_{i,j'})\,\omega(x^*_{i,j''}) = \mathrm{Tr}_{L_i/L}(x_{i,j}x^*_{i,j'}x^*_{i,j''}) \in \mathcal{O}_L \qquad (9)$$

for all $i \in \{1, \ldots, r\}$ and all $j', j'' \in \{1, \ldots, r_i\}$. But since $x^*_{i,j}$, $j = 1, \ldots, r_i$, form an $\mathcal{O}_L$-basis of $\mathcal{D}^{-1}_{L_i/L}$, the condition in (9) holds for given $i \in \{1, \ldots, r\}$ and all $j', j'' \in \{1, \ldots, r_i\}$ if and only if $\mathrm{Tr}_{L_i/L}(\mathcal{D}^{-2}_{L_i/L}) \subseteq \mathcal{O}_L$. But this is equivalent to $\mathcal{D}_{L_i/L} = \mathcal{O}_{L_i}$ and to $d_{L_i/L} = \mathcal{O}_L$. Now the result follows. □

Corollary 2.9 *The following statements are equivalent:*
(i) *The order $\mathcal{A}^\circ_L$ is a Hopf order in A_L.*
(ii) *The discriminant ideal d_{B_L} is trivial.*
(iii) *One has $\mathcal{A}^\circ_L = \mathcal{B}^*_L$.*
(iv) *One has $(\mathcal{A}^\circ_L)^* = \mathcal{B}_L$.*
(v) *The maximal order $\mathcal{B}_L$ of B_L is an $\mathcal{O}_L$-Hopf order.*
If (i)–(v) hold then $\mathcal{A}^\circ_L$ is the smallest $\mathcal{O}_L$-Hopf order of A_L.

Proof The equivalence of (i) and (ii) is the content of Proposition 2.8. The statements (ii) and (iii) are equivalent by Corollary 2.5 which states $[\mathcal{B}^*_L : \mathcal{A}^\circ_L] = d_{B_L}$. Obviously, (iii) and (iv) are equivalent, since $\mathcal{O}_L$ is a Dedekind domain. Moreover, (i) and (iv) imply (v). Finally, (v) implies that $\mathcal{B}^*_L$ is an order in A_L, and then Lemma 2.4 implies (ii).

If (i)–(v) hold then $\mathcal{B}_L$ is certainly the largest $\mathcal{O}_L$-Hopf order in B_L. Therefore its dual $\mathcal{A}^\circ_L$ is the smallest $\mathcal{O}_L$-Hopf order in A_L. □

Proposition 2.10 *Let G be abelian. Then the maximal $\mathcal{O}_L$-order $\mathcal{A}_L$ of A_L is a Hopf order if and only if $d_{A_L} = \mathcal{O}_L$.*

Proof Since the antipode S is an L-algebra automorphism of A_L, the maximal $\mathcal{O}_L$-order of A_L is stable under S. As in the proof of Proposition 2.8 we may assume that $\mathcal{O}_L$ is local. Now let χ_k, $\hat{L}_k$, $y_{k,l}$, and $\hat{a}_{k,l}$ be given as in Lemma 2.2 such that, for each $k \in \{1, \ldots, s\}$, the elements $y_{k,1}, \ldots, y_{k,s_k}$ form an $\mathcal{O}_L$-basis of $\mathcal{O}_{\hat{L}_k}$. Then the elements $\hat{a}_{k,l}$, $1 \leqslant k \leqslant s$, $1 \leqslant l \leqslant s_k$, form an $\mathcal{O}_L$-basis of $\mathcal{A}_L$. The matrix S in the notation prededing Lemma 2.7 is given by

$$\frac{1}{|G|}\Big(\sum_{\omega\in\Omega_L/\mathrm{stab}_{\Omega_L}(\chi_k)} \omega(y_{k,l})\,({}^{\omega}\chi_k)(g^{-1})\Big)_{\substack{(k,l)\\ g\in G}} .$$

We can write $S = S_1 S_2$, where S_1 is the block diagonal matrix with blocks indexed by $k = 1, \dots, s$ and whose k-th block is given by

$$S_{1,k} = \Big(\omega(y_{k,l})\Big)_{\substack{l\in\{1,\dots,s_k\} \\ \omega\in\Omega_L/\mathrm{stab}_{\Omega_L}(\chi_k)}},$$

and where

$$S_2 = \frac{1}{|G|}\Big(({}^{\omega}\chi_k)(g^{-1})\Big)_{\substack{(k,\omega)\\ g\in G}}.$$

If, for each $k \in \{1, \dots, s\}$, we denote by $y^*_{k,1}, \dots, y^*_{k,s_k} \in \hat{L}_k$ the dual basis of $y_{k_1}, \dots, y_{k,s_k}$ with respect to $\mathrm{Tr}_{\hat{L}_k/L}$, then

$$T_{1,k} = \Big(\omega(y^*_{k,l})\Big)_{\substack{\omega\in\Omega_L/\mathrm{stab}_{\Omega_L}(\chi_k)\\ l\in\{1,\dots,s_k\}}}$$

is the inverse of $S_{1,k}$. Moreover, by the orthogonality relations of irreducible characters, the inverse of S_2 is given by

$$T_2 = \Big(({}^{\omega}\chi_k)(g)\Big)_{\substack{g\in G\\ (k,\omega)}}.$$

Thus, the inverse of S is given by

$$T = \Big(\sum_{\omega\in\Omega_L/\mathrm{stab}_{\Omega_L}(\chi_k)} \omega(y^*_{k,l})\,({}^{\omega}\chi_k)(g)\Big)_{\substack{g\in G\\ (k,l)}}.$$

Now, Lemma 2.7 states that $\Delta(\mathcal{A}_L) \subseteq \mathcal{A}_L \otimes_{\mathcal{O}_L} \mathcal{A}_L$ if and only if

$$\begin{aligned}
&\frac{1}{|G|}\sum_{g\in G}\sum_{\omega,\omega',\omega''} \omega(y_{k,l})\,({}^{\omega}\chi_k)(g)\,\omega'(y^*_{k',l'})\,({}^{\omega'}\chi_{k'})(g)\,\omega''(y^*_{k'',l''})\,({}^{\omega''}\chi_{k''})(g) = \\
&\quad= \frac{1}{|G|}\sum_{\omega,\omega',\omega''} \omega(y_{k,l})\,\omega'(y^*_{k',l'})\,\omega''(y^*_{k'',l''})\,\sum_{g\in G}({}^{\omega}\chi_k)({}^{\omega'}\chi_{k'})({}^{\omega''}\chi_{k''})(g) \in \mathcal{O}_L
\end{aligned}$$

for all pairs (k,l), (k',l'), (k'',l''), where the triple sum runs independently over all $\omega \in \Omega_L/\mathrm{stab}_{\Omega_L}(\chi_k)$, $\omega' \in \Omega_L/\mathrm{stab}_{\Omega_L}(\chi_{k'})$, and $\omega'' \in \Omega_L/\mathrm{stab}_{\Omega_L}(\chi_{k''})$. By the orthogonality relations of irreducible characters the last sum over $g \in G$ reduces to $|G|$ if $({}^{\omega}\chi_k)({}^{\omega'}\chi_{k'})({}^{\omega''}\chi_{k''}) = 1$ and vanishes otherwise. If $d_{A_L} = \mathcal{O}_L$ then $y^*_{k,l} \in \mathcal{O}_{\hat{L}_k}$ for all pairs (k,l), and the above condition is certainly satisfied. Conversely, if the above condition is satisfied, then we choose $k' \in \{1, \dots, s\}$ arbitrarily and remark that $\mathrm{stab}_{\Omega_L}(\chi_{k'}) = \mathrm{stab}_{\Omega_L}(\chi_{k'}^{-1})$. Let $k'' \in \{1, \dots, s\}$ and $\kappa \in \Omega_L$ be such that $\chi_{k'}^{-1} = {}^{\kappa}\chi_{k''}$. Moreover let $k \in \{1, \dots, s\}$ be such that $\chi_k = 1$. Then $\hat{L}_k = L$ and the above sum reduces further to

$$\begin{aligned}
&\sum_{\omega',\omega''} \omega'(y^*_{k',l'})\,\omega''(y^*_{k'',l''})\,\delta_{{}^{\omega'}\chi_{k'}\,{}^{\omega''}\chi_{k''},1} = \\
&\qquad= \sum_{\omega'} \omega'(y^*_{k',l'})\,\omega'\kappa(y^*_{k'',l''}) = \mathrm{Tr}_{\hat{L}_{k'}/L}\big(y^*_{k',l'}\,\kappa(y^*_{k'',l''})\big),
\end{aligned}$$

since ${}^{\omega'}\chi_{k'}\, {}^{\omega''}\chi_{k''} = 1$ if and only if $\omega'' = \omega'\kappa$. The elements $\kappa(y_{k'',1}), \ldots, \kappa(y_{k'',s_{k''}})$ form an $\mathcal{O}_L$-basis of $\kappa(\mathcal{D}^{-1}_{\hat{L}_{k''}/L}) = \mathcal{D}^{-1}_{\hat{L}_{k'}/L}$. Since the last term in the above equation lies in $\mathcal{O}_L$ for all l' and l'', we have $\mathrm{Tr}_{\hat{L}_{k'}/L}(\mathcal{D}^{-2}_{\hat{L}_{k'}/L}) \subseteq \mathcal{O}_L$. But this implies $d_{\hat{L}_{k'}/L} = \mathcal{O}_L$. This holds for all $k' \in \{1, \ldots, s\}$. Thus $d_{A_L} = \mathcal{O}_L$. □

2.4 Some A-modules and resolvents

Let $\mathbf{C} := \mathrm{Map}(\Gamma, \bar{K})$ be the $\bar{K}$-algebra with pointwise multiplication. Then, Ω acts on $\mathbf{C}$ via K-algebra automorphisms by

$$({}^{\omega}f)(\gamma) := \omega\big(f({}^{\omega^{-1}}\gamma)\big)\,,$$

for $\omega \in \Omega$, $f \in \mathbf{C}$, $\gamma \in \Gamma$. For an intermediate field $K \subseteq L \subseteq \bar{K}$ let

$$C_L := \mathbf{C}^{\Omega_L} = \mathrm{Map}(\Gamma, \bar{K})^{\Omega_L}$$

be th L-algebra of Ω_L-fixed points of $\mathbf{C}$. Moreover, let $\mathcal{C}_L$ be the maximal $\mathcal{O}_L$-order of C_L. Thus,

$$\mathcal{C}_L = \mathrm{Map}(\Gamma, \mathcal{O}_{\bar{K}})^{\Omega_L}\,.$$

Note that $\mathbf{C}$ is a right $\mathbf{A}$-module via the G-action on Γ:

$$\big(f \cdot (\sum_{g \in G} \lambda_g g)\big)(\gamma) := \sum_{g \in G} \lambda_g f({}^{g}\gamma) \tag{10}$$

for $\lambda_g \in \bar{K}$, $f \in \mathbf{C}$, $\omega \in \Omega$. This action of $\mathbf{A}$ on $\mathbf{C}$ satisfies

$${}^{\omega}(f \cdot a) = ({}^{\omega}f) \cdot ({}^{\omega}a)$$

for all $a \in \mathbf{A}$, $f \in \mathbf{C}$, $\omega \in \Omega$. Thus, the $\mathbf{A}$-module structure on $\mathbf{C}$ restricts to an A_L-module structure on C_L for any intermediate field $K \subseteq L \subseteq \bar{K}$. Moreover, as apparent from (10), $\mathcal{C}_L$ is an $\mathcal{A}^{\circ}_L$-module by restriction.

Similar to Lemma 2.3 for the algebra $\mathbf{B}$ we have the following lemma for $\mathbf{C}$.

Lemma 2.11 *Let $K \subseteq L \subseteq \bar{K}$ be an intermediate field, and let $\gamma_1, \ldots, \gamma_t \in \Gamma$ be a set of representatives for the Ω_L-orbits of Γ. For each $m \in \{1, \ldots, t\}$ let $\tilde{L}_m$ denote the fixed field of $\mathrm{stab}_{\Omega_L}(\gamma_m) \leqslant \Omega_L$, and let $z_{m,1}, \ldots, z_{m,t_m}$ be an L-basis of $\tilde{L}_m$. For $1 \leqslant m \leqslant t$ and $1 \leqslant n \leqslant t_m$, let $c_{m,n} \in \mathbf{C}$ be defined by*

$$c_{m,n}(\gamma) := \begin{cases} \omega(z_{m,n}), & \text{if } \gamma = {}^{\omega}\gamma_m \text{ for some } \omega \in \Omega_L, \\ 0, & \text{otherwise,} \end{cases}$$

for $\gamma \in \Gamma$. Assume that $L \subseteq M \subseteq N \subseteq \bar{K}$ are further intermediate fields. Then the following assertions hold:

(i) *The map*

$$\tau\colon C_L \simeq \prod_{m=1}^{t} \tilde{L}_m\,, \quad f \mapsto \big(f(\gamma_m)\big)\,,$$

is an L-algebra isomorphism. In particular, τ restrict to an isomorphism

$$\tau_L\colon \mathcal{C}_L \simeq \prod_{m=1}^{t} \mathcal{O}_{\tilde{L}_m}\,.$$

(ii) *The elements $c_{m,n}$, $1 \leqslant m \leqslant t$, $1 \leqslant n \leqslant t_m$, form an L-basis of C_L. If, for each $m \in \{1, \dots, t\}$, the elements $z_{m,1}, \dots, z_{m,t_m}$ form an $\mathcal{O}_L$-basis of $\mathcal{O}_{\tilde{L}_m}$, then the elements $c_{m,n}$, $1 \leqslant m \leqslant t$, $1 \leqslant n \leqslant t_m$, form an $\mathcal{O}_L$-basis of $\mathcal{C}_L$.*

(iii) *One has $\dim_L(C_L) = |G|$.*

(iv) *The elements $c_{m,n}$, $1 \leqslant m \leqslant t$, $1 \leqslant n \leqslant t_m$, form an M-basis of C_M.*

(v) *The map*

$$\pi_L^M\colon M \otimes_L C_L \to C_M\,, \quad \lambda \otimes_L c \mapsto \lambda c\,,$$

is an isomorphism of M-algebras such that the diagrams

$$\begin{tikzcd}
M \otimes_L C_L \arrow[r, "\pi_L^M"] \arrow[d, "\omega\otimes\omega"'] & C_M \arrow[d, "\omega"] \\
\omega(M) \otimes_{\omega(L)} C_{\omega(L)} \arrow[r, "\pi_{\omega(L)}^{\omega(M)}"] & C_{\omega(M)}
\end{tikzcd}
\qquad
\begin{tikzcd}
N \otimes_M M \otimes_L C_L \arrow[r, "N\otimes\pi_L^M"] \arrow[d, "\mathrm{can}\otimes C_L"'] & N \otimes_M C_M \arrow[d, "\pi_M^N"] \\
N \otimes_L C_L \arrow[r, "\pi_L^N"] & C_N
\end{tikzcd}$$

commute for all $\omega \in \Omega$.

Proof All assertions are proved in a similar way as the analogous assertions of Lemma 2.3. □

Next we show that the L-algebra C_L is an A_L-Galois extension in the sense of [CS]. Let us shortly recall the relevant notions in a general setting.

Let R be a commutative ring, let H be an R-Hopf algebra which is finitely generated and projective as R-module. Furthermore, let S be a commutative R-algebra, finitely generated and projective as R-module, which is also a right H-module. Then S is called an *H-Galois extension* of R if and only if the following conditions are satisfied:

(G1) (i) $(st) \cdot h = \sum_{(h)} (s \cdot h_{(1)})(t \cdot h_{(2)})\,,$
(ii) $1_S \cdot h = \epsilon(h) 1_S\,,$
for all $h \in H$, $s, t \in S$, where $\Delta(h) = \sum_{(h)} h_{(1)} \otimes h_{(2)}$ is the Sweedler notation and the module structure of S over H is denoted by a dot.

(G2) The map

$$H \otimes_R S \to \mathrm{Hom}_R(S,S)\,, \quad h \otimes_R s \mapsto \big(t \mapsto (t \cdot h)s\big)\,,$$

is an isomorphism.

In fact, it is well-known that (G1) is equivalent to S being an H^*-object, and that (G2) is equivalent to the condition that the H^*-object S is a Galois H^*-object in the terminology of [CS, §7].

Proposition 2.12 *Let $K \subseteq L \subseteq \bar{K}$ be an intermediate field. Then the L-algebra C_L is an A_L-Galois extension of L. Moreover, if G is abelian, then C_L is a free A_L-module of rank 1.*

Proof It suffices to verify (G1) in the case $L = \bar{K}$. So let $g \in G$, $f, f' \in \mathbf{C}$, and $\gamma \in \Gamma$. Then

$$\begin{aligned}((ff')\cdot g)(\gamma) &= (ff'({}^g\gamma) = f({}^g\gamma)f'({}^g\gamma) = (f\cdot g)(\gamma)(f'\cdot g)(\gamma)\\ &= \big((f\cdot g)(f'\cdot g)\big)(\gamma)\,,\end{aligned}$$

thus, $(ff')\cdot g = (f\cdot g)(f'\cdot g)$ which is the statement in (G1) (i). Moreover, $(1_{\mathbf{C}}\cdot g)(\gamma) = 1_{\mathbf{C}}({}^g\gamma) = 1 = 1_{\mathbf{C}}(\gamma)$, for all $\gamma \in \Gamma$. Hence, also (G1) (ii) holds.

In order to prove (G2), we use Lemma 2.1 (vi) and Lemma 2.11 (v) to reduce the assertion to the case $L = \bar{K}$. Moreover, by Lemma 2.1 (ii) and Lemma 2.11 (iii), it suffices to show that the map in (G2) is injective. So let $\sum_{g\in G} g \otimes f_g \in \mathbf{A} \otimes_{\bar{K}} \mathbf{C}$ with arbitrarily chosen $f_g \in \mathbf{C}$ for $g \in G$ such that it vanishes under the map in (G2). Then

$$\sum_{g\in G} f({}^g\gamma)f_g(\gamma) = 0\,, \quad \text{for all } f \in \mathbf{C} \text{ and all } \gamma \in \Gamma\,. \tag{11}$$

Let $g_0 \in G$ and $\gamma \in \Gamma$. Then, choosing $f \in \mathbf{C}$ in such a way that $f({}^{g_0}\gamma) = 1$ and $f(\gamma') = 0$ for $\gamma' \neq {}^{g_0}\gamma$, the equation in (11) implies $f_{g_0}(\gamma) = 0$. Thus $f_{g_0} = 0$ for all $g_0 \in G$. This shows that C_L is an A_L-Galois extension of L.

If G is abelian, A_L is commutative and B_L is cocommutative. By [CH, Prop. 2.3, Thm. 3.1], C_L and B_L are isomorphic as A_L-modules, where the A_L-module structure of B_L is given by $(b\cdot\sum_{g\in G}\lambda_g g)(g') := \sum_{g\in G}\lambda_g b(gg')$ for all $b \in B_L$, $g' \in G$. Moreover, A_L and B_L are isomorphic as A_L-modules by sending 1_{A_L} to the element $l_1 \in B_L$ with $l_1(g) = \delta_{g,1}$. □

Let G be abelian. Since C_L is free over A_L for any intermediate field $K \subset L \subset \bar{K}$, the following question arises naturally: Is $\mathcal{C}_L$ free over some $\mathcal{O}_L$-order in A_L. It is well-known that, if this is the case, it is only possible for the *associated order*

$$\mathcal{A}_L^{\mathrm{ass}} := \{a \in A_L \mid \mathcal{C}_L \cdot a \subseteq \mathcal{C}_L\}$$

of $\mathcal{C}_L$ in A_L. Obviously, $\mathcal{A}_L^\circ \subseteq \mathcal{A}_L^{\mathrm{ass}} \subseteq \mathcal{A}_L$. We will prove in the following chapters that in many of the examples described in 1.1 the module $\mathcal{C}_L$ is free over $\mathcal{A}_L^{\mathrm{ass}}$. In the proofs we make use of the *resolvent*

$$(f,\chi)_{\gamma_0} := \sum_{g\in G} f({}^g\gamma_0)\chi(g^{-1}) \in \bar{K} \tag{12}$$

attached to $f \in \mathbf{C}$ and $\chi \in \hat{G}$ for fixed $\gamma_0 \in \Gamma$.

For an intermediate field $K \subseteq L \subseteq \bar{K}$, let $L' \subseteq \bar{K}$ now denote a finite extension of L such that $\Omega_{L'}$ acts trivially on $\hat{G}$ and Γ. We call such a field a *splitting field* for A_L and C_L. Note that, since

$$\omega\big((f,\chi)_{\gamma_0}\big) = ({}^\omega f, {}^\omega\chi)_{{}^\omega\gamma_0}\ ,$$

for all $\omega \in \Omega$, $f \in \mathbf{C}$, $\chi \in \hat{G}$, and $\gamma_0 \in \Gamma$, we then have $(f,\chi)_{\gamma_0} \in L'$ for all $f \in C_L$, $\chi \in \hat{G}$, and $\gamma_0 \in \Gamma$. We denote by d_{C_L} the discriminant ideal of $\mathcal{C}_L$ over $\mathcal{O}_L$. Thus, in the notation of Proposition 2.11 we have $d_{C_L} = \prod_{m=1}^t d_{\tilde{L}_m/L}$.

Proposition 2.13 *Assume that G is abelian and fix $\gamma_0 \in \Gamma$. Let $K \subseteq L \subseteq \bar{K}$ be an intermediate field, let $L \subseteq L' \subseteq \bar{K}$ be a splitting field for A_L and C_L, and let $f \in C_L$. Then $f \cdot A_L = C_L$ if and only if $(f,\chi)_{\gamma_0} \neq 0$ for all $\chi \in \hat{G}$. Moreover, if $f \cdot A_L = C_L$ then*

$$[\mathcal{C}_L : f\cdot\mathcal{A}_L^\circ]^2_{\mathcal{O}_L}\mathcal{O}_{L'} = d_{B_L} d_{C_L}^{-1} \prod_{\chi\in\hat{G}} (f,\chi)^2_{\gamma_0}\mathcal{O}_{L'}\ .$$

Proof (a) Let χ_k, $\hat{L}_k$, $y_{k,l}$, and the L-basis

$$\hat{a}_{k,l} = \sum_{\omega\in\Omega_L/\mathrm{stab}_{\Omega_L}(\chi_k)} \omega(y_{k,l})\,{}^\omega e_\chi \qquad (1 \leqslant k \leqslant s,\ 1 \leqslant l \leqslant s_k) \tag{13}$$

of A_L be given as in Lemma 2.2. Then the elements

$$\big((f\cdot\hat{a}_{k,l})(\gamma)\big)_{\gamma\in\Gamma} \in \prod_{\gamma\in\Gamma} L' \tag{14}$$

generate $(\tau_{L'}\circ\pi_L^{L'})(L'\otimes_L f\cdot A_L) \subseteq \prod_{\gamma\in\Gamma} L'$ over L'. We express these generators by the primitive idempotents ε_γ, $\gamma \in \Gamma$, of $\prod_{\gamma\in\Gamma} L'$and obtain a transition matrix

$$M = \big((f\cdot\hat{a}_{k,l})(\gamma)\big)_{\substack{(k,l)\\ \gamma\in\Gamma}} = \big((f\cdot\hat{a}_{k,l})({}^g\gamma_0)\big)_{\substack{(k,l)\\ g\in G}}\ ,$$

so that $f \cdot A_L = C_L$ if and only if $\det(M) \neq 0$. We determine $\det(M)$. For the entry of M we have

$$\begin{aligned}
(f\cdot\hat{a}_{k,l})({}^{g}\gamma_0) &= \frac{1}{|G|}\sum_{\omega\in\Omega_L/\mathrm{stab}_{\Omega_L}(\chi_k)}\ \sum_{g'\in G}\omega(y_{k,l})\,({}^{\omega}\chi_k)(g'^{-1})f({}^{g'g}\gamma_0)\\
&= \frac{1}{|G|}\sum_{\omega\in\Omega_L/\mathrm{stab}_{\Omega_L}(\chi_k)}\ \sum_{h\in G}\omega(y_{k,l})\,({}^{\omega}\chi_k)(gh^{-1})f({}^{h}\gamma_0)\\
&= \frac{1}{|G|}\sum_{\omega\in\Omega_L/\mathrm{stab}_{\Omega_L}(\chi_k)}\omega(y_{k,l})\,(f,{}^{\omega}\chi_k)_{\gamma_0}({}^{\omega}\chi_k)(g)\,.
\end{aligned}$$

We can write M as $M = M_1M_2$, where M_1 is a block diagonal matrix, the blocks $M_{1,k}$ indexed by $k=1,\ldots,s$, with

$$M_{1,k} = \big(\omega(y_{k,l})\big)_{\substack{l\in\{1,\ldots,s_k\}\\ \omega\in\Omega_L/\mathrm{stab}_{\Omega_L}(\chi_k)}}\,,$$

and where

$$M_2 = \frac{1}{|G|}\Big((f,{}^{\omega}\chi_k)_{\gamma_0}({}^{\omega}\chi_k)(g)\Big)_{\substack{k,\omega\in\Omega_L/\mathrm{stab}_{\Omega_L}(\chi_k)\\ g\in G}} = \frac{1}{|G|}\Big((f,\chi)_{\gamma_0}\chi(g)\Big)_{\substack{\chi\in\hat{G}\\ g\in G}}\,.$$

Now, $\det(M_{1,k})^2\mathcal{O}_L = d_{\hat{L}_k/L}$, hence $\det(M_1)^2\mathcal{O}_L = d_{A_L/L}$. Moreover,

$$\det(M_2)^2 = \left(\prod_{\chi\in\hat{G}}(f,\chi)^2_{\gamma_0}\right)|G|^{-2|G|}\det\big(\chi(g)\big)^2_{\substack{\chi\in\hat{G}\\ g\in G}} = \pm\left(\prod_{\chi\in\hat{G}}(f,\chi)^2_{\gamma_0}\right)|G|^{-|G|}$$

by (7). Thus,

$$\det(M)^2\mathcal{O}_{L'} = d_{A_L}|G|^{-|G|}\prod_{\chi\in\hat{G}}(f,\chi)^2_{\gamma_0}\mathcal{O}_{L'}\,. \tag{15}$$

This shows that $f\cdot A_L = C_L$ if and only if $(f,\chi)_{\gamma_0}\neq 0$ for all $\chi\in\hat{G}$.

(b) Next we show the assertion about $[\mathcal{C}_L : f\cdot\mathcal{A}_L^{\circ}]_{\mathcal{O}_L}$. Since both sides of the equation behave well under localization, we may assume that $\mathcal{O}_L$ is local. We transport the two $\mathcal{O}_{L'}$-lattices $\mathcal{O}_{L'}\otimes_{\mathcal{O}_L}\mathcal{C}_L$ and $\mathcal{O}_{L'}\otimes_{\mathcal{O}_L} f\cdot\mathcal{A}_L^{\circ}$ by the isomorphism $\tau_{L'}\circ\pi_L^{L'}$ into $\prod_{\gamma\in\Gamma}L'$.

Retracing the calculations in (a) one observes that, if $y_{k,1},\ldots,y_{k,s_k}$ is an $\mathcal{O}_L$-basis of $\mathcal{O}_{\hat{L}_k}$, for each $k=1,\ldots,s$, then the elements (13) form an $\mathcal{O}_L$-basis of $\mathcal{A}_L$, and the elements in (14) form an $\mathcal{O}_{L'}$-basis of $(\tau_{L'}\circ\pi_L^{L'})(\mathcal{O}_{L'}\otimes_{\mathcal{O}_L} f\cdot\mathcal{A}_L)$. Thus, the calculation in (a) shows that

$$\big[\tau_{L'}(\mathcal{C}_{L'}) : (\tau_{L'}\circ\pi_L^{L'})(\mathcal{O}_{L'}\otimes_{\mathcal{O}_L} f\cdot\mathcal{A}_L)\big]^2_{\mathcal{O}_{L'}} = d_{A_L}|G|^{-|G|}\prod_{\chi\in\hat{G}}(f,\chi)^2_{\gamma_0}\mathcal{O}_{L'}\,. \tag{16}$$

Moreover, we already know from Proposition 2.6 that

$$[f\cdot\mathcal{A}_L : f\cdot\mathcal{A}_L^\circ]^2_{\mathcal{O}_L} = [\mathcal{A}_L : \mathcal{A}_L^\circ]^2_{\mathcal{O}_L} = d_{B_L} d_{A_L}^{-1} |G|^{|G|}\,. \tag{17}$$

Now, it suffices to show that

$$\left[\tau(\mathcal{C}_{L'}) : (\tau_{L'}\circ\pi_L^{L'})(\mathcal{O}_{L'}\otimes_{\mathcal{O}_L}\mathcal{C}_L)\right]^2_{\mathcal{O}_{L'}} = d_{C_L}\mathcal{O}_{L'}\,, \tag{18}$$

since then, dividing the product of (16) and (17) by (18) yields the result.

Let γ_m, $\tilde{L}_m$, $z_{m,n}$, and $c_{m,n}$ be given as in Lemma 2.11 such that, for each $m\in\{1,\dots,t\}$, the elements $z_{m,1},\dots,z_{m,t_m}$ form an $\mathcal{O}_L$-basis of $\mathcal{O}_{\tilde{L}_m}$. Then, the elements $c_{m,n}$, $1\leqslant m\leqslant t$, $1\leqslant n\leqslant t_m$, form an $\mathcal{O}_L$-basis of $\mathcal{C}_L$. Thus, the elements $(\tau_{L'}\circ\pi_L^{L'})(c_{m,n})$ form an $\mathcal{O}_{L'}$-basis of $(\tau_{L'}\circ\pi_L^{L'})(\mathcal{O}_{L'}\otimes_{\mathcal{O}_L}\mathcal{C}_L)$. We express this $\mathcal{O}_{L'}$-basis by the canonical $\mathcal{O}_{L'}$-basis of primitive idempotents ε_γ, $\gamma\in\Gamma$, of $\prod_{\gamma\in\Gamma}\mathcal{O}_{L'}$ and obtain a transition matrix M. This is a block diagonal matrix with blocks $M_1,\dots,M_t$, where

$$M_m = \big(\omega(z_{m,n})\big)_{\substack{n\in\{1,\dots,t_m\}\\ \omega\in\Omega_L/\mathrm{stab}_{\Omega_L}(\gamma_m)}}$$

for $m\in\{1,\dots,t\}$. Since $\det(M_m)^2\mathcal{O}_L = d_{\tilde{L}_m/L}$, we obtain (18), and the proof is complete. □

As an immediate consequence of Proposition 2.13 we obtain:

Corollary 2.14 *In the situation of Proposition 2.13 with $f\in\mathcal{C}_L$ such that $(f,\chi)_{\gamma_0}\neq 0$ for all $\chi\in\hat{G}$ one has*

$$[\mathcal{C}_L : f\cdot\tilde{\mathcal{A}}_L]^2_{\mathcal{O}_L}\mathcal{O}_{L'} = d_{B_L} d_{C_L}^{-1}[\tilde{\mathcal{A}}_L : \mathcal{A}_L^\circ]^{-2}_{\mathcal{O}_L}\prod_{\chi\in\hat{G}}(f,\chi)^2_{\gamma_0}\mathcal{O}_{L'}$$

for each $\mathcal{O}_L$-order $\tilde{\mathcal{A}}_L$ of A_L contained in $\mathcal{A}_L^{\mathrm{ass}}$. In particular, if $f\in\mathcal{C}_L$ is such that

$$[\tilde{\mathcal{A}}_L : \mathcal{A}_L^\circ]^2_{\mathcal{O}_L} d_{C_L}\mathcal{O}_{L'} = d_{B_L}\prod_{\chi\in\hat{G}}(f,\chi)^2_{\gamma_0}\mathcal{O}_{L'}\,,$$

then $\mathcal{C}_L = f\cdot\tilde{\mathcal{A}}_L$ is a free $\tilde{\mathcal{A}}_L$-module of rank one with basis $\{f\}$, and consequently, $\tilde{\mathcal{A}}_L = \mathcal{A}_L^{\mathrm{ass}}$.

□

To conclude this chapter we consider the case $G=\Gamma$. Then $C_L = B_L$ for any intermediate field $K\subseteq L\subseteq\bar{K}$. We define a map $l\in C_L$ by

$$l(g) = \begin{cases} 1, & \text{if } g=1,\\ 0, & \text{if } g\neq 1\end{cases} \tag{19}$$

Corollary 2.15 *Let $G=\Gamma$. Then $\mathcal{A}_L^{\mathrm{ass}} = \mathcal{A}_L^\circ$ and $\mathcal{C}_L$ is a free $\mathcal{A}_L^\circ$-module of rank one with basis $\{l\}$, where l is defined in (19).*

Proof We fix $\gamma_0=1$. Then $(l,\chi)_{\gamma_0}=1$ for all $\chi\in\hat{G}$. Thus the corollary is an immediate consequence of the second part of Corollary 2.14. □

3 The cyclotomic case

This section mainly serves as a motivation and a guide-line for the applications to Lubin-Tate formal groups and elliptic curves.

3.1 First proof

Let $r, m \in \mathbb{N}_0$, $m \geq 1$, and let p be a rational prime number. Fix a primitive p^r-th root of unity ζ_{p^r}, let $G = \mu_{p^m}$ be the group of p^m-th roots of unity and let Γ be the set of p^m-th roots of ζ_{p^r},

$$\Gamma = \{\gamma \in \bar{\mathbb{Q}} \mid \gamma^{p^m} = \zeta_{p^r}\}.$$

We consider $\mathbb{Q}(\zeta_{p^r})$ as our base field and set

$$K = \mathbb{Q}(\zeta_{p^r}), \quad \Omega = \Omega_K, \quad L = \mathbb{Q}(\zeta_{p^{r+m}}),$$

where $\zeta_{p^{r+m}}$ is a primitive p^{r+m}-th root of unity such that $\zeta_{p^{r+m}}^{p^m} = \zeta_{p^r}$. Then G acts simply transitive on Γ,

$$\Gamma = \{g \cdot \zeta_{p^{r+m}} \mid g \in G\},$$

and Ω acts on G and Γ such that ${}^{\omega}(g \cdot \gamma) = {}^{\omega}g\, {}^{\omega}\gamma$ for all $\omega \in \Omega$, $g \in G$ and $\gamma \in \Gamma$. Following Section 1 we set

$$A = (\bar{K}G)^{\Omega}, \quad B = \mathrm{Map}(G, \bar{K})^{\Omega}, \quad C = \mathrm{Map}(\Gamma, \bar{K})^{\Omega}.$$

As an immediate consequence of Lemma 2.11 we obtain an isomorphism τ,

$$\begin{array}{rcl} \tau : C & \longrightarrow & \mathbb{Q} \oplus \mathbb{Q}(\zeta_p) \oplus \dots \mathbb{Q}(\zeta_{p^m}), \\ f & \longmapsto & (f(1), f(\zeta_p), \dots, f(\zeta_{p^m})), \end{array} \quad \text{if } r = 0, \tag{20}$$

and

$$\begin{array}{rcl} \tau : C & \longrightarrow & L = \mathbb{Q}(\zeta_{p^{r+m}}), \\ f & \longmapsto & f(\zeta_{p^{r+m}}), \end{array} \quad \text{if } r \geq 1. \tag{21}$$

We first have a closer look at the more interesting case $r \geq 1$. Via τ we endow L with the structure of an A-module. In the sequel we will always write $G = \{g_k = \zeta_{p^m}^k \mid k \in \mathbb{Z}/p^m\mathbb{Z}\}$. Let $a = \sum_{k=0}^{p^m-1} a_k g_k \in A$ and $f \in C$. Then

$$\begin{aligned} \tau\left(f \cdot \sum_{k=0}^{p^m-1} a_k g_k\right) &= \sum_{k=0}^{p^m-1} a_k f\left(\zeta_{p^{r+m}}^{1+p^r k}\right) \\ &= \sum_{k=0}^{p^m-1} a_k f\left(\zeta_{p^{r+m}}\right)^{\sigma(1+p^r k)}, \end{aligned}$$

where $\sigma(1+p^r k)$ denotes the Artin symbol. Thus the A-module structure of L is explicitly given by

$$\alpha \cdot \sum_{k=0}^{p^m-1} a_k g_k = \sum_{k=0}^{p^m-1} a_k \alpha^{\sigma(1+p^r k)} \tag{22}$$

for $\alpha \in L$, $\sum_{k=0}^{p^m-1} a_k g_k \in A$.

Note that the map

$$\begin{array}{rcl} \mathbb{Z}/p^m\mathbb{Z} & \longrightarrow & \mathrm{Gal}(L/K), \\ k + p^m\mathbb{Z} & \longmapsto & \sigma(1+p^r k) \end{array}$$

is a bijection. In addition, if $m \leq r$, then it is also a homomorphism of groups, since then $\sigma(1+p^r k_1)\sigma(1+p^r k_2) = \sigma(1+p^r(k_1+k_2))$ for $k_1, k_2 \in \mathbb{Z}$. Moreover, $A = KG$ in this case, and identifying G and $\mathrm{Gal}(L/K)$ via $g_k \mapsto \sigma(1+p^r k)$ the new module structure defined in (22) is nothing else but the usual $K\mathrm{Gal}(L/K)$-module structure. However, if $m > r$, then the new structure does not coincide with the classical Galois module structure. But from a geometric point of view it is nevertheless very natural.

For $r \geq 1$ we shall always identify C and L via τ; in particular we write $c_x = \tau^{-1}(x)$ for $x \in L$. For $r = 0$ we define a map $l \in C$ by

$$l(\gamma) = \begin{cases} 1, & \text{if } \gamma = 1, \\ 0, & \text{if } \gamma \neq 1. \end{cases} \tag{23}$$

Recall also that $\mathcal{A}^\circ = (\mathcal{O}_{\bar{K}} G)^\Omega$.

Our aim is to study the integral closure $\mathcal{C}$ of $\mathcal{O}_K$ in C as a module over its associated order $\mathcal{A}^{\mathrm{ass}} = \{a \in A \mid \mathcal{C} \cdot a \subseteq \mathcal{C}\}$.The main result of this Section reads as follows:

Theorem 3.1 *(i) Let $r = 0$. Then $\mathcal{A}^{\mathrm{ass}} = \mathcal{A}^\circ$and $\mathcal{C}$ is free of rank one over $\mathcal{A}^{\mathrm{ass}}$. An explicit generator is given by the map l defined in (23).*

(ii) Let $r \geq 1$. Then $\mathcal{A}^{\mathrm{ass}}$ is equal to the unique maximal order $\mathcal{A} \subseteq A$ and $\mathcal{C}$ is free of rank one over $\mathcal{A}^{\mathrm{ass}}$. An explicit generator is given by the map c_θ, where $\theta = \frac{1-\zeta_{p^r}}{1-\zeta_{p^{r+m}}}$.

Since this section should serve as a motivation on the one hand and a guideline for further applications on the other hand we will give two proofs of Theorem 3.1. The first one is quite short and completely elementary, but has the disadvantage that it does not carry over to applications to Lubin-Tate formal groups or elliptic curves. The second one may appear to be artificial, but it is more structural and based on geometric properties which are shared by the cyclotomic example and the examples concerning Lubin-Tate groups and elliptic curves.

First proof of Theorem 3.1 (i) This is exactly the assertion of Corollary 2.15.

(ii) We claim that Ω acts trivially on $\hat{G}$. The action of Ω obviously factors through $\Omega_{\mathbb{Q}(\zeta_{p^m})}$. Thus the claim is certainly true for $m \leq r$. For $m > r$ every Galois automorphism ω of $\mathbb{Q}(\zeta_{p^m})/\mathbb{Q}(\zeta_{p^r})$ is of the form $\omega = \sigma(1+p^r x)$ with $x \in \mathbb{Z}$. Then $\omega^{-1} = \sigma(1+p^r y)$ with $y \in \mathbb{Z}$ such that

$$(1+p^r x)(1+p^r y) \equiv 1 (\mathrm{mod}\ p^m).$$

Let $\chi \in \hat{G}$ be defined by $\chi(g_1) = \zeta_{p^m}^s$, $s \in \mathbb{Z}$. Then ${}^{\omega}\chi = \chi$ because of

$$\begin{aligned} & ({}^{\omega}\chi)(g_1) = \omega(\chi(\omega^{-1}(g_1)) = \sigma(1+p^r x)\big(\chi(\sigma(1+p^r y)\zeta_{p^m}\big) \\ = \;& \sigma(1+p^r x)\left(\chi(\zeta_{p^m}^{1+p^r y})\right) = \sigma(1+p^r x)\left(\zeta_{p^m}^{(1+p^r y)s}\right) \\ = \;& \zeta_{p^m}^{(1+p^r x)(1+p^r y)s} = \zeta_{p^m}^s . \end{aligned}$$

As a consequence of Lemma 2.2 the K-algebra A splits completely over K and the idempotents e_χ, $\chi \in \hat{G}$, form a $\mathbb{Z}$-basis of the maximal order $\mathcal{A}$.

Via the ismorphism τ of (21) the order $\mathcal{C}$ identifies with $\mathcal{O}_L = \mathcal{O}_K[\zeta_{p^{r+m}}]$. Let $\chi \in \hat{G}$ be uniquely defined by $\chi(g_1) = \zeta_{p^m}^s$, $0 \leq s \leq p^m - 1$. Using (22) we derive for $0 \leq j \leq p^m - 1$

$$\begin{aligned} \zeta_{p^{r+m}}^j \cdot e_\chi &= \frac{1}{p^m} \sum_{k=0}^{p^m-1} \chi(g_k^{-1}) \zeta_{p^{r+m}}^{j\sigma(1+p^r k)} \\ &= \frac{1}{p^m} \sum_{k=0}^{p^m-1} \zeta_{p^m}^{k(j-s)} \zeta_{p^{r+m}}^j = \begin{cases} \zeta_{p^{r+m}}^j, & \text{if } j = s, \\ 0, & \text{otherwise.} \end{cases} \end{aligned}$$

Thus for $\theta = 1 + \zeta_{p^{r+m}} + \ldots \zeta_{p^{r+m}}^{p^m-1}$ we obtain $\tau(\mathcal{C}) = \mathcal{O}_L = \theta \cdot \mathcal{A}$ and the assertion of the Theorem follows. □

Remarks 3.2 (i) In the case $r \geq 1$ the associated order $\mathcal{A}^{\mathrm{ass}}$ is a Hopf order by Proposition 2.10. This raises the following natural question: what is the affine $\mathcal{O}_K$-group scheme which is represented by $\mathcal{A}^{\mathrm{ass}}$? This question is somehow the starting point for the second proof of Theorem 3.1 in the case $r \geq 1$.

(ii) In the case $r = 0$ the associated order $\mathcal{A}^{\mathrm{ass}}$ is not a Hopf order by Proposition 2.8, except for $p = 2$ and $m = 1$.

3.2 Second proof

We assume the situation described in Section 1. Since the case $r = 0$ is settled in full generality by Corollary 2.15, we also assume $r \geq 1$. Combining ideas of [T1] and [T2] the strategy for our second proof is as follows:

1. Compute the Cartier dual $\mathcal{A}^{\mathrm{gs}}$ of the $\mathcal{O}_K$-Hopf order $\mathcal{B}^{\mathrm{gs}} \subseteq B$ which represents the affine $\mathcal{O}_K$-group scheme μ_{p^m} of p^m-th roots of unity. $\mathcal{A}^{\mathrm{gs}}$ is a $\mathcal{O}_K$-Hopf order in A.

2. Prove that $\mathcal{A}^{\mathrm{gs}} \subseteq \mathcal{A}^{\mathrm{ass}}$.

3. Apply the theory of tame objects over Hopf algebras of [CH], in particular [CH, Th,(5.4)], to derive that $\mathcal{C}$ is locally free over $\mathcal{A}^{\mathrm{gs}}$. This implies $\mathcal{A}^{\mathrm{gs}} = \mathcal{A}^{\mathrm{ass}}$.

4. Define "suitable" resolvents $(c_\theta, \chi)_{\gamma_0}$ as in (12), where $\gamma_0 = \zeta_{p^{r+m}}$, and compute their prime ideal factorization.

5. Compute $[\mathcal{A}^{\mathrm{ass}} : \mathcal{A}^\circ]_{\mathcal{O}_K}$, d_B and d_C and apply Corollary 2.14 to conclude that $\mathcal{C} = c_\theta \cdot \mathcal{A}^{\mathrm{ass}}$.

The affine group scheme μ_{p^m} of p^m-th roots of unity is represented by the $\mathcal{O}_K$-Hopf order

$$\mathcal{B}^{\mathrm{gs}} = \mathcal{O}_K[X]/\left(X^{p^m} - 1\right).$$

We view $\mathcal{B}^{\mathrm{gs}}$ as a order in B via the rule $b(X)(g) = b(g)$ for $b(X) \in \mathcal{O}_K[X]$ and $g \in G$.

Let $\mathrm{Tr}_{B/K} : B \to K$ denote the trace map $\mathrm{Tr}_{B/K}(b(X)) = \sum_{g\in G} b(g)$ and define, as usual, the inverse different of $\mathcal{B}^{\mathrm{gs}}$ by

$$D^{-1}(\mathcal{B}^{\mathrm{gs}}) = \{b \in B \mid \mathrm{Tr}_{B/K}(b\mathcal{B}^{\mathrm{gs}}) \subseteq \mathcal{O}_K\}.$$

In order to make this chapter as self-contained as possible, we will provide proofs of the following two results, although they are already stated in [T2].

Lemma 3.3 *[T2, Lemma 1] The inverse different of $\mathcal{B}^{\mathrm{gs}}$ is given by*

$$D^{-1}(\mathcal{B}^{\mathrm{gs}}) = \frac{1}{p^m}\mathcal{B}^{\mathrm{gs}}.$$

Proof We view the set $\{1, \bar{X}, \ldots, \bar{X}^{p^m-1}\} \subseteq \mathcal{B}^{\mathrm{gs}}$ as a K-basis of B. Let $b = \sum_{i=0}^{p^m-1} a_i \bar{X}^i \in B$, $a_i \in K$. Then

$$b \in D^{-1}(\mathcal{B}^{\mathrm{gs}}) \iff \sum_{i=0}^{p^m-1} a_i \sum_{g\in G} g^{i-j} \in \mathcal{O}_K \text{ for } j = 0, \ldots, p^m - 1. \tag{24}$$

From

$$\sum_{g\in G} g^{i-j} = \sum_{k=0}^{p^m-1} \zeta_{p^m}^{k(i-j)} = \begin{cases} p^m, & \text{if } i - j \equiv 0 \pmod{p^m}, \\ 0, & \text{otherwise,} \end{cases}$$

and (24) we conclude that

$$\begin{aligned} b \in D^{-1}(\mathcal{B}^{\mathrm{gs}}) \quad &\iff \quad p^m a_i \in \mathcal{O}_K \text{ for } i = 0, \ldots, p^m - 1 \\ &\iff \quad b \in \frac{1}{p^m}\mathcal{B}^{\mathrm{gs}}. \end{aligned}$$

$\square$

Proposition 3.4 *[T2, Prop. 1] The Cartier dual $\mathcal{A}^{\mathrm{gs}}$ of $\mathcal{B}^{\mathrm{gs}}$ is given by*

$$\mathcal{A}^{\mathrm{gs}} = \left\{ \frac{1}{p^m} \sum_{g \in G} f(g)g \mid f \in \mathcal{B}^{\mathrm{gs}} \right\}.$$

Proof We follow very closely the proof of [T2, Prop. 1]. Since the trace pairing

$$(\ ,\ ) : B \times B \to K, \quad (b_1, b_2) = \mathrm{Tr}_{B/K}(b_1 b_2)$$

is non-degenerate we have a natural isomorphism

$$\begin{array}{rcl} \xi : D^{-1}(\mathcal{B}^{\mathrm{gs}}) & \longrightarrow & \mathrm{Hom}_{\mathcal{O}_K}(\mathcal{B}^{\mathrm{gs}}, \mathcal{O}_K), \\ d & \longmapsto & (b \mapsto \xi(d)(b) = \mathrm{Tr}_{B/K}(db)). \end{array}$$

By the definition of the Cartier dual we get a natural identification

$$\begin{array}{rcl} \eta : \mathrm{Hom}_{\mathcal{O}_K}(\mathcal{B}^{\mathrm{gs}}, \mathcal{O}_K) & \longrightarrow & \mathcal{A}^{\mathrm{gs}}, \\ h & \longmapsto & \displaystyle\sum_{g \in G} a_g g, \quad \text{if } h(b) = \sum_{g \in G} a_g b(g), \forall b \in \mathcal{B}^{\mathrm{gs}}. \end{array}$$

Thus for $d \in D^{-1}(\mathcal{B}^{\mathrm{gs}})$ we obtain

$$(\eta \circ \xi)(d) = \sum_{g \in G} d(g)g$$

and the equality in the proposition follows from Lemma 3.3. $\square$

Since $\{1, \bar{X}, \ldots, \bar{X}^{p^m-1}\}$ constitutes an $\mathcal{O}_K$-basis of $\mathcal{B}^{\mathrm{gs}}$, the elements

$$e_s = \frac{1}{p^m} \sum_{k=0}^{p^m-1} \zeta_{p^m}^{ks} g_k, \quad s = 0, \ldots, p^m - 1,$$

form an $\mathcal{O}_K$-basis of $\mathcal{A}^{\mathrm{gs}}$ by Proposition 3.4. Obviously $e_s = e_\chi$ for the abelian character $\chi \in \hat{G}$ defined by $\chi(g_1) = \zeta_{p^m}^{-s}$ and thus $\mathcal{A}^{\mathrm{gs}} = \mathcal{A}$.

So far we have worked out the first step of our stratgy for the second proof of Theorem 3.1. In order to show that $\mathcal{A}^{\mathrm{gs}} \subseteq \mathcal{A}^{\mathrm{ass}}$ we proceed as in our first proof. The $\mathcal{A}^{\mathrm{gs}}$-module $\mathcal{C}$ is certainly locally free, since $\mathcal{A}^{\mathrm{gs}} = \mathcal{A} = \mathcal{A}^{\mathrm{ass}}$ is a maximal order. In further applications this will not be true, but the theory of tame objects over Hopf orders of Childs and Hurley [CH] provides an easily tested criterion to prove local freeness.

We now compute the resolvent $(c_\theta, \chi)_{\gamma_0}$ for $\theta = 1 + \zeta_{p^{r+m}} + \ldots + \zeta_{p^{r+m}}^{p^m-1}$, $\gamma_0 = \zeta_{p^{r+m}}$ and $\chi \in \hat{G}$ uniquely defined by $\chi(g_1) = \zeta_{p^m}^s$, $0 \leq s \leq p^m - 1$. We obtain

$$\begin{aligned}
(c_\theta, \chi)_{\gamma_0} &= \sum_{g\in G} \chi(g^{-1}) c_\theta(g\gamma_0) \\
&= \sum_{k=0}^{p^m-1} \zeta_{p^m}^{-ks} c_\theta\left(\zeta_{p^{r+m}}^{1+p^r k}\right) \\
&= \sum_{k=0}^{p^m-1} \zeta_{p^m}^{-ks} c_\theta\left(\zeta_{p^{r+m}}\right)^{\sigma(1+p^r k)} \\
&= \sum_{k=0}^{p^m-1} \zeta_{p^m}^{-ks} \theta^{\sigma(1+p^r k)} \\
&= \zeta_{p^{r+m}}^{s} \cdot p^m.
\end{aligned}$$

From Lemma 2.6 we know that $[\mathcal{A}^{\mathrm{ass}} : \mathcal{A}^\circ]^2_{\mathcal{O}_K} = p^{mp^m} d_B$ (note that $d_A = (1)$) and [Wa, Ch. 2, Prop. 2.1] implies that $d_C = d_{L/K} = p^{mp^m}$. We are now in position to apply Corollary 2.14:

$$\begin{aligned}
\left([\mathcal{A}^{\mathrm{ass}} : \mathcal{A}^\circ]^2_{\mathcal{O}_K} d_C\right) \mathcal{O}_{\mathbb{Q}(\zeta_{p^m})} &= \left(p^{mp^m} d_B d_C\right) \mathcal{O}_{\mathbb{Q}(\zeta_{p^m})} \\
&= \left(p^{2mp^m} d_B\right) \mathcal{O}_{\mathbb{Q}(\zeta_{p^m})} \\
&= \left(d_B \prod_{\chi\in\hat{G}} (c_\theta, \chi)^2_{\gamma_0}\right) \mathcal{O}_{\mathbb{Q}(\zeta_{p^m})}.
\end{aligned}$$

Hence $\mathcal{C} = c_\theta \cdot \mathcal{A}^{\mathrm{ass}}$. In fact we have proved a slightly stronger result, namely:

Theorem 3.5 *If $r \geq 1$, then the $\mathcal{A}^{\mathrm{ass}}$-module $\mathcal{C}$ is free of rank one on any map $c \in \mathcal{C}$ with the property*

$$(c, \chi)_{\gamma_0} \sim p^m$$

for all $\chi \in \hat{G}$. Moreover, $\mathcal{A}^{\mathrm{ass}} = \mathcal{A}^{\mathrm{gs}}$.

□

3.3 Composite results

So far we have only considered the prime power case. In this section we will use Theorem 3.1 to derive a complete result in the composite case.

Let $n, f^* \in \mathbb{N}$ and set $f = nf^*$. Let $G = \mu_n$ and $\Gamma = \{\gamma \in \bar{\mathbb{Q}} \mid \gamma^n = \zeta_{f^*}\}$. We write

$$n = \prod_{i=1}^{s} p_i^{m_i}, \quad f^* = \prod_{i=1}^{s} p_i^{r_i}, \quad f^* = \prod_{i=1}^{s} p_i^{r_i+m_i}, \quad 0 \leq r_i, m_i, \quad r_i + m_i \geq 1,$$

with mutually distinct rational primes p_i. Then

$$G = \prod_{i=1}^{s} G_i, \quad \Gamma = \prod_{i=1}^{s} \Gamma_i,$$

where $G_i = \mu_{p_i^{m_i}}$ and $\Gamma_i = \{\gamma \in \bar{\mathbb{Q}} \mid \gamma^{p_i^{m_i}} = \zeta_{p_i^{r_i}}\}$, $i = 1, \dots, s$. We write

$$K = \mathbb{Q}(\zeta_{f^*}), \quad L = \mathbb{Q}(\zeta_f), \quad \Omega = \Omega_K,$$

and define

$$A = (\bar{K}G)^{\Omega}, \quad B = \mathrm{Map}(G, \bar{K})^{\Omega}, \quad C = \mathrm{Map}(\Gamma, \bar{K})^{\Omega}.$$

Let $\mathcal{B}^{\mathrm{gs}} \subseteq B$ denote the $\mathcal{O}_K$-Hopf order which represents the affine $\mathcal{O}_K$-group scheme μ_n of n-th roots of unity. As before we write $\mathcal{A}^{\mathrm{gs}}$ for its Cartier dual in A.

Theorem 3.6 *Assume the notation as above. Then $\mathcal{C}$ is free of rank one over its associated order $\mathcal{A}^{\mathrm{ass}}$. If, in addition, $r_i \geq 1$ for $i = 1, \dots, s$, then $\mathcal{A}^{\mathrm{ass}} = \mathcal{A}^{\mathrm{gs}}$.*

Proof For $i = 1, \dots, s$ we set $A_i = (\bar{K}G_i)^{\Omega}$ and $C_i = \mathrm{Map}(\Gamma_i, \bar{K})^{\Omega}$. Then

$$A_1 \otimes_K \ldots \otimes_K A_s \to A, \quad a_1 \otimes \ldots \otimes a_s \mapsto a_1 \cdots a_s$$

is an isomorphism of K-algebras. Furthermore,

$$C_1 \otimes_K \ldots \otimes_K C_s \to C, \quad h_1 \otimes \ldots \otimes h_s \mapsto \big(\gamma_1 \cdots \gamma_s \mapsto h_1(\gamma_1) \cdots h_s(\gamma_s)\big)$$

is a isomorphism of A-modules.

For $i = 1, \dots, s$ we set

$$K_i = \mathbb{Q}(\zeta_{p_i^{r_i}}), \quad A_i' = (\bar{K}_i G_i)^{\Omega_{K_i}}, \quad C_i' = \mathrm{Map}(\Gamma_i, \bar{K}_i)^{\Omega_{K_i}}.$$

Note that Lemma 2.1(vi) and Lemma 2.11(v) imply

$$K \otimes_{K_i} A_i' \simeq A_i, \quad K \otimes_{K_i} C_i' \simeq C_i.$$

Let $\mathcal{C}_i'$ denote the integral closure of $\mathcal{O}_{K_i}$ in C_i' and denote by $\mathcal{A}_i'^{\mathrm{ass}}$ its associated order. Then, by Theorem 3.1, there exists a map $c_i \in \mathcal{C}_i'$ such that

$$\mathcal{C}_i' = c_i \cdot \mathcal{A}_i'^{\mathrm{ass}}$$

for $i = 1, \dots, s$. Since the discriminants $d_{\mathcal{C}_i'}$ and d_{K/K_i} are relatively prime, we obtain by applying $\mathcal{O}_K \otimes_{\mathcal{O}_{K_i}} \_$:

$$\mathcal{C}_i \simeq \mathcal{O}_K \otimes_{\mathcal{O}_{K_i}} \mathcal{C}_i' = c_i \left(\mathcal{O}_K \otimes_{\mathcal{O}_{K_i}} \mathcal{A}_i'^{\mathrm{ass}}\right).$$

Thus $\mathcal{A}_i^{\mathrm{ass}} \simeq \mathcal{O}_K \otimes_{\mathcal{O}_{K_i}} \mathcal{A}_i'^{\mathrm{ass}}$. Again we note that the discriminants $d_{\mathcal{C}_i}$, $i = 1, \dots, s$, are mutually relative coprime. Hence

$$\mathcal{C} \simeq \mathcal{C}_1 \otimes_{\mathcal{O}_K} \ldots \otimes_{\mathcal{O}_K} \mathcal{C}_s = c_1 \cdot \mathcal{A}_1^{\mathrm{ass}} \otimes_{\mathcal{O}_K} \ldots \otimes_{\mathcal{O}_K} c_s \mathcal{A}_s^{\mathrm{ass}},$$

or in other words,

$$\mathcal{C} = c \cdot \mathcal{A}^{\mathrm{ass}} \text{ with } c = c_1 \cdots c_s, \quad \mathcal{A}^{\mathrm{ass}} \simeq \mathcal{A}_1^{\mathrm{ass}} \otimes_{\mathcal{O}_K} \ldots \otimes_{\mathcal{O}_K} \mathcal{A}_s^{\mathrm{ass}}.$$

If $r_i \geq 1$ for $i = 1, \ldots, s$, then $\mathcal{A}_i^{\mathrm{ass}}$ is the dual of the $\mathcal{O}_K$-Hopf order $\mathcal{B}_i^{\mathrm{gs}}$ which represents the $\mathcal{O}_K$-group scheme $\mu_{p_i^{m_i}}$. The affine group scheme μ_n is the fibre product of the $\mu_{p_i^{m_i}}$ and therefore represented by $\mathcal{B}^{\mathrm{gs}} = \mathcal{B}_1^{\mathrm{gs}} \otimes_{\mathcal{O}_K} \ldots \otimes_{\mathcal{O}_K} \mathcal{B}_s^{\mathrm{gs}}$. Now the second assertion of Theorem 3.6 follows from $\mathcal{A}^{\mathrm{ass}} \simeq \mathcal{A}_1^{\mathrm{ass}} \otimes_{\mathcal{O}_K} \ldots \otimes_{\mathcal{O}_K} \mathcal{A}_s^{\mathrm{ass}}$. □

4 Relative Lubin-Tate formal groups

Our main reference for the general theory of relative Lubin-Tate formal groups is [dS].

Throughout this section p denotes a rational prime number. For any extension field $\mathbb{Q}_p \subseteq L \subseteq \bar{\mathbb{Q}}_p$ we write $\mathcal{O}_L$ for the integral closure of $\mathbb{Z}_p$ in L and $\mathfrak{p}_L$ for its maximal ideal. We fix a finite extension field F of $\mathbb{Q}_p$ and we set $q = |\mathcal{O}_F/\mathfrak{p}_F|$.

Let $d > 0$ be a fixed integer. We denote by F'/F the unramified extension of degree $d > 0$ and by ϕ the Frobenius automorphism of F'/F. We fix an element $\xi \in F$ such that $v_F(\xi) = d$, where v_F denotes the normalized valuation (i.e., $v_F(F^*) = \mathbb{Z}$) of F.

As in [dS, Ch. I] we set

$$\begin{aligned} F_\xi = \{f \in \mathcal{O}_{F'}[[X]] \quad | \quad & f \equiv \pi' X \bmod X^2, \\ & \mathrm{N}_{F'/F}(\pi') = \xi \text{ and } f \equiv X^q \bmod \mathfrak{p}_{F'}[[X]]\} \end{aligned}$$

For any power series g over $\mathcal{O}_{F'}$ in one or more indeterminates, let g^ϕ arise from applying ϕ to the coefficients of g.

From [dS, Ch.I, Th.1.3] we know that for every $f \in F_\xi$ there exists a unique one-dimensional commutative formal group $\mathcal{F}_f$ defined over $\mathcal{O}_{F'}$ such that $f \in \mathrm{Hom}(\mathcal{F}_f, \mathcal{F}_f^\phi)$. Note that $f^\phi \in F_\xi$ and $\mathcal{F}_f^\phi = \mathcal{F}_{f^\phi}$. Of course, classical Lubin-Tate formal groups correspond to the case $d = 1$.

In order to introduce all the necessary notation we recall

Proposition 4.1 *([dS, Ch.I, (1.5)]) Let $f(X) = \pi_1 X + \ldots$, $g(X) = \pi_2 X + \ldots$ be in F_ξ. Let $a \in \mathcal{O}_{F'}$ satisfy $a^{\phi - 1} = \pi_2/\pi_1$. Then there exists a unique power series $[a]_{f,g} \in \mathcal{O}_{F'}[[X]]$ such that*

$$\begin{aligned} &(i) \qquad [a]_{f,g} \equiv aX \bmod X^2, \\ &(ii) \qquad [a]_{f,g}^\phi \circ f = g \circ [a]_{f,g}. \end{aligned}$$

Moreover, $[a]_{f,g} \in \mathrm{Hom}(\mathcal{F}_f, \mathcal{F}_g)$. The map

$$\{a \in \mathcal{O}_{F'} \mid a^{\phi-1} = \pi_2/\pi_1\} \to \mathrm{Hom}(\mathcal{F}_f, \mathcal{F}_g), \quad a \mapsto [a]_{f,g}$$

is a group isomorphism and in the case $f = g$ a ring isomorphism $\mathcal{O}_F \simeq \mathrm{End}(\mathcal{F}_f)$. Furthermore, if $h(X) = \pi_3 X + \ldots \in F_\xi$ and $b^{\phi-1} = \pi_3/\pi_2$, then $[ab]_{f,h} = [b]_{g,h} \circ [a]_{f,g}$.

□

In the sequel we shall always write $[a]_f$ for $[a]_{f,f}$. If $f(X) = \pi' X + \ldots \in F_\xi$ and $i \geq 0$, then we put

$$f^{(i)} = f^{\phi^{i-1}} \circ \ldots \circ f^{\phi} \circ f. \tag{25}$$

Then $f^{(i)} \in \mathrm{Hom}(\mathcal{F}_f, \mathcal{F}_{f^{\phi^i}})$ and $f^{(d)} = [\xi]_f \in \mathrm{End}(\mathcal{F}_f)$. Moreover, for $\alpha \in \mathcal{O}_{F'}$ we write $\alpha^{(i)} = \alpha^{\phi^{i-1}} \cdots \alpha^{\phi} \cdot \alpha$. It then follows that $f^{(i)}(X) = [\pi'^{(i)}]_{f,f^{\phi^i}}(X)$.

As usual we endow the set $\mathfrak{p}_{\bar{F}}$ with the structure of an $\mathcal{O}_F$-module, denoted by $\mathcal{F}_f(\mathfrak{p}_{\bar{F}})$, by setting

$$x +_f y = \mathcal{F}_f(x, y)\,, \quad a \cdot x = [a]_f(x)\,,$$

for $x, y \in \mathfrak{p}_{\bar{F}}$ and $a \in \mathcal{O}_F$.

We now fix $\xi \in \mathcal{O}_F$ with $v_F(\xi) = d$ and a power series $f(X) = \pi' X + \ldots \in F_\xi$. Let $\pi \in \mathcal{O}_F$ be any prime element. For $n \in \mathbb{N}_0$ we define the group of $\mathfrak{p}_F^n$-torsion points of $\mathcal{F}_f$ by

$$\begin{aligned} G_{f,n} &= \{x \in \mathfrak{p}_{\bar{F}} \mid [a]_f(x) = 0, \forall a \in \mathfrak{p}_F^n\} \\ &= \{x \in \mathfrak{p}_{\bar{F}} \mid [\pi^n]_f(x) = 0\} \\ &= \ker(f^{(n)} : \mathcal{F}_f(\mathfrak{p}_{\bar{F}}) \to \mathcal{F}_{f^{\phi^n}}(\mathfrak{p}_{\bar{F}})) \end{aligned}$$

(see [dS, Ch. I, 1.7]).

In fact, $G_{f,n}$ is an abelian group under $+_f$ of order q^n. The field $F_{\xi,n} = F'(G_{f,n})$ does not depend on the choice of $f \in F_\xi$. $F_{\xi,n}/F$ is abelian and $F_{\xi,n}/F'$ is totally ramified of degree $q^{n-1}(q-1)$. Every $\alpha \in G_{f,n} \smallsetminus G_{f,n-1}$ generates $F_{\xi,n}$ over F' and, in addition, α is a uniformizer for $F_{\xi,n}$. This implies that $\mathcal{O}_{F_{\xi,n}} = \mathcal{O}_{F'}[\alpha]$. See [dS, Ch. I, Prop. 1.8] for more details.

We are now ready to describe a set-up that fits into the general framework of Section 1. We fix integers $r \geq 0$, $m \geq 1$ and set $G = G_{f,m}$. We choose a primitive $\mathfrak{p}_F^r$-torsion point β (i.e. $\beta \in G_{f,r} \smallsetminus G_{f,r-1}$) and set

$$\Gamma = \{\gamma \in \mathfrak{p}_{\bar{F}} \mid f^{(m)}(\gamma) = \beta\}\,.$$

We consider $F_{\xi,r}$ as our base field and in order to simplify notation we set

$$K := F_{\xi,r}\,, \quad \Omega := \Omega_K\,, \quad L := F_{\xi,r+m}\,.$$

The data $\mathcal{O}_K$, K, G and Γ now satisfy the axioms postulated at the beginning of Section 1, where $\Omega := \Omega_K$ acts on G and Γ through Galois automorphisms (thus we also write $\omega(g)$ and $\omega(\gamma)$ instead of ${}^{\omega}g$ and ${}^{\omega}\gamma$), and where G acts on Γ by translation:

$${}^{g}\gamma = g +_f \gamma\,,$$

for $g \in G$ and $\gamma \in \Gamma$. In particular, $|\Gamma| = |G| = q^m$.

As in Section 1 we set

$$A := (\bar{K}G)^\Omega\,, \quad B := \mathrm{Map}(G, \bar{K})^\Omega\,, \quad C := \mathrm{Map}(\Gamma, \bar{K})^\Omega\,,$$

omitting the index K.

For $r \geq 1$ we have $L = K(\gamma_0)$. The following lemma reveals the connection to results of Cassou-Noguès and Taylor (see [CT, Ch. X, Thm. 3.3]).

For the rest of this section we fix an element $\gamma_0 \in \Gamma$. Then $L = K(\gamma_0)$.

Lemma 4.2 *Suppose that $r \geqslant m \geqslant 1$. Then the following assertions hold:*

(a) *The map*

$$\tau : C \longrightarrow L, \quad c \longmapsto c(\gamma_0),$$

is an isomorphism of K-algebras.

(b) *One has $A = KG$.*

(c) *The map*

$$G \to \mathrm{Gal}(L/K)\,, \quad g \mapsto \omega_g\,,$$

where ω_g is uniquely determined by ${}^{(\omega_g)}\gamma_0 = {}^g\gamma_0$ $(= g +_f \gamma_0)$, is a group isomorphism.

(d) *Identifying G and $\mathrm{Gal}(L/K)$ as in (c), the map τ is also an isomorphism of A-modules, where we consider L endowed with the right A-module structure $x \cdot a := ax$ for $a \in A$ and $x \in L$.*

Proof (a) First we show that Ω acts transitively on Γ. In fact, applying the Weierstrass Preparation theorem we can write $f^{(m)}(X) - \beta = h(X)u(X)$ with a distinguished polynomial $h(X) \in \mathcal{O}_K[[X]]$ of degree q^m and a unit $u(X) \in \mathcal{O}_K[[X]]^*$. Since β is a uniformizer in K, $h(X)$ is an Eisenstein polynomial and therefore irreducible. Hence the Galois group Ω acts transitively on $\Gamma = \{x \in \bar{F} \mid h(x) = 0\}$. Now the result follows from $K(\gamma_0) = L$.

(b) This is immediate from $G \subseteq K$.

(c) Let $g, h \in G$. Then

$$\begin{aligned} {}^{\omega_{(g+_f h)}}\gamma_0 &= (g +_f h) +_f \gamma_0 = g +_f \omega_h(\gamma_0) = \omega_h(g +_f \gamma_0) \\ &= \omega_h \omega_g(\gamma_0) = (\omega_g \omega_h)(\gamma_0)\,, \end{aligned}$$

since $g \in K$ and Ω/Ω_L is an abelian group. This implies that the map $g \mapsto \omega_g$ is a group homomorphism, which is bijective, since G and Ω act transitively on Γ.

(d) This follows from

$$(c \cdot g)(\gamma_0) = c(g +_f \gamma_0) = c({}^{(\omega_g)}\gamma_0) = \omega_g(c(\gamma_0))\,,$$

for $c \in C$ and $g \in G$. □

At this point the same remarks as in the cyclotomic case (following (22)) apply. Of course, the map τ of Lemma 6.2 is an isomorphism of K-algebras for arbitrary $r, m \geqslant 1$. The map in (c), however, is in general just a bijection and not a homomorphism. Via τ we can endow L with the structure of an A-module, which for $m > r$ does not coincide with the usual Galois module structure.

If $r \geq 1$ we shall always identify C and L via τ in the following; in particular we write $c_x = \tau^{-1}(x)$ for $x \in L$.

We recall the following trace relation which is basic for the rest of this section.

Proposition 4.3 *([Ch, Lemma 3.2]) For $i \in \mathbb{N}_0$ one has*

$$s_i = \sum_{g \in G} g^i \ \in \ \mathfrak{p}_{F'}^m.$$

Moreover, s_{q^m-1} has exact F'-valuation m and for $i > q^m - 1$ the F'-valuation of s_i is strictly bigger than m.

□

Although obvious at this point, we remark that for $i = 0$ the summand 0^0 has to be interpreted as 1. We also remark that $\pi'^{(m)}$ is associated to π^m.

We recall that the associated order of $\mathcal{C}$ in A is defined by

$$\mathcal{A}^{\mathrm{ass}} = \{a \in A \mid \mathcal{C} \cdot a \subseteq \mathcal{C}\}.$$

Motivated by [T1, Theorem 3] and the cyclotomic case of Section 3.2 we will prove that $\mathcal{A}^{\mathrm{ass}}$ coincides with the Cartier dual of the $\mathcal{O}_K$-Hopf order which represents the $\mathcal{O}_K$-group scheme of $\mathfrak{p}_F^m$-torsion on $\mathcal{F}_f$. This affine group scheme is represented by the $\mathcal{O}_K$-Hopf order

$$\mathcal{B}^{\mathrm{gs}} = \frac{\mathcal{O}_K[[X]]}{(f^{(m)}(X))}. \tag{26}$$

We view $\mathcal{B}^{\mathrm{gs}}$ as an order in B via the rule $b(X)(g) = b(g)$ for $b(X) \in \mathcal{O}_K[[X]]$ and $g \in G$. Let $\mathcal{A}^{\mathrm{gs}} \subseteq A$ be the Cartier dual of $\mathcal{B}^{\mathrm{gs}}$. Then $\mathcal{A}^{\mathrm{gs}}$ is an $\mathcal{O}_K$-Hopf order. For a thorough discussion of these facts the reader is referred to [BT, II, §7].

Let $\mathrm{Tr}_{B/K} : B \to K$ denote the trace map $\mathrm{Tr}_{B/K}(b(X)) = \sum_{g \in G} b(g)$ and write $D^{-1}(\mathcal{B}^{\mathrm{gs}})$ for the inverse different of $\mathcal{B}^{\mathrm{gs}}$:

$$D^{-1}(\mathcal{B}^{\mathrm{gs}}) = \{b \in B \mid \mathrm{Tr}_{B/K}(b\mathcal{B}^{\mathrm{gs}}) \subseteq \mathcal{O}_K\}.$$

The following Lemma is completely analogous to Lemma 3.3 (see also [T2, Lemma 1]).

Lemma 4.4 *The inverse different of $\mathcal{B}^{\mathrm{gs}}$ is given by*

$$D^{-1}(\mathcal{B}^{\mathrm{gs}}) = \frac{1}{\pi'^{(m)}} \mathcal{B}^{\mathrm{gs}}.$$

Proof Replacing the well-known trace relations for roots of unity by the trace relations of Proposition 4.3 this is proved as Lemma 3.3. For the reader's convenience we give the details.

The set $\{\bar{1}, \bar{X}, \dots, \bar{X}^{q^m-1}\}$ constitutes an $\mathcal{O}_K$-basis of $\mathcal{B}^{\mathrm{gs}}$ and also an K-basis of B. Let $b = \sum_{i=0}^{q^m-1} a_i \bar{X}^i \in B$, $a_i \in K$. Then:

$$b \in D^{-1}(\mathcal{B}^{\mathrm{gs}}) \Longleftrightarrow \sum_{i=0}^{q^m-1} a_i \sum_{g\in G} g^{i+j} \in \mathcal{O}_K \text{ for } j = 0, \dots, q^m - 1. \tag{27}$$

From Propostion 4.3 it follows immediately that $\frac{1}{\pi'^{(m)}}\mathcal{B}^{\mathrm{gs}} \subseteq D^{-1}(\mathcal{B}^{\mathrm{gs}})$. For the converse inclusion we set $v_0 = \min\{v_{\bar{F}}(a_i) \mid i = 0, \dots, q^m - 1\}$ and $i_0 = \min\{i \mid v_{\bar{F}}(a_i) = v_0\}$, where $v_{\bar{F}}$ is the extension to $\bar{F}$ of the normalized valuation v_F. Then the right hand side of (27) equals for $j = q^m - 1 - i_0$

$$\sum_{i=0}^{i_0-1} a_i \sum_{g\in G} g^{q^m-1+i-i_0} + a_{i_0} \sum_{g\in G} g^{q^m-1} + \sum_{i=i_0+1}^{q^m-1} a_i \sum_{g\in G} g^{q^m-1+i-i_0} \in \mathcal{O}_K.$$

Again from Proposition 4.3 we conclude that the $v_{\bar{F}}$-valuation of the middle summand is equal to v_0+m, whereas the other summands have valuation strictly bigger than $v_0 + m$. Thus $v_0 + m \geq 0$, which proves $D^{-1}(\mathcal{B}^{\mathrm{gs}}) \subseteq \frac{1}{\pi'^{(m)}}\mathcal{B}^{\mathrm{gs}}$. $\square$

In what follows, the elements of G play two different roles in the group algebra $\bar{F}G$: on the one hand they occur as group elements, on the other hand they are field elements of $\bar{F}$ and occur as coefficients in $\bar{F}G$. To distinguish these different roles we henceforth write x_g instead of g whenever g is considered as a field element. Moreover we write g_0 for the unit element in G. Following [CT, Ch. X, Def. 3.2] we introduce certain special elements of the algebra A. For $i \geq 0$ we set

$$\sigma_i := \frac{1}{\pi'^{(m)}} \sum_{g\in G} x_g^i (g - g_0). \tag{28}$$

It is immediate that these elements are Ω-invariant.

The next proposition is the analogue of Proposition 3.4 (see also [T2, Prop. 1]).

Proposition 4.5 *The Cartier dual $\mathcal{A}^{\mathrm{gs}}$ of $\mathcal{B}^{\mathrm{gs}}$ is given by*

$$\mathcal{A}^{\mathrm{gs}} = \{\frac{1}{\pi'^{(m)}} \sum_{g\in G} f(g)g \mid f \in \mathcal{B}^{\mathrm{gs}}\} = \mathcal{O}_K \cdot g_0 + \sum_{i=0}^{q^m-2} \mathcal{O}_K \cdot \sigma_i.$$

Proof The first equality is proved as Proposition 3.4. In order to prove the second one we first define $l' \in \mathcal{B}^{\mathrm{gs}}$ by

$$l'(g) = \begin{cases} \pi'^{(m)}, & \text{if } g = g_0, \\ 0, & \text{if } g \neq g_0. \end{cases} \tag{29}$$

Note that $l' = f^{(m)}(X)/X$. Writing $f^{(m)}(X) = h(X)u(X)$ with a distinguished polynomial $h(X) \in \mathcal{O}_K[[X]]$ of degree q^m and a unit $u(X) = u_0 + \ldots \in \mathcal{O}_K[[X]]^*$ we see that

$$l' = u_0 \frac{h(X)}{X} + h(X)\frac{u(X) - u_0}{X} \equiv u_0 \frac{h(X)}{X} \pmod{(f^{(m)}(X))}.$$

It immediately follows that the set $\{\bar{1}, \bar{X}, \ldots, \bar{X}^{q^m-2}, l'\}$ also forms an $\mathcal{O}_K$-basis of $\mathcal{B}^{\mathrm{gs}}$. Now the second equality is an immediate consequence of Lemma 4.3. □

For later reference we deduce from Lemma 4.4 and Proposition 4.5

Corollary 4.6 *[T2, Proposition 2] $\mathcal{B}^{\mathrm{gs}}$ is a free $\mathcal{A}^{\mathrm{gs}}$-module on the map l' defined in (29).*

Proof Consider the map $\kappa = {}^{-} \circ \eta \circ \xi : D^{-1}(\mathcal{B}^{\mathrm{gs}}) \to \mathcal{A}^{\mathrm{gs}}$ defined by

$$\kappa(d) = ({}^{-} \circ \eta \circ \xi)(d) = \sum_{g \in G} d(g) g^{-1}, \quad d \in D^{-1}(\mathcal{B}^{\mathrm{gs}})$$

(for the definition of $\eta \circ \xi$ see the proof of Proposition 3.4). It is easily verified that κ is an isomorphism of $\mathcal{A}^{\mathrm{gs}}$-modules. Hence we obtain

$$\frac{1}{\pi'(m)} \mathcal{B}^{\mathrm{gs}} = D^{-1}(\mathcal{B}^{\mathrm{gs}}) = \kappa^{-1}(\mathcal{A}^{\mathrm{gs}}) = \kappa^{-1}(1) \cdot \mathcal{A}^{\mathrm{gs}} = l \cdot \mathcal{A}^{\mathrm{gs}}.$$

□

In the sequel we assume $r \geq 1$, since by Corollary 2.15 the module structure of $\mathcal{C} = \mathcal{B}$ is well-known for $r = 0$. Our aim is to show that $\mathcal{A}^{\mathrm{gs}}$ is equal to the associated order $\mathcal{A}^{\mathrm{ass}}$. The following lemma is a first step in this direction.

Lemma 4.7 *The elements σ_i, $i \geqslant 0$, are contained in $\mathcal{A}^{\mathrm{ass}}$. In particular, $\mathcal{A}^{\mathrm{gs}} \subseteq \mathcal{A}^{\mathrm{ass}}$.*

Proof The proof is simply an adaptation of the proof of [CT, Ch. X, Lemma 3.5] to our situation. For the reader's convenience we give a short translation into our setting and notation. The maximal $\mathcal{O}_K$-order $\mathcal{C}$ of C identifies via τ with the ring of integers $\mathcal{O}_L$ in L. Since $\mathcal{O}_L = \mathcal{O}_K[\gamma_0]$, it suffices to show that

$$c_{\gamma_0^k} \cdot \sigma_i \in \mathcal{C} \tag{30}$$

for $0 \leqslant i$ and $0 \leqslant k \leqslant q^m - 1$. To achieve this we compute $\tau(c_{\gamma_0^k} \cdot \sigma_i)$:

$$\begin{aligned}
\tau(c_{\gamma_0^k} \cdot \sigma_i) &= \frac{1}{\pi'(m)} \sum_{g \in G} x_g^i \left(c_{\gamma_0^k}(\gamma_0 +_f g) - c_{\gamma_0^k}(\gamma_0) \right) \\
&= \frac{1}{\pi'(m)} \sum_{g \in G} x_g^i \left({}^{\omega_g}(\gamma_0^k) - \gamma_0^k \right) \\
&= \frac{1}{\pi'(m)} \sum_{g \in G} x_g^i \left(\mathcal{F}_f(\gamma_0, g)^k - \gamma_0^k \right) \\
&= \frac{1}{\pi'(m)} \sum_{g \in G} x_g^i \cdot g\mathcal{F}_1(\gamma_0, g)\,,
\end{aligned}$$

where we have set $\mathcal{F}_f(X,Y)^k = X^k + Y\mathcal{F}_1(X,Y)$. Recall that $g = x_g$ and write $Y\mathcal{F}_1(X,Y) = \sum_{s=0}^{\infty} X^s a_s(Y)$ with $a_s(Y) \in \mathcal{O}_{F'}[[Y]]$. Then

$$\tau(c_{\gamma_0^k} \cdot \sigma_i) = \sum_{s=0}^{\infty} \gamma_0^s \cdot \frac{1}{\pi'^{(m)}} \sum_{g\in G} g^i a_s(g).$$

Since the right-hand term is integral by Proposition 4.3, this establishes (30). □

From Lemma 4.7 we deduce the following corollary which may be viewed as a generalization of the trace relations of Proposition 4.3.

Corollary 4.8 *Let $\chi \in \hat{G}$ and $i \geqslant 0$. Then*

$$\frac{1}{\pi'^{(m)}} \sum_{g\in G} g^i \chi(g) \ \in \ \mathcal{O}_{\bar{F}}\,.$$

Proof Each $\chi \in \hat{G}$ induces a homomorphism $A \to \bar{F}$ of F-algebras, which we again denote by χ. Together with Lemma 4.7, this implies that

$$\chi(\sigma_i) = \frac{1}{\pi'^{(m)}} \sum_{g\in G} g^i(\chi(g) - 1)$$

is integral over $\mathcal{O}_F$. Now we easily deduce the integrality of $\frac{1}{\pi'^{(m)}} \sum_{g\in G} g^i\chi(g)$ from Proposition 4.3. □

Now that we know that the Hopf order $\mathcal{A}^{\mathrm{gs}}$ acts on $\mathcal{C}$ we can apply the results of [CH] to show that $\mathcal{C}$ is a free $\mathcal{A}^{\mathrm{gs}}$-module (necessarily of rank one). In this context recall the definition of tamenes of [CH, Def. (2.2)].

The module of integrals I is defined by

$$I = \{a \in \mathcal{A}^{\mathrm{gs}} \mid a'a = \epsilon(a')a \text{ for all } a' \in \mathcal{A}^{\mathrm{gs}}\}\,.$$

Recall the definition of σ_i in (28).

Lemma 4.9 *With the above notation one has $I = \frac{1}{\pi^m}\mathcal{O}_K \sum_{g\in G} g$.*

Proof The inclusion "$\supseteq$" is immediate. For the converse let $a = \sum_{g\in G} \lambda_g g$, $\lambda_g \in \bar{F}$, be an element in I. Since $\mathcal{A}^{\mathrm{gs}}$ is generated by $g_0, \sigma_0, \ldots, \sigma_{q^m-1}$ we obtain the condition

$$a \in I \Longleftrightarrow \sigma_i \cdot \sum_{g\in G} \lambda_g g = 0 \qquad \text{for } i = 0, \ldots, q^m - 2\,.$$

On multiplying and comparing coefficients we derive

$$\sum_{g\in G\setminus\{g_0\}} x_g^i(\lambda_{hg^{-1}} - \lambda_h) = 0\,,$$

for all $i = 0, \dots, q^m - 2$ and $h \in G$. The Vandermonde matrix $(x_g^i)_{i=0,\dots,q^m-2,\ g\in G\setminus\{g_0\}}$ is obviously invertible. Therefore, $\lambda_{hg^{-1}} = \lambda_h$, for all $g, h \in G$, which in turn implies $\lambda = \lambda \cdot \sum_{g\in G} g$ with $\lambda \in K$. Now the result follows, since π^m is the highest possible denominator for elements in $\mathcal{A}^{\mathrm{gs}}$. $\square$

Corollary 4.10 *Let $r \geq 1$. Then the associated order $\mathcal{A}^{\mathrm{ass}}$ is equal to $\mathcal{A}^{\mathrm{gs}}$ and $\mathcal{C}$ is free of rank one over $\mathcal{A}^{\mathrm{ass}}$.*

Proof From [Ch, Lemma 3.1 (b)] we deduce that $\mathcal{C} \cdot I = \mathcal{O}_K$, which shows that $\mathcal{C}$ is a tame $\mathcal{A}^{\mathrm{gs}}$-object. Now [CH, Thm. (5.4)] implies that $\mathcal{C}$ is free over $\mathcal{A}^{\mathrm{gs}}$ of rank one. Hence $\mathcal{A}^{\mathrm{ass}} = \mathcal{A}^{\mathrm{gs}}$. $\square$

The disadvantage of the approach we have taken so far is that we do not get an explicit generator. These local results are certainly of interest for themselves, but they also play an important role if we want to derive analogous results in the global situation of Example 1.1 (d). To obtain a link between global and local we will need an explicit generator or, and this will lead to even stronger results, a relation between local and global resolvents.

For $\chi \in \hat{G}$, we define the resolvent function

$$R_\chi(X) := \sum_{g\in G} \frac{f^{(m)}(X)}{g +_f X} \chi(g^{-1}) \in \bar{F}[[X]]\,.$$

Theorem 4.11 *For each $\chi \in \hat{G}$ one has*

$$R_\chi(X) = \pi'^{(m)} \cdot u_\chi(X)$$

with a unit $u_\chi(X) \in \mathcal{O}_{\bar{F}}[[X]]^\times$.

Proof First we note that

$$R_\chi(0) = \left.\frac{f^{(m)}(X)}{X}\right|_{X=0} = \pi'^{(m)}\,.$$

Note that for $g \in G$ one has $f^{(m)}(g +_f X) = f^{(m)}(X)$. Since $f^{(m)}(X)$ has no constant term, it follows from

$$R_\chi(X) = \sum_{g\in G} \frac{f^{(m)}(g +_f X)}{g +_f X} \chi(g^{-1})$$

that $R_\chi(X) \in \mathcal{O}_{\bar{F}}[[X]]$. Hence it suffices to show that each coefficient of $R_\chi(X)$ is divisible by $\pi'^{(m)}$. However, it is easily seen that we may write

$$\frac{f^{(m)}(g +_f X)}{g +_f X} = \sum_{i=0}^{\infty} q_i(g) X^i\,,$$

where $q_i \in \mathcal{O}_{F'}[[X]]$, $i \in \mathbb{N}_0$, are power series depending only on the formal group $\mathcal{F}_f$. Hence we may deduce

$$R_\chi(X) = \sum_{i=0}^{\infty} [\sum_{g \in G} q_i(g)\chi(g^{-1})] X^i .$$

This completes the proof, since by Corollary 4.8 the terms in brackets are divisible by $\pi'^{(m)}$. □

Consider the map

$$c \colon \Gamma \to \bar{F}\,, \quad \gamma \mapsto \frac{f^{(m)}(\gamma)}{\gamma}\,. \tag{31}$$

Since $f^{(m)}(X) \in \mathcal{O}_{F'}[[X]]$, it is Ω-invariant. Thus, $c \in C$, and $c = c_\theta$ with $\theta = \frac{f^{(m)}(\gamma_0)}{\gamma_0}$. Moreover, recalling the definition of the resolvent $(c,\chi)_{\gamma_0}$ for $\chi \in \hat{G}$ from Section 2.4, we have the following relation:

$$\begin{aligned} (c,\chi)_{\gamma_0} &= \sum_{g \in G} c({}^{g}\gamma_0)\,\chi(g^{-1}) = \sum_{g \in G} \frac{f^{(m)}(g +_f \gamma_0)}{g +_f \gamma_0}\,\chi(g^{-1}) \\ &= \sum_{g \in G} \frac{f^{(m)}(\gamma_0)}{g +_f \gamma_0}\chi(g^{-1}) = R_\chi(\gamma_0)\,. \end{aligned} \tag{32}$$

We are now ready to state and prove the main result of this section.

Theorem 4.12
(i) Let $r = 0$. Then $\mathcal{A}^{\mathrm{ass}} = \mathcal{A}^\circ$ and $\mathcal{C} = \mathcal{B}$ is free of rank one with $\mathcal{A}^\circ$-generator $l \in \mathcal{B}$, where l is defined in (19).
(ii) Let $r \geq 1$. Then one has:

(a) The $\mathcal{A}^{\mathrm{ass}}$-module $\mathcal{C}$ is free of rank one on any map $c \in \mathcal{C}$ with the property that

$$(c,\chi)_{\gamma_0} \sim \pi^m$$

for all $\chi \in \hat{G}$.

(b) Any function $c_x \in \mathcal{C}$ with $x \in L^\times$ having $\mathfrak{p}_L$-valuation $q^m - 1$ is an $\mathcal{A}^{\mathrm{ass}}$-basis of $\mathcal{C}$. In particular,

$$\mathcal{C} = c \cdot \mathcal{A}^{\mathrm{ass}} \tag{33}$$

with $c = c_\theta$ from (31).

Proof (i) follows from Corollary 2.15, so we only have to consider (ii).
(a) Let L' be a splitting field for A, B and C. Then, by Corollary 2.14, it suffices to show that

$$[\mathcal{A}^{\mathrm{ass}} : \mathcal{A}^\circ]^2_{\mathcal{O}_K} d_C \mathcal{O}_{L'} = d_B \prod_{\chi \in \hat{G}} (c,\chi)^2_{\gamma_0} \mathcal{O}_{L'}\,, \tag{34}$$

with $\mathcal{A}^\circ = (\mathcal{O}_{\bar{F}}G)^\Omega$. By assumption

$$(c,\chi)_{\gamma_0} \sim \pi^m \,,$$

for each $\chi \in \hat{G}$. On the other hand [Ch, Lemma 3.1] implies that $d_C \sim \pi^{mq^m}$. It therefore suffices to show

$$[\mathcal{A}^{\mathrm{ass}} : \mathcal{A}^\circ]^2_{\mathcal{O}_K} = d_B \pi^{mq^m} \,. \tag{35}$$

In order to prove this equality we split the above index and show

$$[\mathcal{O}_{L'} \otimes_{\mathcal{O}_K} \mathcal{A}^{\mathrm{ass}} : \mathcal{O}_{L'}G]^2_{\mathcal{O}_{L'}} = \pi^{mq^m}\mathcal{O}_{L'} \tag{36}$$

and

$$[\mathcal{O}_{L'}G : \mathcal{O}_{L'} \otimes_{\mathcal{O}_K} \mathcal{A}^\circ]^2_{\mathcal{O}_{L'}} = d_B \mathcal{O}_{L'} \,. \tag{37}$$

Equation (37) follows immediately if we recall from Lemma 2.1 that the elements

$$\sum_{\omega \in \Omega/\mathrm{stab}_\Omega(g_i)} \omega(x_{i,j}) \, {}^\omega g_i \qquad (1 \leqslant i \leqslant r,\ 1 \leqslant j \leqslant r_i)$$

constitute an $\mathcal{O}_K$-basis of $\mathcal{A}^\circ$, where $\{g_1, \dots, g_r\} \subseteq G$ is a set of representatives for the Ω-orbits of G and $x_{i,1}, \dots, x_{i,r_i}$ is an $\mathcal{O}_K$-basis of $\mathcal{O}_{K_i}$, for K_i being the fixed field of $\mathrm{stab}_\Omega(g_i)$.

The proof of (36) follows very closely the proof of [CT, Ch. X, Thm. 4.1]. The $\mathcal{O}_{L'}$-basis $g_0 \cup \{g - g_0 \mid g \in G \setminus \{g_0\}\}$ of $\mathcal{O}_{L'}G$ is transformed to the $\mathcal{O}_{L'}$-basis $1 \otimes g_0 \cup \{1 \otimes \sigma_i \mid i = 0, \dots, q^m - 2\}$ of $\mathcal{O}_{L'} \otimes_{\mathcal{O}_K} \mathcal{A}^{\mathrm{ass}}$ by means of the matrix

$$S = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & {\pi'^{(m)}}^{-1} & \cdots & {\pi'^{(m)}}^{-1} \\ 0 & {\pi'^{(m)}}^{-1} g_1 & \cdots & {\pi'^{(m)}}^{-1} g_N \\ \vdots & \vdots & & \vdots \\ 0 & {\pi'^{(m)}}^{-1} g_1^{N-1} & \cdots & {\pi'^{(m)}}^{-1} g_N^{N-1} \end{pmatrix} ,$$

where we have set $G = \{g_0, g_1, \dots, g_N\}$ with $N = q^m - 1$. Recall that $\pi'^{(m)} \sim \pi^m$. By the Weierstrass Preparation Theorem we may write $f^{(m)}(X) = h_m(X)u(X)$ with a distinguished polynomial $h_m(X)$ and a unit $u(X) \in \mathcal{O}_L[[X]]^\times$. Since

$$\frac{h_m(X)}{X} = \prod_{j=1}^{N} (X - g_j) \,,$$

we conclude by Vandermonde that

$$\det(S)^2 \sim \pm\pi^{-2mN} \cdot \prod_{j=1}^{N} \left(\frac{d}{dX} \frac{h_m(X)}{X} \right)\Bigg|_{X=g_j} = \pm\pi^{-2mN} \cdot \prod_{j=1}^{N} \frac{h'_m(g_j)}{g_j}.$$

Adapting the proof of [CT, Ch. X, Lemma 2.5] we can show that $h'_m(g_j) \sim \pi'^{(m)}$ for $j = 1, \ldots, N$. Furthermore $\prod_{j=1}^{N} g_j$ is associated to the leading coefficient of $f^{(m)}(X)$, which is $\pi'^{(m)}$. Summing up we obtain

$$\det(S)^2 \sim \pm\pi^{-2mN} \cdot \pi^{mN-m} = \pi^{-mq^m} ,$$

which proves (36).

(b) It follows from Theorem 4.11 together with (32) that for $c = c_\theta$ we have $(c, \chi)_{\gamma_0} \sim \pi^m$ for all $\chi \in \hat{G}$. By (a) we conclude that $\mathcal{C} = c \cdot \mathcal{A}^{\mathrm{ass}}$. Note that $v_L(\theta) = q^m - 1$ since γ_0 (resp. β) is a uniformizing element in L (resp. K).

Let $x \in N^\times$ have $\mathfrak{p}_L$-valuation $q^m - 1$. Since L/K is totally ramified of degree q^m, there exists a unit $u \in \mathcal{O}_K^\times$ such that

$$x \equiv u\theta \pmod{\mathfrak{p}_K \mathcal{O}_L} \quad \text{resp.} \quad c_x \equiv uc_\theta \pmod{\mathfrak{p}_K \mathcal{C}} .$$

Together with (33) this implies

$$\mathcal{C} = c_x \cdot \mathcal{A}^{\mathrm{ass}} + \mathfrak{p}_L \mathcal{C} .$$

Now the full statement in (b) is a consequence of Nakayama's Lemma. □

We now have a closer look at the associated order when $F = \mathbb{Q}_p$. The next theorem should be compared to Theorem 3.1 and [CT, Ch. X, Th. 4.1].

Theorem 4.13 *Let $F = \mathbb{Q}_p$ and assume that $r \geq 1$. Then $\mathcal{A}^{\mathrm{ass}}$ is the maximal order $\mathcal{A}$ in A, and $d_A = \mathcal{O}_K$.*

Proof From Lemma 2.6 we know that

$$[\mathcal{A} : \mathcal{A}^\circ]^2_{\mathcal{O}_K} = d_B d_A^{-1} p^{mp^m} ,$$

whereas from (35) we obtain

$$[\mathcal{A}^{\mathrm{ass}} : \mathcal{A}^\circ]^2_{\mathcal{O}_K} = d_B p^{mp^m} .$$

Therefore $[\mathcal{A} : \mathcal{A}^{\mathrm{ass}}]^2_{\mathcal{O}_K} = d_A^{-1}$, which forces $\mathcal{A} = \mathcal{A}^{\mathrm{ass}}$ and $d_A = \mathcal{O}_K$. □

To conclude this Section we prove that $\mathcal{B}^{\mathrm{gs}}$ and $\mathcal{C}$ are naturally isomorphic as $\mathcal{A}^{\mathrm{gs}}$-modules after applying the functor $\mathcal{O}_L \otimes_{\mathcal{O}_K} \_$. In the terminology of [T2] or [BT] this means that $\mathcal{C}$ is a principal homogeneous space for $\mathcal{B}^{\mathrm{gs}}$. Note that $\mathcal{O}_L \otimes_{\mathcal{O}_K} \mathcal{B}^{\mathrm{gs}} = \mathcal{B}_L^{\mathrm{gs}}$ and $\mathcal{O}_L \otimes_{\mathcal{O}_k} \mathcal{A}^{\mathrm{gs}} = \mathcal{A}_L^{\mathrm{gs}}$.

Proposition 4.14 *Suppose that $r \geq 1$. Then the map $\xi' : B \to C$ defined by $\xi'(b)(\gamma) = b(\gamma -_f \gamma_0), b \in B, \gamma \in \Gamma$, induces an isomorphism*

$$\xi : \mathcal{O}_L \otimes_{\mathcal{O}_K} \mathcal{B}^{\mathrm{gs}} \longrightarrow \mathcal{O}_L \otimes_{\mathcal{O}_K} \mathcal{C}$$

of $\mathcal{A}_L^{\mathrm{gs}}$-modules.

Proof By Theorem 4.12(b) it suffices to show that $\xi^{-1}(c_\theta)$ generates $\mathcal{B}_L^{\mathrm{gs}}$ over $\mathcal{A}_L^{\mathrm{gs}}$. We write

$$\xi^{-1}(c_\theta) = \sum_{g\in G} \frac{1}{\pi'(m)} c_\theta(\gamma_0 +_f g) l'^g$$

with the map l' defined in (29). By the definition of c_θ we further compute

$$\begin{aligned} \xi^{-1}(c_\theta) &= \sum_{g\in G} \frac{1}{\pi'(m)} \theta^{\omega_g} l'^g \\ &= l' \cdot \sum_{g\in G} \frac{1}{\pi'(m)} \theta^{\omega_g} g. \end{aligned}$$

By Corollary 4.6 it remains to show that

$$\lambda := \sum_{g\in G} \frac{1}{\pi'(m)} \theta^{\omega_g} g \in (\mathcal{A}_L^{\mathrm{gs}})^*.$$

From the definition of θ we deduce

$$\theta^{\omega_g} = \left(\frac{f^{(m)}(\gamma_0)}{\gamma_0}\right)^{\omega_g} = \frac{f^{(m)}(\gamma_0 +_g g)}{\gamma_0 +_f g}.$$

Therefore $\theta^{\omega_g} = b(X)(g)$ with $b(X) = \frac{f^{(m)}(\gamma_0 +_g X)}{\gamma_0 +_f X} \in \mathcal{O}_L[[X]]$ and we conclude from (26) and Proposition 4.5 that $\lambda \in \mathcal{A}_L^{\mathrm{gs}}$. Mapping λ to its Wedderburn components (see Lemma 2.2(i)) we derive from (32) and Theorem 4.11 that λ is an invertible element of the maximal order $\mathcal{A}_L$. Hence the result follows from $(\mathcal{A}_L^{\mathrm{gs}} \cap \mathcal{A}^*) = (\mathcal{A}_L^{\mathrm{gs}})^*$. $\square$

5 Elliptic curves

5.1 A special class of elliptic curves

The purpose of this section is to introduce a special class of elliptic curves. General references for the theory of elliptic curves are the books of Silverman [Sil1] and [Sil2], in particular [Sil2, Ch. II] for CM-elliptic curves. We will follow very closely the exposition in [GS, §4] and [dS, Ch. II, 1].

Throughout this section k denotes a quadratic imaginary number field. For an integral ideal $\mathfrak{f}$ of k the ray class field of conductor $\mathfrak{f}$ is denoted by $k(\mathfrak{f})$. In particular we write $k(1)$ for the Hilbert class field.

Once and for all we fix an algebraic closure $\bar{\mathbb{Q}}$ of $\mathbb{Q}$ and an embedding $\bar{\mathbb{Q}} \hookrightarrow \mathbb{C}$. Via this embedding we view all number fields as subfields of $\mathbb{C}$.

For an abelian extension N/M of number fields and an integral ideal $\mathfrak{a}$ of M relatively prime to the conductor $\mathfrak{f}_{N/M}$ of N/M we denote the Artin symbol by $\sigma(\mathfrak{a})$ or $(\mathfrak{a}, N/M)$.

Let F be a finite abelian extension of k and let E be an elliptic curve defined over F with complex multiplication by the ring of integers $\mathcal{O}_k$. We fix a generalized Weierstrass model for E/F,

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \tag{38}$$

with $a_1, a_2, a_3, a_4, a_6 \in F$ and denote by $\omega = \omega_E = dx/(2y + a_1x + a_3)$ the standard invariant differential associated with (38).

In characteristics $\neq 2, 3$ we can replace x and y by

$$\wp = x + \frac{a_1^2 + 4a_2}{12}, \quad \wp' = 2y + a_1x + a_3,$$

and (38) is transformed to

$$(\wp')^2 = 4\wp^3 - g_2\wp - g_3 \text{ with } g_2, g_3 \in F. \tag{39}$$

The pair (E, ω_E) determines a complex lattice $\mathfrak{w} \subseteq \mathbb{C}$ which is characterized by

$$g_2(\mathfrak{w}) = g_2, \quad g_3(\mathfrak{w}) = g_3,$$

where, as usual,

$$g_2(\mathfrak{w}) = 60 \sum\nolimits'_{\omega\in\mathfrak{w}} \omega^{-4}, \quad g_3(\mathfrak{w}) = 140 \sum\nolimits'_{\omega\in\mathfrak{w}} \omega^{-6}$$

denote the coefficients in the differential equation of the Weierstass $\wp$-function.

Since E has complex multiplication by $\mathcal{O}_k$, the lattice $\mathfrak{w}$ is of the form $\Omega\mathfrak{a}$ with $\Omega \in \mathbb{C}^*$ and a fractional ideal $\mathfrak{a}$ of k. Once $\mathfrak{a}$ is fixed, Ω is uniquely determined up to a root of unity in k.

We denote by

$$\begin{aligned} \xi(\ ,\mathfrak{w}) : \mathbb{C}/\mathfrak{w} \quad &\longrightarrow \quad E(\mathbb{C}), \\ z + \mathfrak{w} \quad &\longmapsto \quad \begin{cases} [\wp(z \mid \mathfrak{w}), \wp'(z \mid \mathfrak{w}), 1], & \text{if } z \notin \mathfrak{w}, \\ [0, 1, 0], & \text{if } z \in \mathfrak{w}, \end{cases} \end{aligned} \tag{40}$$

the corresponding Weierstrass isomorphism.

Let $\theta : \mathcal{O}_k \to \mathrm{End}(E)$ be normalized in the sense of Shimura [Sh, 5.1], i.e. $\omega \circ \theta(\mu) = \mu\omega$ for $\mu \in \mathcal{O}_k$. Then

$$\theta(\mu)\,(\xi(z, \mathfrak{w})) = \xi(\mu z, \mathfrak{w}), \quad z \in \mathbb{C}, \mu \in \mathcal{O}_k. \tag{41}$$

For an integral ideal $\mathfrak{g}$ of k we define the group of $\mathfrak{g}$-torsion points of E by

$$E[\mathfrak{g}] = \{\xi(z, \mathfrak{w}) \mid z \in \mathfrak{g}^{-1}\mathfrak{w}/\mathfrak{w}\}.$$

Furthermore we write E_{tor} for the torsion subgroup of $E(\mathbb{C})$. From the fact that the j-invariant j_E of E generates the Hilbert class field $k(1)$ over k we derive $k(1) \subseteq F$. Therefore [Sil2, Th. 2.3] implies that $F(E[\mathfrak{g}])/F$ is abelian.

Let $\psi = \psi_{E/F}$ be the Groessencharacter associated to E/F and denote by $\mathfrak{f}_\psi$ its conductor. Thus ψ is a homomorphism from the group of all fractional ideals of F relatively prime to $\mathfrak{f}_\psi$ to k^*. For any principal ideal $\mathfrak{A} = (a)$ of F such that $a \equiv 1 \pmod{^* \mathfrak{f}_\psi}$ one has $\psi((a)) = \prod_{\sigma \in \mathrm{Gal}(F/k)} a^\sigma$.

Let $\mathfrak{A}$ be any integral ideal of F with $(\mathfrak{A}, \mathfrak{f}_\psi) = 1$. Then $\psi(\mathfrak{A}) \in \mathcal{O}_k$ and we have the formula

$$\xi(\rho, \mathfrak{w})^{\sigma(\mathfrak{A})} = \xi(\psi(\mathfrak{A})\rho, \mathfrak{w}) \tag{42}$$

for any $\rho \in \mathfrak{g}^{-1}\mathfrak{w}$, $(\mathfrak{g}, N_{F/k}(\mathfrak{A})) = 1$.

We now impose the following hypothesis on E:

$$F(E_{\mathrm{tor}}) \text{ is an abelian extension of } k. \tag{43}$$

By [Sh, Th. 7.44] this condition is equivalent to the existence of a Groessencharacter φ of k such that $\psi = \varphi \circ N_{F/k}$ (see also [GS, Th. 4.1]). Such a Groessencharacter φ is uniquely determined up to multiplication with an abelian character χ of $\mathrm{Gal}(L/k)$, where χ is regarded as a Dirichlet character of k ([GS, Remarque (4.2)]). Once and for all we fix such a φ and denote by

$$\mathfrak{f} = \mathrm{lcm}(\mathfrak{f}_\varphi, \mathfrak{f}_{F/k}) \tag{44}$$

the least common multiple of the conductors of φ and F/k. The ideal $\mathfrak{f}$ is in fact independent of the choice of φ (see [GS, p.197]) and only depends on E/F. Note also that φ satisfies $\varphi(\eta) = \eta$ for $\eta \equiv 1 \pmod{\mathfrak{f}}$, $\eta \in \mathcal{O}_k$.

Lemma 5.1 *Let φ be a Groessencharacter of k with conductor $\mathfrak{f}_\varphi$ and infinity type $(1,0)$ (i.e., $\varphi((\eta)) = \eta$ for all $\eta \in \mathcal{O}_k$ with $\eta \equiv 1 \pmod{\mathfrak{f}_\varphi}$). Then $w(\mathfrak{f}_\varphi) = 1$, where $w(\mathfrak{a}) = |\{\varepsilon \in \mathcal{O}_k \mid \varepsilon \equiv 1 \pmod{\mathfrak{a}}\}|$ for any integral $\mathcal{O}_k$-ideal $\mathfrak{a}$.*

Proof By setting $\varphi_f(a) := \varphi((a))/a$ we obtain a well-defined character $\varphi_f : (\mathcal{O}_k/\mathfrak{f}_\varphi)^* \to \mathbb{C}^*$. Let $W = \{\varepsilon \in \mathcal{O}_k{}^* \mid \varepsilon \equiv 1 \pmod{\mathfrak{f}_\varphi}\}$. Then we have an embedding

$$\mathcal{O}_k{}^*/W \hookrightarrow (\mathcal{O}_k/\mathfrak{f}_\varphi)^* .$$

For any $\eta \in \mathcal{O}_k{}^*$ we have $\varphi_f(\eta) = 1/\eta$. Since $|\mathcal{O}_k{}^*/W| = w(1)/w(\mathfrak{f}_\varphi)$ we necessarily have $\varphi_f(\eta)^{w(1)/w(\mathfrak{f}_\varphi)} = 1 = \left(\frac{1}{\eta}\right)^{w(1)/w(\mathfrak{f}_\varphi)}$. Since $\mathcal{O}_k{}^*$ is cyclic of order $w(1)$ we conclude that $w(\mathfrak{f}_\varphi) = 1$. □

Particular instances of this type of elliptic curves are the analytic models of Fueter, Deuring and Legendre in [CT], [Co], [Fl] and [Sch2]. See also the examples (4.5) in [GS].

Let $\mathfrak{a}$ be an integral ideal of k relatively prime to $\mathfrak{f}$. From [GS, (4.3),(4.6)] one deduces the existence of a unique isogeny

$$\lambda(\mathfrak{a}) : E \longrightarrow E^{\sigma(\mathfrak{a})} \tag{45}$$

characterized by the property

$$P^{\sigma(\mathfrak{a})} = \lambda(\mathfrak{a})(P) \text{ for } P \in E[\mathfrak{g}], \quad (\mathfrak{g}, \mathfrak{a}) = 1. \tag{46}$$

Since ω is a F-basis for the space of differentials of the first kind, we may define the quantity $\Lambda(\mathfrak{a}) \in F$ by

$$\omega^{\sigma(\mathfrak{a})} \circ \lambda(\mathfrak{a}) = \Lambda(\mathfrak{a})\omega.$$

We write $\mathfrak{w}_\mathfrak{a}$ for the lattice which corresponds to the couple $(E^{\sigma(\mathfrak{a})}, \omega^{\sigma(\mathfrak{a})})$.

Proposition 5.2 *[GS, Prop. (4.10)]*

(i) For an integral ideal $\mathfrak{a}$ of k relatively prime to $\mathfrak{f}$ the map $\mathfrak{a} \mapsto \Lambda(\mathfrak{a})$ is characterized by the following commutative diagram:

$$\begin{array}{ccc} \mathbb{C}/\mathfrak{w} & \xrightarrow{\xi(\cdot,\mathfrak{w})} & E(\mathbb{C}) \\ {\scriptstyle \cdot\Lambda(\mathfrak{A})}\downarrow & & \downarrow{\scriptstyle \lambda(\mathfrak{a})} \\ \mathbb{C}/\mathfrak{w}_\mathfrak{a} & \xrightarrow{\xi(\cdot,\mathfrak{w}_\mathfrak{a})} & E^{\sigma(\mathfrak{a})}(\mathbb{C}) \end{array}$$

(ii) For all $\mathfrak{a}$ as above, $\mathfrak{w}_\mathfrak{a} = \Lambda(\mathfrak{a})\mathfrak{a}^{-1}\mathfrak{w}$.

(iii) Let $\mathfrak{g}$ be an integral ideal of k such that $\mathfrak{f} \mid \mathfrak{g}$. Then one has for all $\rho \in \mathfrak{g}^{-1}\mathfrak{w}$

$$\xi(\rho, \mathfrak{w})^{\sigma(\mathfrak{a})} = \xi(\Lambda(\mathfrak{a})\rho, \mathfrak{w}_\mathfrak{a}).$$

(iv) If $\mathfrak{a}$ and $\mathfrak{b}$ are two integral ideals of k such that $(\mathfrak{a}, \mathfrak{b}) = 1$, $(\mathfrak{a}\mathfrak{b}, \mathfrak{f}) = 1$, then

$$\Lambda(\mathfrak{a}\mathfrak{b}) = \Lambda(\mathfrak{a})^{\sigma(\mathfrak{b})}\Lambda(\mathfrak{b}) = \Lambda(\mathfrak{a})\Lambda(\mathfrak{b})^{\sigma(\mathfrak{a})} \tag{47}$$

□

There is a unique way to extend the definition of Λ to the whole group of fractional ideals relatively prime to $\mathfrak{f}$ such that (47) remains valid. Namely we have to set

$$\Lambda(\mathfrak{a}^{-1})^{\sigma(\mathfrak{a})} = \frac{1}{\Lambda(\mathfrak{a})}. \tag{48}$$

This extension will again be called Λ.

The following proposition gives the precise class field theoretical description of the fields generated by the $\mathfrak{g}$-torsion points for $\mathfrak{f} \mid \mathfrak{g}$.

Proposition 5.3 *[GS, Lemme (4.7)] Let $\mathfrak{g}$ be an integral ideal of k divisible by $\mathfrak{f}$. Then $F(E[\mathfrak{g}]) = k(\mathfrak{g})$.*

□

In the rest of this section we will concentrate on relative extensions $F(E[\mathfrak{f}\mathfrak{p}^{r+m}])/F(E[\mathfrak{f}\mathfrak{p}^r])$ with $r, m \geq 1$ and a prime ideal $\mathfrak{p}$ of k. In particular we will work out the values for φ, Λ and λ for $\mathfrak{a}$ such that $(\mathfrak{a}, F/k) = 1$ in greater detail.

Lemma 5.4 *Let $\mathfrak{a}$ be an integral ideal of k relatively prime to $\mathfrak{f}$ such that $(\mathfrak{a}, F/k) = 1$. Then:*
(i) $\Lambda(\mathfrak{a}) \in k^*$, $\Lambda(\mathfrak{a})\mathcal{O}_k = \mathfrak{a}$ *and* $\mathfrak{w} = \mathfrak{w}_\mathfrak{a}$.
(ii) $\lambda(\mathfrak{a}) = \theta(\Lambda(\mathfrak{a}))$.
(iii) $\Lambda(\mathfrak{a}) = \varphi(\mathfrak{a})$, *in particular* $\Lambda(\eta) = \eta$ *for* $\eta \equiv 1 \pmod{\mathfrak{f}}$, $\eta \in \mathcal{O}_k$.

Proof Let $\mathfrak{b}$ be any integral ideal of k such that $(\mathfrak{af}, \mathfrak{b}) = 1$. From Proposition 5.2 (iv) we obtain

$$\Lambda(\mathfrak{ab}) = \Lambda(\mathfrak{a})^{\sigma(\mathfrak{b})}\Lambda(\mathfrak{b}) = \Lambda(\mathfrak{a})\Lambda(\mathfrak{b})^{\sigma(\mathfrak{a})} = \Lambda(\mathfrak{a})\Lambda(\mathfrak{b}).$$

Hence $\Lambda(\mathfrak{a})^{\sigma(\mathfrak{b})} = \Lambda(\mathfrak{a})$, which implies $\Lambda(\mathfrak{a}) \in k^*$. From $E^{\sigma(\mathfrak{a})} = E$ and $\omega^{\sigma(\mathfrak{a})} = \omega$ we derive $\mathfrak{w}_\mathfrak{a} = \mathfrak{w}$ and $\Lambda(\mathfrak{a})\mathcal{O}_k = \mathfrak{a}$.

The commutative diagram of Proposition 5.2 (i) implies that

$$\lambda(\mathfrak{a})\,(\xi(z, \mathfrak{w})) = \xi(\Lambda(\mathfrak{a})z, \mathfrak{w}) = \theta(\Lambda(\mathfrak{a}))(\xi(z, \mathfrak{w})).$$

From this (ii) is immediate.

The cocycle relation (47) implies that Λ is multiplicative on the set of ideals $\mathfrak{a}$ with $(\mathfrak{a}, F/k) = 1$. Let φ' be any extension of Λ to a Groessencharacter of k. For any integral ideal $\mathfrak{A}$ of F we have

$$\begin{aligned} \xi(\rho, \mathfrak{w})^{\sigma(\mathfrak{A})} &= \xi(\rho, \mathfrak{w})^{\sigma(N_{F/k}(\mathfrak{A}))} \\ &= \xi(\Lambda(N_{F/k}(\mathfrak{A}))\rho, \mathfrak{w}), \end{aligned}$$

where $\rho \in \mathfrak{g}^{-1}\mathfrak{w}$ for any integral $\mathcal{O}_k$-ideal $\mathfrak{g}$ with $(\mathfrak{g}, N_{F/k}(\mathfrak{A})) = 1$.

By the defining property of $\psi_{E/F}$ we obtain $\Lambda \circ N_{F/k} = \psi_{E/F}$ and thus also $\varphi' \circ N_{F/k} = \psi_{E/F}$. Therefore φ' is of the form $\varphi' = \varphi\chi$ for a character χ of $\mathrm{Gal}(F/k)$. But then $\Lambda(\mathfrak{a}) = \varphi'(\mathfrak{a}) = \varphi(\mathfrak{a})\chi(\mathfrak{a}) = \varphi(\mathfrak{a})$ for any $\mathfrak{a}$ such that $(\mathfrak{a}, F/k) = 1$. □

Remark 5.5 From (48) it is clear that (i) and (iii) are also valid for any fractional ideal $\mathfrak{a}$ of k relatively prime to $\mathfrak{f}$ such that $(\mathfrak{a}, F/k) = 1$.

Corollary 5.6 *Let $\mathfrak{g}$ be an integral ideal of k divisible by $\mathfrak{f}$. Let Q be a primitive $\mathfrak{g}$-torsion point of E. Then $F(Q) = k(\mathfrak{g})$.*

Proof From Proposition 5.3 we know $F(Q) \subseteq k(\mathfrak{g})$. Let $\mathfrak{a}$ be an integral ideal of k such that $\sigma(\mathfrak{a})\mid_{F(Q)} = 1$. Let $\rho \in \mathfrak{g}^{-1}\mathfrak{w}$ be such that $Q = \xi(\rho, \mathfrak{w})$. By (46) and Lemma 5.4(ii) we obtain $Q^{\sigma(\mathfrak{a})} = \xi(\Lambda(\mathfrak{a})\rho, \mathfrak{w})$. Hence $\xi(\Lambda(\mathfrak{a})\rho, \mathfrak{w}) = \xi(\rho, \mathfrak{w})$ and since Q is primitive, this implies $\Lambda(\mathfrak{a}) \equiv 1 \pmod{\mathfrak{g}}$. Let $Q_1 = \xi(\rho_1, \mathfrak{w})$ be an arbitrary $\mathfrak{g}$-torsion point. Then $\rho_1 \in \mathfrak{g}^{-1}\mathfrak{w}$ and

$$Q_1^{\sigma(\mathfrak{a})} = \xi(\Lambda(\mathfrak{a})\rho_1, \mathfrak{w}) = \xi(\rho_1, \mathfrak{w}) = Q_1.$$

Therefore $\sigma(\mathfrak{a})$ fixes $F(E[\mathfrak{g}]) = k(\mathfrak{g})$, and thus $F(Q) = k(\mathfrak{g})$. □

For a prime ideal $\mathfrak{P}$ of F we denote the $\mathfrak{P}$-adic valuation by $v_\mathfrak{P}$.

Corollary 5.7 *Let $\mathfrak{p}$ be a prime ideal of k such that $\mathfrak{p} \not| \mathfrak{f}$. Then $v_{\mathfrak{P}}(\mathfrak{p}\mathcal{O}_F) = v_{\mathfrak{P}}(\Lambda(\mathfrak{p}))$ for all $\mathfrak{P} \mid \mathfrak{p}$.*

Proof Let $n \in \mathbb{N}$ be such that $(\mathfrak{p}^n, F/k) = 1$. Then Lemma 5.4 (i) and Proposition 5.2 (iv) impliy

$$\mathfrak{p}^n\mathcal{O}_F = \Lambda(\mathfrak{p}^n)\mathcal{O}_F = \Lambda(\mathfrak{p})\Lambda(\mathfrak{p})^{\sigma(\mathfrak{p})} \cdots \Lambda(\mathfrak{p})^{\sigma(\mathfrak{p})^{n-1}}.$$

One deduces that $v_{\mathfrak{P}}(\mathfrak{p}\mathcal{O}_F) = v_{\mathfrak{P}}(\Lambda(\mathfrak{p}))$, since $\sigma(\mathfrak{p})$ is an element of the decomposition group $G_{\mathfrak{P}}$ for all $\mathfrak{P}$ above $\mathfrak{p}$. □

Let now $\mathfrak{p}$ be a prime ideal of k such that $(\mathfrak{p}, \mathfrak{f}) = 1$. Let $\mathfrak{P}$ denote a prime of F above $\mathfrak{p}$. Since E has good reduction at $\mathfrak{P}$, we can fix a Weierstrass model (38) over the localization $\mathcal{O}_{F,\mathfrak{P}}$ of $\mathcal{O}_F$ at $\mathfrak{P}$ such that $\Delta \in \mathcal{O}_{F,\mathfrak{P}}^*$.

In the following we will work out the connection to the relative Lubin-Tate theory as it was presented in Section 5.

We view E as an elliptic curve over the completion $\mathcal{O}_{F_{\mathfrak{P}}}$ and denote by $\hat{E}$ the one-parameter formal group of E with respect to the parameter

$$z = -\frac{x}{y}$$

(see [Sil1, Ch.IV]).

Lemma 5.8 *[dS, CH.II,1.10] $\hat{E}$ is a relative Lubin-Tate group with respect to the unramified extension $F_{\mathfrak{P}}/k_{\mathfrak{p}}$ associated with the parameter $\Lambda(\mathfrak{p})$.*

Proof Let $\phi = \sigma(\mathfrak{p})$ be the Frobenius automorphism of $F_{\mathfrak{P}}/k_{\mathfrak{p}}$. The isogeny $\lambda(\mathfrak{p}) : E \to E^{\phi}$ induces a homomorphism of formal groups

$$\widehat{\lambda(\mathfrak{p})} : \hat{E} \longrightarrow \hat{E^{\phi}}.$$

We put $q = N_{F/\mathbb{Q}}(\mathfrak{P})$. It follows from (46) that $\lambda(\mathfrak{p})$ gives the q-power Frobenius on the reduction of the curve modulo $\mathfrak{P}$. Therefore one has

$$\widehat{\lambda(\mathfrak{p})}(z) \equiv z^q \pmod{\mathfrak{P}}. \tag{49}$$

The invariant differential $\omega = dx/(2y + a_1x + a_3)$ has an expression

$$\omega(z) = (1 + a_1z + O(z^2))dz.$$

Since $\lambda(\mathfrak{p})$ is unramified we can write

$$\widehat{\lambda(\mathfrak{p})}(z) = b_1z + O(z^2), \quad b_1 \in \mathcal{O}_{F_{\mathfrak{P}}}.$$

From $(\omega \circ \widehat{\lambda(\mathfrak{p})})(z) = \Lambda(\mathfrak{p})\omega(z)$ we obtain the equality

$$(1 + a_1b_1z + O(z^2))d(b_1z + O(z^2)) = (\Lambda(\mathfrak{p}) + O(z))dz,$$

and therefore $b_1 = \Lambda(\mathfrak{p})$. This implies

$$\widehat{\lambda(\mathfrak{p})}(z) \equiv \Lambda(\mathfrak{p})z \pmod{\deg 2}. \tag{50}$$

By (49), (50), [dS, ChI, Th. 1.3] and Corollary 5.7 we conclude that $\hat{E}$ is the unique relative Lubin-Tate group with respect to $F_{\mathfrak{P}}/k_{\mathfrak{p}}$ associated with the parameter $\Lambda(\mathfrak{p})$. □

5.2 Modules associated with elliptic curves

In this section we will use the special class of elliptic curves discussed in the previous section to produce interesting and non-trivial examples that fit into the framework of Section 1. We adopt the notation of Section 5.1. So k is a quadratic imaginary number field and F/k a finite abelian extension. E/F denotes an elliptic curve with complex multiplication by $\mathcal{O}_k$ and such that $F(E_{\mathrm{tor}})/k$ is abelian. Let $\mathfrak{p}$ be a prime ideal of k such that $(\mathfrak{p}, \mathfrak{f}) = 1$, where $\mathfrak{f}$ is the integral ideal of k defined in (44). The extensions that we will consider are in most cases relative ray class field extensions of the form $k(\mathfrak{f}\mathfrak{p}^{r+m})/k(\mathfrak{f}\mathfrak{p}^r)$ with integers $r, m \geq 1$. This kind of extension was already studied by Ph. Cassou-Noguès and M.J. Taylor [CT] and R. Schertz [Sch2] under the additional Kummer condition $m \leq r$. In this case the module structure we introduced in Section 1 coincides with classical Galois module structure and we will recover (parts of) their results.

Let $r \geq 0, m \geq 1$ be rational integers. We set $G = E[\mathfrak{p}^m]$. Fix a primitive $\mathfrak{p}^{r+m}$-torsion point $Q_0 = \xi(\rho_0, \mathfrak{w})$, $\rho_0 \in \mathfrak{p}^{-r-m}\mathfrak{w}$, of E and put

$$\Gamma = \{Q_0 +_E P \mid P \in G\}.$$

In the sequel we will use the more convenient notation notation $[\alpha]$ instead of $\theta(\alpha)$ for the endomorphism of E corresponding to $\alpha \in \mathcal{O}_k$.

If $\mathfrak{p} = (\pi)$ is principal, then Γ is just the set of "π^m-th roots" of the primitive π^r-torsion point $P_0 = [\pi^m](Q_0)$, namely

$$\Gamma = \{Q \in E(\bar{\mathbb{Q}}) \mid [\pi^m](Q) = P_0\}.$$

In the following we will write

$$F_s = F(E[\mathfrak{f}\mathfrak{p}^s]) = k(\mathfrak{f}\mathfrak{p}^s) \text{ for } s \in \mathbb{N}.$$

The case $r = 0$ is completely settled by Corollary 2.15. Therefore we henceforth assume $r \geq 1$ unless stated otherwise.

We consider F_r as our base field and set

$$K = F_r, \quad \Omega = \Omega_K, \quad L = F_{r+m}.$$

From class field theory we know that $[k(\mathfrak{f}\mathfrak{p}^s) : k(1)] = \frac{w(1)}{w(\mathfrak{f}\mathfrak{p}^s)}\Phi(\mathfrak{f}\mathfrak{p}^s)$ with the Euler function Φ for the ring $\mathcal{O}_k$. Therefore Lemma 5.1 implies

$$[L : K] = N_{k/\mathbb{Q}}(\mathfrak{p}^m).$$

Lemma 5.9 *Let $r \geq 1$. Then one has*

$$\begin{array}{ll} (i) & L = K(Q_0). \\ (ii) & \Gamma = \{Q_0^\sigma \mid \sigma \in \mathrm{Gal}(L/K)\}. \end{array}$$

In particular, Ω acts on Γ.

Proof From Corollary 5.6 and Proposition 5.3 we deduce

$$L = F_{r+m} = F(E[\mathfrak{f}], Q_0) = k(\mathfrak{f})(Q_0) = F_r(Q_0) = K(Q_0).$$

For the proof of (ii) first note that

$$\mathrm{Gal}(L/K) = \{\sigma(1+\eta) \mid \eta \in \mathfrak{f}\mathfrak{p}^r/\mathfrak{f}\mathfrak{p}^{r+m}\}.$$

For $\eta \in \mathfrak{f}\mathfrak{p}^r$ we obtain

$$\begin{aligned} Q_0^{\sigma(1+\eta)} &= \xi(\rho_0, \mathfrak{w})^{\sigma(1+\eta)} \\ &= \xi(\rho_0 + \rho_0\eta, \mathfrak{w}) \\ &= \xi(\rho_0, \mathfrak{w}) +_E \xi(\eta\rho_0, \mathfrak{w}) \\ &= Q_0 +_E \xi(\eta\rho_0, \mathfrak{w}). \end{aligned} \tag{51}$$

Since $\eta\rho_0 \in \mathfrak{f}\mathfrak{p}^{-m}\mathfrak{w} \subseteq \mathfrak{p}^{-m}\mathfrak{w}$ we derive $\xi(\eta\rho_0, \mathfrak{w}) \in G$. From (i) we already know that the conjugates are mutually distinct, and therefore the map

$$\begin{aligned} \mathfrak{f}\mathfrak{p}^r/\mathfrak{f}\mathfrak{p}^{r+m} &\longrightarrow G, \\ \eta + \mathfrak{f}\mathfrak{p}^{r+m} &\longmapsto \xi(\eta\rho_0, \mathfrak{w}) \end{aligned}$$

is injective. Now (ii) is implied by $|G| = N_{k/\mathbb{Q}}(\mathfrak{p}^m) = [L : K]$.

Finally we remark that by Proposition 5.3 the action of Ω on Γ factors through Ω_L. Thus the "in particular" statement follows from (ii). □

We set

$$A = (\bar{K}G)^\Omega, \quad B = \mathrm{Map}(G, \bar{K})^\Omega, \quad C = \mathrm{Map}(\Gamma, \bar{K})^\Omega$$

and are now exactly in the set-up of Section 1.

We consider the K-algebra homomorphism

$$\tau : C \longrightarrow L, \quad f \longmapsto f(Q_0). \tag{52}$$

Since Ω acts transitively on Γ, τ is in fact an isomorphism of K-algebras (Lemma 2.11).

From (51) we obtain a bijection

$$\begin{aligned} \varphi : G &\longrightarrow \mathrm{Gal}(L/K), \\ \xi(\beta, \mathfrak{w}) &\longmapsto \sigma(1 + \frac{\beta}{\rho_0}), \quad \beta \in \mathfrak{p}^{-m}\mathfrak{f}\mathfrak{w}. \end{aligned} \tag{53}$$

We endow L via the isomorphism τ with the structure of an A-module. Explicitly this means for $\alpha \in L$ and $\sum_{g \in G} a_g g$

$$\alpha \cdot \sum_{g \in G} a_g g = \sum_{g \in G} a_g \alpha^{\sigma(1+\beta_g/\rho_0)}, \tag{54}$$

where we have set $g = \xi(\beta_g, \mathfrak{w})$, $\beta_g \in \mathfrak{p}^{-m}\mathfrak{f}\mathfrak{w}$.

Note that for $m > r$ this new module structure does not coincide with the usual Galois module structure. However, under the additional Kummer condition $m \leq r$ we are in the classical situation studied by [CT] and [Sch2].

Lemma 5.10 *Suppose that $r \geq m \geq 1$.*
(i) One has $A = KG$.
(ii) φ is a group isomorphism.
(iii) Identifying G and $\mathrm{Gal}(L/K)$ via φ the map τ is an isomorphism of A-modules.

Proof If $m \leq r$ we have $G \subseteq K = F_r$ and therefore (i) is evident. Let $\beta_1, \beta_2 \in \mathfrak{p}^{-m}\mathfrak{f}\mathfrak{w}$. Then $\beta_1\beta_2/\rho_0^2 \in \mathfrak{f}\mathfrak{p}^{r+m}$ and we obtain

$$\begin{aligned}\varphi(\xi(\beta_1, \mathfrak{w})) \cdot \varphi(\xi(\beta_2, \mathfrak{w})) &= \sigma(1 + \beta_1/\rho_o) \cdot \sigma(1 + \beta_2/\rho_0) \\ &= \sigma(1 + \frac{\beta_1 + \beta_2}{\rho_0} + \frac{\beta_1\beta_2}{\rho_0^2}) \\ &= \sigma(1 + \frac{\beta_1 + \beta_2}{\rho_0}) \\ &= \varphi(\xi(\beta_1 + \beta_2, \mathfrak{w})).\end{aligned}$$

Thus φ is a group homomorphism. (iii) is then immediate from (54). □

5.3 An analytic resolvent formula à la Schertz

One of the main sources for many results in the field of Galois module structure for rings of integers is the determination of some sort of resolvent (for instance see [CT, Ch. VI], [Fr2] or [Sch2]).

We will use the analytic resolvent function of Schertz [Sch2, §3], since it seems to be best suited for our applications. As already Schertz remarked in [Sch2, Bemerkungen (3), p. 283], his analytic resolvent function produces also some kind of arithmetical resolvent in the case $m > r$, but it can no longer be interpreted as a Galois resolvent. In fact, this is exactly the resolvent that we need in our context.

Let $\mathfrak{w} = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$, $\mathrm{Im}(\frac{\omega_1}{\omega_2}) > 0$, be a complex lattice. We write

$$\sigma(z \mid \mathfrak{w}) = z \prod_{\omega \in \mathfrak{w}, \omega \neq 0} (1 - \frac{z}{\omega}) e^{\frac{z}{\omega} + \frac{1}{2}(\frac{z}{\omega})^2}, \quad z \in \mathbb{C},$$

for the Weierstrass σ-function and define the Dedekind η-function by

$$\eta(\tau) = q_\tau^{1/24} \prod_{n=1}^{\infty} (1 - q_\tau^n), \quad \mathrm{Im}(\tau) > 0,$$

where $q_\tau = e^{2\pi i \tau}$. Finally we denote by

$$\zeta(z \mid \mathfrak{w}) = \frac{1}{z} + \sum_{\omega \in \mathfrak{w}, \omega \neq 0} \left(\frac{1}{z - \omega} + \frac{1}{\omega} + \frac{z}{\omega^2} \right), \quad z \in \mathbb{C},$$

the Weierstrass ζ-function and put

$$\eta_1 = 2\zeta(\frac{\omega_1}{2} \mid \mathfrak{w}), \quad \eta_2 = 2\zeta(\frac{\omega_2}{2} \mid \mathfrak{w})$$

for the basic quasi-periods of ζ.

The resolvents that we are interested in are resolvents of certain elliptic units (or elliptic $\mathfrak{p}$-units). These elliptic units are defined as singular values of the following normalization of the Weierstrass σ-function:

$$\varphi\left(z\,\middle|\,\begin{matrix}\omega_1\\ \omega_2\end{matrix}\right) = 2\pi i\exp(-(a_1\eta_1+a_2\eta_2)\frac{z}{2})\sigma\left(z\,|\mathfrak{w}\right)\eta^2(\frac{\omega_1}{\omega_2})\omega_2^{-1},$$

where the real numbers a_1, a_2 are uniquely determined by $z = a_1\omega_1 + a_2\omega_2$.

For later reference we record the transformation formulas

$$\begin{aligned}&\varphi\left((a_1+b_1)\omega_1+(a_2+b_2)\omega_2\,\middle|\,\begin{matrix}\omega_1\\ \omega_2\end{matrix}\right)\\ =\ &(-1)^{b_1b_2+b_1+b_2}e^{-\frac{2\pi i}{2}(b_1a_2-b_2a_1)}\varphi\left(a_1\omega_1+a_2\omega_2\,\middle|\,\begin{matrix}\omega_1\\ \omega_2\end{matrix}\right)\end{aligned}\tag{55}$$

for $a_1, a_2 \in \mathbb{Q}$, $b_1, b_2 \in \mathbb{Z}$, and

$$\varphi\left((a_1,a_2)\begin{pmatrix}M\tau\\ 1\end{pmatrix}\,\middle|\,\begin{matrix}M\tau\\ 1\end{matrix}\right) = \varepsilon(M)^2\varphi\left((a_1,a_2)M\begin{pmatrix}\tau\\ 1\end{pmatrix}\,\middle|\,\begin{matrix}\tau\\ 1\end{matrix}\right)\tag{56}$$

for $a_1, a_2 \in \mathbb{Q}$, $\mathrm{Im}(\tau) > 0$, $M = \begin{pmatrix} a & b\\ c & d\end{pmatrix} \in \mathrm{Sl}_2(\mathbb{Z})$. Herein $\varepsilon(M)$ is the 24-th root of unity arising from the transformation formula of the Dedekind η-function (see e.g. [KL, pp.27/28]). Furthermore for $z = a_1\tau + a_2$, $\mathrm{Im}(\tau) > 0$, $a_1, a_2 \in \mathbb{Q}$, we have the q-expansion

$$\begin{aligned}&\varphi\left(z\,\middle|\,\begin{matrix}\tau\\ 1\end{matrix}\right)\\ =\ &-q_\tau^{\frac{1}{2}B_2(a_1)}e^{2\pi i a_2(a_1-1)/2}(1-q_z)\prod_{n=1}^{\infty}(1-q_\tau^n q_z)(1-q_\tau^n q_z^{-1}),\end{aligned}\tag{57}$$

where $B_2(X) = X^2 - X + \frac{1}{6}$ is the second Bernoulli polynomial and $q_z = e^{2\pi i z}$ (see [KL, p.29]).

Note that φ is homogenous of degree 0, i.e. $\varphi\left(\alpha z\,\middle|\,\begin{smallmatrix}\alpha\omega_1\\ \alpha\omega_2\end{smallmatrix}\right) = \varphi\left(z\,\middle|\,\begin{smallmatrix}\omega_1\\ \omega_2\end{smallmatrix}\right)$ for all $\alpha \in \mathbb{C}^*$. It is not a function of lattices, but depends on the choice of a basis ω_1, ω_2. Nevertheless we will write $\varphi\left(z\,|\mathfrak{w}\right)$ in the sequel. Moreover φ is non-meromorphic as a function of z. We therefore introduce the "analytic substitute"

$$\vartheta\left(z\,\middle|\,\begin{matrix}\omega_1\\ \omega_2\end{matrix}\right) = 2\pi i\exp(-\frac{1}{2}\frac{\eta_2}{\omega_2}z^2)\sigma\left(z\,|\mathfrak{w}\right)\eta^2(\frac{\omega_1}{\omega_2})\omega_2^{-1},\quad z\in\mathbb{C}.$$

This ϑ-function is homogenous of degree 0 and holomorphic for $z \in \mathbb{C}$ with simple zeroes in $z \in \mathfrak{w}$. By abuse of notation we write, as for the φ-function, $\vartheta\left(z\,|\mathfrak{w}\right)$ instead of $\vartheta\left(z\,\middle|\,\begin{smallmatrix}\omega_1\\ \omega_2\end{smallmatrix}\right)$.

From the transformation formula of the Weierstrass σ-function we deduce

$$\begin{aligned}\vartheta\left(z+\omega_1\left|\begin{matrix}\omega_1\\ \omega_2\end{matrix}\right.\right) &= -e^{-\frac{2\pi i}{\omega_2}(z+\frac{\omega_1}{2})}\vartheta\left(z\left|\begin{matrix}\omega_1\\ \omega_2\end{matrix}\right.\right),\\ \vartheta\left(z+\omega_2\left|\begin{matrix}\omega_1\\ \omega_2\end{matrix}\right.\right) &= -\vartheta\left(z\left|\begin{matrix}\omega_1\\ \omega_2\end{matrix}\right.\right)\end{aligned}$$

(see [BBC, Prop. 3.3]). ϑ is very closely related to the φ-function. The Legendre relation $\eta_2\omega_1 - \eta_1\omega_2 = 2\pi i$ implies

$$\vartheta\left(z\left|\begin{matrix}\omega_1\\ \omega_2\end{matrix}\right.\right) = e^{-\pi i a_1 \frac{z}{\omega_2}}\varphi\left(z\left|\begin{matrix}\omega_1\\ \omega_2\end{matrix}\right.\right). \tag{58}$$

Finally we introduce for $z = a_1\omega_1 + a_2\omega_2$, $a_1, a_2 \in \mathbb{R}$, the short hand

$$z^* = a_1\eta_1 + a_2\eta_2$$

and set

$$h_{\mathfrak{w}}(u,v) = uv^* - u^*v = 2\pi i(u_1v_2 - u_2v_1) \tag{59}$$

for $u = u_1\omega_1 + u_2\omega_2$, $v = v_1\omega_1 + v_2\omega_2$. The second equality follows immediately from the Legendre relation.

Proposition 5.11 *[Sch2, (3.19)] Let $\mathfrak{w} \subseteq \hat{\mathfrak{w}}$ be two complex lattices,*

$$\mathfrak{w} = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2, \quad \hat{\mathfrak{w}} = \mathbb{Z}\frac{\omega_1}{n_1} + \mathbb{Z}\frac{\omega_2}{n_2}, \quad \mathrm{Im}(\frac{\omega_1}{\omega_2}) > 0, n_1, n_2 \in \mathbb{N}.$$

(i) Let $z, \gamma \in \mathbb{C}$. Then

$$\exp\left(\frac{1}{2}h_{\mathfrak{w}}(\xi,\gamma)\right)\frac{\varphi(z+\gamma+\xi\,|\mathfrak{w})}{\varphi(z+\xi\,|\mathfrak{w})}$$

only depends on ξ modulo $\mathfrak{w}$.

(ii) Let χ be an abelian character of $\hat{\mathfrak{w}}/\mathfrak{w}$, uniquely determined by

$$\chi\left(\frac{\omega_1}{n_1}\right) = e^{2\pi i\mu_1/n_1}, \quad \chi\left(\frac{\omega_2}{n_2}\right) = e^{2\pi i\mu_2/n_2}, \quad \mu_1, \mu_2 \in \mathbb{Z},$$

and set $\delta_\chi = \frac{1}{[\hat{\mathfrak{w}}:\mathfrak{w}]}(\gamma + \mu_2\omega_1 - \mu_1\omega_2)$. Then

$$\begin{aligned}&\sum_{\xi\in\hat{\mathfrak{w}}/\mathfrak{w}} e^{\frac{1}{2}h_{\mathfrak{w}}(\xi,\gamma)}\frac{\varphi(z+\gamma+\xi\,|\mathfrak{w})}{\varphi(z+\xi\,|\mathfrak{w})}\bar{\chi}(\xi) =\\ &= e^{-\frac{1}{2}h_{\mathfrak{w}}(z,\mu_2\omega_1-\mu_1\omega_2)}\cdot\sqrt[12]{\frac{\Delta(\hat{\mathfrak{w}})}{\Delta(\mathfrak{w})}}\cdot\frac{\varphi(\gamma\,|\mathfrak{w})\,\varphi(z+\delta_\chi\,|\hat{\mathfrak{w}})}{\varphi(\delta_\chi\,|\hat{\mathfrak{w}})\,\varphi(z\,|\hat{\mathfrak{w}})}.\end{aligned}$$

Proof Part (i) follows easily from (55) and (59). The second part is just a reformulation of [Sch2, (3.19)]. For the convenience of the reader we give the details. We put

$$\begin{aligned}\mathfrak{w}' &= \frac{1}{\omega_2}\mathfrak{w} = \mathbb{Z}\tau + \mathbb{Z},\\ \hat{\mathfrak{w}}' &= \frac{1}{\omega_2}\hat{\mathfrak{w}} = \mathbb{Z}\frac{\tau}{n_1} + \mathbb{Z}\frac{1}{n_2}\end{aligned}$$

with $\tau = \frac{\omega_1}{\omega_2}$ and view χ as an abelian character of $\hat{\mathfrak{w}}'/\mathfrak{w}'$. We write $z' = \frac{z}{\omega_2}$, $\xi' = \frac{\xi}{\omega_2}$ and $\gamma' = \frac{\gamma}{\omega_2}$. Then [Sch2, (3.19)] reads as follows

$$\begin{aligned}&\sum_{\xi'\in\hat{\mathfrak{w}}'/\mathfrak{w}'} e^{2\pi i\gamma' a_1'(\xi')}\frac{\vartheta\left(z'+\xi'+\gamma' \left|\begin{smallmatrix}\tau\\1\end{smallmatrix}\right.\right)}{\vartheta\left(z'+\xi' \left|\begin{smallmatrix}\tau\\1\end{smallmatrix}\right.\right)}\bar{\chi}(\xi')\\ =\;& e^{2\pi i\mu_2 z'}\cdot n_2\cdot\left(\frac{\eta(n_2\tau/n_1)}{\eta(\tau)}\right)^2\cdot\frac{\vartheta\left(\gamma' \left|\begin{smallmatrix}\tau\\1\end{smallmatrix}\right.\right)\vartheta\left(n_2 z'+\delta' \left|\begin{smallmatrix}n_2\tau/n_1\\1\end{smallmatrix}\right.\right)}{\vartheta\left(\delta' \left|\begin{smallmatrix}n_2\tau/n_1\\1\end{smallmatrix}\right.\right)\vartheta\left(n_2 z' \left|\begin{smallmatrix}n_2\tau/n_1\\1\end{smallmatrix}\right.\right)}\end{aligned}$$

with $\delta' = \frac{1}{n_1}(\gamma' + \mu_2\tau - \mu_1)$ and $\xi' = a_1'(\xi')\tau + a_2'(\xi')$. Since ϑ is homogenous of degree 0 this implies

$$\begin{aligned}&\sum_{\xi\in\hat{\mathfrak{w}}/\mathfrak{w}} e^{2\pi i\frac{\gamma}{\omega_2}a_1(\xi)}\frac{\vartheta(z+\xi+\gamma\,|\mathfrak{w})}{\vartheta(z+\xi\,|\mathfrak{w})}\bar{\chi}(\xi)\\ =\;& e^{2\pi i\mu_2\frac{z}{\omega_2}}n_2\left(\frac{\eta(n_2\tau/n_1)}{\eta(\tau)}\right)^2\frac{\vartheta(\gamma\,|\mathfrak{w})\,\vartheta(z+\delta_\chi\,|\hat{\mathfrak{w}})}{\vartheta(\delta_\chi\,|\hat{\mathfrak{w}})\,\vartheta(z\,|\hat{\mathfrak{w}})},\end{aligned}$$

where we have set $\xi = a_1(\xi)\omega_1 + a_2(\xi)\omega_2$. From the equality

$$\Delta\left(\frac{\omega_1}{\omega_2}\right) = \left(\frac{2\pi i}{\omega_2}\right)^{12}\eta\left(\frac{\omega_1}{\omega_2}\right)^{24}$$

we derive

$$n_2\left(\frac{\eta(n_2\tau/n_1)}{\eta(\tau)}\right)^2 = \sqrt[12]{\frac{\Delta(\hat{\mathfrak{w}})}{\Delta(\mathfrak{w})}}.$$

Using (58) we now replace the ϑ-functions by the φ-functions. Then a long, but straight-forward computation proves (ii). □

5.4 Special values of the φ-function

In the following we will investigate the arithmetical nature of certain singular values of the φ-function. To that end we will apply the Shimura reciprocity law as it is presented in [St, §4]. We follow very closely the exposition of Schertz in [Sch2, §4].

Let $(m_1, m_2), (n_1, n_2) \in \mathbb{Z}^2$ and $f \in \mathbb{N}$ be such that $\frac{1}{f}(n_1, n_2) \notin \mathbb{Z}^2$ and consider the function

$$g(\tau) = \frac{\varphi\left(\frac{1}{f}(m_1, m_2)\left(\begin{smallmatrix}\tau\\1\end{smallmatrix}\right) \bigm| \begin{smallmatrix}\tau\\1\end{smallmatrix}\right)}{\varphi\left(\frac{1}{f}(n_1, n_2)\left(\begin{smallmatrix}\tau\\1\end{smallmatrix}\right) \bigm| \begin{smallmatrix}\tau\\1\end{smallmatrix}\right)}, \quad \operatorname{Im}(\tau) > 0.$$

From (55) and (56) we deduce that $g(\tau)$ is a modular function for the congruence subgroup

$$\Gamma(2f^2) = \left\{ M \in \mathrm{Sl}_2(\mathbb{Z}) \mid M \equiv \pm \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \pmod{2f^2} \right\}.$$

By (57) the q-expansion of $g(\tau)$ has coefficients in $\mathbb{Q}(\zeta_{2f^2})$.

Let $\mathfrak{a} = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$, $\operatorname{Im}(\frac{\omega_1}{\omega_2}) > 0$, be a fractional ideal of k and put $\omega = \frac{\omega_1}{\omega_2}$. From [St, Th. 3] we deduce

$$g(\omega) \in k(2f^2). \tag{60}$$

Let p be a rational prime relatively prime to $2f^2 d_{k/\mathbb{Q}}$ such that $p = \mathfrak{p}\bar{\mathfrak{p}}$ decomposes in $k/\mathbb{Q}$. Let B be an integral 2×2 matrix of determinant p such that $B\left(\begin{smallmatrix}\omega_1\\\omega_2\end{smallmatrix}\right)$ is a $\mathbb{Z}$-basis of $\bar{\mathfrak{p}}\mathfrak{a}$. Then the action of the Frobenius automorphism $\sigma(\mathfrak{p})$ on $g(\omega)$ is explicitly described by [St, Th. 3]. Namely

$$g(\omega)^{\sigma(\mathfrak{p})} = \left[g \circ pB^{-1}\right](B\omega). \tag{61}$$

The recipe for computing $g \circ pB^{-1}$ is explained in [St, pp.210/211]. We have to decompose the matrix pB^{-1} in the form

$$pB^{-1} = M_1 \begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix} M_2 \text{ with } M_1, M_2 \in \mathrm{Sl}_2(\mathbb{Z})$$

and may then use the associativity of the symbol $\circ$. For $(a_1, a_2) \in \mathbb{Q}^2$ such that $f(a_1, a_2) \in \mathbb{Z}^2$ and $M \in \mathrm{Sl}_2(\mathbb{Z})$ we obtain from (56)

$$\varphi\left((a_1, a_2)\begin{pmatrix}\tau\\1\end{pmatrix} \Bigm| \begin{matrix}\tau\\1\end{matrix}\right) \circ M = \varepsilon(M)^2 \varphi\left((a_1, a_2)M\begin{pmatrix}\tau\\1\end{pmatrix} \Bigm| \begin{matrix}\tau\\1\end{matrix}\right), \tag{62}$$

and (57) implies

$$\varphi\left((a_1, a_2)\begin{pmatrix}\tau\\1\end{pmatrix} \Bigm| \begin{matrix}\tau\\1\end{matrix}\right) \circ \begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix} = \varphi\left((a_1, a_2)\begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix}\begin{pmatrix}\tau\\1\end{pmatrix} \Bigm| \begin{matrix}\tau\\1\end{matrix}\right). \tag{63}$$

Using (62) and (63) we derive

$$\left[g \circ pB^{-1}\right](\tau) = \frac{\varphi\left(\frac{1}{f}(m_1, m_2)pB^{-1}\left(\begin{smallmatrix}\tau\\1\end{smallmatrix}\right) \bigm| \begin{smallmatrix}\tau\\1\end{smallmatrix}\right)}{\varphi\left(\frac{1}{f}(n_1, n_2)pB^{-1}\left(\begin{smallmatrix}\tau\\1\end{smallmatrix}\right) \bigm| \begin{smallmatrix}\tau\\1\end{smallmatrix}\right)}. \tag{64}$$

We are particularly interested in the action of elements $\sigma \in \mathrm{Gal}(k(2f^2)/k(1))$ on $g(\omega)$. Let $\lambda \in \mathcal{O}_k$ be relatively prime to $2f^2$. By the Tchebotarev density theorem we can find $\lambda_1 \in \mathcal{O}_k$ such that $\lambda \equiv \lambda_1 \pmod{2f^2}$, $(\lambda_1, 2fd_{k/\mathbb{Q}}) = 1$ and $(\lambda_1) = \mathfrak{p}$ is a prime of k which decomposes in $k/\mathbb{Q}$. Obviously $\sigma(\lambda) = \sigma(\lambda_1)$.

As a basis of $\bar{\mathfrak{p}}\mathfrak{a}$ we take $\bar{\lambda}_1\omega_1, \bar{\lambda}_1\omega_2$ and define B by

$$\bar{\lambda}_1 \begin{pmatrix} \omega_1 \\ \omega_2 \end{pmatrix} = B \begin{pmatrix} \omega_1 \\ \omega_2 \end{pmatrix}.$$

It follows that $p = \lambda_1\bar{\lambda}_1$ and $B\omega = \omega$. Therefore we obtain from (61) and (64)

$$g(\omega)^{\sigma(\lambda)} = \frac{\varphi\left(\frac{\lambda_1}{f}(m_1, m_2)\binom{\omega}{1} \,\middle|\, {\omega \atop 1}\right)}{\varphi\left(\frac{\lambda_1}{f}(n_1, n_2)\binom{\omega}{1} \,\middle|\, {\omega \atop 1}\right)}.$$

Since $\lambda_1 \equiv \lambda \bmod 2f^2$ we deduce from (55) the final formula

$$g(\omega)^{\sigma(\lambda)} = \frac{\varphi\left(\frac{\lambda}{f}(m_1, m_2)\binom{\omega}{1} \,\middle|\, {\omega \atop 1}\right)}{\varphi\left(\frac{\lambda}{f}(n_1, n_2)\binom{\omega}{1} \,\middle|\, {\omega \atop 1}\right)}, \quad \lambda \in \mathcal{O}_k, (\lambda, 2f^2) = 1. \tag{65}$$

Let now $\mathfrak{c}, \mathfrak{c}^*$ be two integral ideals of k such that $\left(\prod_{\mathfrak{p}|\mathfrak{c}} \mathfrak{p}\right) \mid \mathfrak{c}^* \mid \mathfrak{c}$ and let $\mathfrak{l}$ be an integral ideal such that $(\mathfrak{l}, \mathfrak{c}\bar{\mathfrak{c}}) = 1$. We set $l = \min(\mathbb{N} \cap \mathfrak{l})$ and put

$$\mathfrak{g} = \mathfrak{l}\mathfrak{c}, \quad \mathfrak{g}^* = \mathfrak{l}\mathfrak{c}^*.$$

We decompose all occuring ideals into a rational and primitive part such that

$$\begin{array}{rcll} \mathfrak{l} & = & l_1(\mathbb{Z}\alpha + \mathbb{Z}l_2), & \\ \mathfrak{c} & = & c_1(\mathbb{Z}\alpha + \mathbb{Z}c_2), & \\ \mathfrak{c}^* & = & c_1^*(\mathbb{Z}\alpha + \mathbb{Z}c_2^*), & \\ \mathfrak{g} & = & g_1(\mathbb{Z}\alpha + \mathbb{Z}g_2), & g_1 = l_1c_1, \quad g_2 = l_2c_2, \\ \mathfrak{g}^* & = & g_1^*(\mathbb{Z}\alpha + \mathbb{Z}g_2^*), & g_1^* = l_1c_1^*, \quad g_2^* = l_2c_2^*. \end{array} \tag{66}$$

We write $\beta = \frac{\alpha}{g_2}$ and $\beta^* = \frac{\alpha}{g_2^*}$ and define

$$\begin{array}{rcl} \varphi_{\mathfrak{g}} & = & \dfrac{\varphi\left(\frac{l}{g} + \frac{\nu_0}{l} \,\middle|\, {\beta \atop 1}\right)}{\varphi\left(\frac{l}{g} \,\middle|\, {\beta \atop 1}\right)}, \\ \varphi_{\mathfrak{g}^*} & = & \dfrac{\varphi\left(\frac{l}{g^*} + \frac{\nu_0}{l} \,\middle|\, {\beta^* \atop 1}\right)}{\varphi\left(\frac{l}{g^*} \,\middle|\, {\beta^* \atop 1}\right)}, \end{array} \tag{67}$$

where we choose $\nu_0 \in \mathbb{Z}$ such that

$$(\nu_0, l) = 1, \qquad \begin{array}{l} \frac{g}{l} \mid \nu_0, \text{ if } 2 \mid l, \\ 2\frac{g}{l} \mid \nu_0, \text{ if } 2 \nmid l. \end{array} \tag{68}$$

Proposition 5.12 *[Sch2, Satz 4.3]*
(i) With the above notation one has

$$\varphi_{\mathfrak{g}} \in \begin{cases} k(2l\mathfrak{g}), & \text{if } 2 \mid l, \\ k(l\mathfrak{g}), & \text{if } 2 \nmid l, \end{cases}$$
$$\varphi_{\mathfrak{g}^*} \in \begin{cases} k(2l\mathfrak{g}^*), & \text{if } 2 \mid l, \\ k(l\mathfrak{g}^*), & \text{if } 2 \nmid l, \end{cases}$$

(ii) For $\xi \in \frac{l^4}{g}\mathfrak{g}^*$ one obtains

$$\varphi_{\mathfrak{g}}^{\sigma(1+\frac{g}{l}\xi)} = \frac{\varphi\left(\frac{l}{g} + \frac{\nu_0}{l} + \xi \,\middle|\, \begin{smallmatrix}\beta\\1\end{smallmatrix}\right)}{\varphi\left(\frac{l}{g} + \xi \,\middle|\, \begin{smallmatrix}\beta\\1\end{smallmatrix}\right)}.$$

(iii) There exists $\mu \in \mathbb{Z}$ such that $\varphi_{\mathfrak{g}}/\varphi_{\mathfrak{g}^*}^{\mu} \in k(\mathfrak{g})$. In addition, if $\mathfrak{c}$ is the power of a prime ideal, then μ can be chosen such that

$$\mu \equiv 1 \bmod \Phi(\mathfrak{c}^*),$$

where Φ denotes the Euler totient function for the ring $\mathcal{O}_k$.

Proof The proof is very similar to the proof of [Sch2, Satz 4.3]. But since we do not assume that $\mathfrak{l}$ is a rational prime, which decomposes in $k/\mathbb{Q}$, some minor modifications are necessary.

From (60) we know that $\varphi_{\mathfrak{g}} \in k(2g^2)$. Any Galois automorphism $\sigma \in \mathrm{Gal}(k(2g^2)/k(\mathfrak{g}))$ can be represented as $\sigma = \sigma(1 + g\xi)$ with $\xi \in \frac{1}{g}\mathfrak{g} = \mathbb{Z}\beta + \mathbb{Z}$. We write $\xi = x\beta + y$ with $x, y \in \mathbb{Z}$ and set

$$a = l + \nu_0 \frac{g}{l}, \quad b = l,$$
$$a^* = l + \nu_0 \frac{g^*}{l}, \quad b^* = l,$$

where $g = g_1 g_2$, $g^* = g_1^* g_2^*$. From (65), together with (55), we deduce

$$\varphi_{\mathfrak{g}}^{\sigma(1+g\xi)}/\varphi_{\mathfrak{g}} = (-1)^{xy(a^2-b^2)+(x+y)(a-b)} e^{-\frac{2\pi i}{2}\nu_0^2 \frac{g}{l^2} x}. \tag{69}$$

Note that $\beta = \frac{g_2^*}{g_2}\beta^*$ and set

$$x^* = \frac{g_1}{g_1^*}x, \quad y^* = \frac{g}{g^*}y.$$

Then $x^*, y^* \in \mathbb{Z}$. Again from (55) and (65) we obtain

$$\varphi_{\mathfrak{g}^*}^{\sigma(1+g\xi)-1} = (-1)^{x^*y^*(a^{*2}-b^{*2})+(x^*+y^*)(a^*-b^*)} e^{-\frac{2\pi i}{2}\nu_0^2 \frac{g^*}{l^2} x^*}. \tag{70}$$

If we assume in addition that $\sigma(1 + g\xi) \in \mathrm{Gal}(k(2g^2)/k(l\mathfrak{g}))$ (resp. $\sigma(1 + g\xi) \in \mathrm{Gal}(k(2g^2)/k(2l\mathfrak{g}))$, if $2 \mid l$), then we have $l \mid x, y$ (resp. $2l \mid x, y$). Considering

(68) it follows immediately from (69) that $\sigma(1+g\xi)$ fixes $\varphi_{\mathfrak{g}}$, and hence $\varphi_{\mathfrak{g}} \in k(l\mathfrak{g})$ (resp. $\varphi_{\mathfrak{g}} \in k(2l\mathfrak{g})$, if $2 \mid l$). Analogously we show $\varphi_{\mathfrak{g}^*} \in k(l\mathfrak{g}^*)$ (resp. $\varphi_{\mathfrak{g}^*} \in k(2l\mathfrak{g}^*)$, if $2 \mid l$). This proves (i).

For the proof of (ii) let $\xi \in \frac{l^4}{g}\mathfrak{g}^*$. The decompositions in (66) imply that

$$\frac{g}{l}\xi = x\beta + y \text{ with } x, y \in \mathbb{Z}, \quad l^3 \mid x, y.$$

The formula (65) leads to

$$\begin{aligned} \varphi_{\mathfrak{g}}^{\sigma(1+\frac{g}{l}\xi)} &= \frac{\varphi\left(\frac{a}{g}(1+\frac{g}{l}\xi) \,\middle|\, {\beta \atop 1}\right)}{\varphi\left(\frac{b}{g}(1+\frac{g}{l}\xi) \,\middle|\, {\beta \atop 1}\right)} \\ &= \frac{\varphi\left(\frac{l}{g} + \frac{\nu_0}{l} + \xi + \frac{\nu_0}{l}(x\beta+y) \,\middle|\, {\beta \atop 1}\right)}{\varphi\left(\frac{l}{g} + \xi \,\middle|\, {\beta \atop 1}\right)}. \end{aligned}$$

The statement of the proposition is now a consequence of the transformation formula (55).

Finally we have to show that there exists $\mu \in \mathbb{Z}$ such that $\varphi_{\mathfrak{g}}/\varphi_{\mathfrak{g}^*}^{\mu} \in k(\mathfrak{g})$. From (69) and (70) we deduce that μ has to be chosen such that

$$(-1)^{xy(a^2-b^2)+(x+y)(a-b)-\mu(x^*y^*(a^{*2}-b^{*2})+(x^*+y^*)(a^*-b^*))} e^{-\frac{2\pi i}{2}(\nu_0^2\frac{g}{l^2}x - \mu\nu_0^2\frac{g^*}{l^2}x^*)} = 1. \tag{71}$$

We claim that it suffices to take $\mu \in \mathbb{Z}$ such that

$$\nu_0^2(\frac{g}{l^2}x - \mu\frac{g^*}{l^2}x^*) = \nu_0^2\frac{g_1}{l^2}x(g_2 - \mu g_2^*) \equiv 0 \pmod 2 \tag{72}$$

holds. We have to prove that if (72) holds, then the first factor in (71) is equal to 1, too. Since 2 divides ν_0 for $2 \nmid l$ by (68) and

$$a - b = \nu_0\frac{g}{l}, \quad a^* - b^* = \nu_0\frac{g^*}{l},$$

this is obvious in this case. For $2 \mid l$ we first note that μ must be odd by (72). Moreover

$$\begin{aligned} &xy(a^2-b^2) + (x+y)(a-b) - \mu(x^*y^*(a^{*2}-b^{*2}) + (x^*+y^*)(a^*-b^*)) \\ \equiv\;& \nu_0^2 xy\frac{1}{l^2}gg_1(g_2 - g_2^*) + x\nu_0\frac{g_1}{l}(g_2 - g_2^*) \\ =\;& \nu_0^2 xycc_1(c_2 - c_2^*) + x\nu_0 c_1(c_2 - c_2^*) \pmod 2. \end{aligned}$$

Since c_2 and c_2^* are both odd the above claim follows.

It remains to prove the existence of $\mu \in \mathbb{Z}$ such that (72) holds. (72) is equivalent to

$$\nu_0^2\frac{c_1}{l}x(c_2 - \mu c_2^*) \equiv 0 \pmod 2.$$

If $2 \nmid l$, then $2 \mid \nu_0$ and it suffices to solve $\mu c_2^* \equiv c_2 \bmod l$. This is possible since $(c_2^*, l) = 1$. If $2 \mid l$, then $(2l, c_2^*) = 1$ and we solve $c_2^* \mu \equiv c_2 \pmod{2l}$.

Finally we have to check the congruence condition of (iii). To that end let

$$\mathfrak{c} = \mathfrak{p}^{r+m}, \quad \mathfrak{c}^* = \mathfrak{p}^r \text{ with } r, m \geq 1.$$

If $\mathfrak{p}$ is inert, then $c_2 = c_2^*$ and we may take $\mu = 1$. For $\mathfrak{p}$ ramified or decomposed we have

$$\Phi(\mathfrak{p}^r) = (p-1)p^{r-1} \text{ with } p = \min(\mathbb{N} \cap \mathfrak{p}).$$

If $\mathfrak{p}$ decomposes, then $c_2^* = p^r$ and $c_2 = p^{r+m}$. Hence we have to solve

$$\begin{aligned} p^r\mu &\equiv p^{r+m} \pmod{l} \text{ (resp. } \pmod{2l}) \\ \mu &\equiv 1 \pmod{p^{r-1}(p-1)}. \end{aligned} \tag{73}$$

We will show at the end that this can be done.

Suppose now that $\mathfrak{p}$ is ramified. If $2 \mid r$ and $2 \mid m$, we obtain $c_2 = c_2^* = 1$ and we take $\mu = 1$. In the case $2 \mid r$ and $2 \nmid m$ we get $c_2^* = 1$ and $c_2 = p$. Thus we need to solve

$$\begin{aligned} \mu &\equiv p \pmod{l} \text{ (resp. } \pmod{2l}) \\ \mu &\equiv 1 \pmod{p^{r-1}(p-1)}. \end{aligned} \tag{74}$$

Suppose that $2 \nmid r$ and $2 \mid m$. Then $c_2^* = c_2 = p$ and we choose $\mu = 1$. Finally, if $2 \nmid rm$, then $c_2^* = p$ and $c_2 = 1$ and we have to find $\mu \in \mathbb{Z}$ such that

$$\begin{aligned} p\mu &\equiv 1 \pmod{l} \text{ (resp. } \pmod{2l}) \\ \mu &\equiv 1 \bmod p^{r-1}(p-1). \end{aligned} \tag{75}$$

In order to solve (73) or (74) it suffices to show that

$$\begin{aligned} \mu &\equiv p^s \pmod{l} \text{ (resp. } \pmod{2l}), \quad s > 0 \\ \mu &\equiv 1 \pmod{p^{r-1}(p-1)}. \end{aligned}$$

has a solution. We set $\mu = 1 + \nu p^{r-1}(p-1)$ and wish to solve

$$\nu \cdot p^{r-1}(p-1) \equiv p^s - 1 \pmod{l} \text{ (resp. } \pmod{2l}).$$

We put $d = (l, p-1)$ (resp. $d = (2l, p-1)$) and solve

$$\nu \cdot \frac{p^{r-1}(p-1)}{d} \equiv \frac{p^s - 1}{d} \; (\bmod \frac{l}{d}) \text{ (resp. } (\bmod \frac{2l}{d})).$$

To find a solution for (75) we choose $q \in \mathbb{Z}$ such that $pq \equiv 1 \pmod{l}$ (resp. $\pmod{2l}$) and have to find $\nu \in \mathbb{Z}$ such that

$$\mu = 1 + \nu p^{r-1}(p-1) \equiv q \pmod{l} \text{ (resp. } \pmod{2l}).$$

Since $q(p-1)+(q-1)=pq-1\equiv 0 \pmod{l}$ (resp. $\pmod{2l}$) we have $d\mid q-1$. Therefore it is possible to solve

$$\nu p^{r-1}\frac{p-1}{d}\equiv\frac{q-1}{d}\ (\mathrm{mod}\ \frac{l}{d})\ (\text{resp. } (\mathrm{mod}\ \frac{2l}{d})).$$

□

In order to complete our collection of properties of the φ-function we consider the prime ideal factorization of its singular values. For a fractional ideal $\mathfrak{a}$ of k and $\xi\in k\smallsetminus\mathfrak{a}$ we denote by $o(\xi\,|\mathfrak{a})$ the denominator of $\xi\mathfrak{a}^{-1}$. The following proposition is originally due to Ramachandra [Ra]. Its present formulation is easily derived from [Sch1, Satz 3].

Proposition 5.13 *Let $\mathfrak{a}$ denote a fractional ideal of k and let $\xi\in k\smallsetminus\mathfrak{a}$. Then one has*

$$\varphi(\xi\,|\mathfrak{a})\sim\begin{cases}1, & \text{if } o(\xi\,|\mathfrak{a}) \text{ is composite,}\\ \mathfrak{p}^{1/\Phi(\mathfrak{p}^n)}, & \text{if } o(\xi\,|\mathfrak{a})=\mathfrak{p}^n \text{ is a prime ideal power.}\end{cases}$$

5.5 Resolvents

Let us recall the notation of Sections 5.1 and 5.2. F is a finite abelian extension of k and E/F is an elliptic curve with complex multiplication by $\mathcal{O}_k$ and the additional property that $F(E_{\mathrm{tor}})/k$ is abelian. Associated to E/F there is a Groessencharacter φ of k and we have set $\mathfrak{f}=\mathrm{lcm}(\mathfrak{f}_\varphi,\mathfrak{f}_{F/k})$. Recall that $\mathfrak{f}$ only depends on E/F.

Let $\xi(\ ,\mathfrak{w})$ be the corresponding Weierstrass isomorphism as in (40) . Let $r,m\geq 1$ be rational integers and fix an prime ideal $\mathfrak{p}$ of k such that $(\mathfrak{p},\mathfrak{f})=1$. We have set $G=E[\mathfrak{p}^m]$ and for a fixed primitive $\mathfrak{p}^{r+m}$-torsion point $Q_0=\xi(\rho_0,\mathfrak{w})$ we defined Γ by $\{Q_0+_E P\mid P\in G\}$. In Section 5.2 we further wrote $K=k(\mathfrak{f}\mathfrak{p}^r)$, $L=k(\mathfrak{f}\mathfrak{p}^{r+m})$, $\Omega=\Omega_K$ and defined

$$A=(\bar{K}G)^\Omega,\quad B=\mathrm{Map}(G,\bar{K})^\Omega,\quad C=\mathrm{Map}(\Gamma,\bar{K})^\Omega.$$

Via the $K-$algebra isomorphism $\tau: C\to L$ of (52) we endowed L with the structure of an A-module. This A-action is explicitly described by (54).

For $\theta\in L$ we set $h_\theta=\tau^{-1}(\theta)$. By the definition of τ this implies $h_\theta(Q_0)=\theta$. Recall the definition of the resolvent in (12). For any abelian character χ of G we obtain from (54)

$$\begin{aligned}(h_\theta,\chi)_{Q_0} &= \sum_{g\in G}h_\theta(Q_0+_E g)\bar{\chi}(g)\\ &= \sum_{g\in G}h_\theta(Q_0)^{\sigma(1+\frac{\beta_g}{\rho_0})}\bar{\chi}(g)\\ &= \sum_{g\in G}\theta^{\sigma(1+\frac{\beta_g}{\rho_0})}\bar{\chi}(g),\end{aligned}\tag{76}$$

where $\beta_g\in\mathfrak{p}^{-m}\mathfrak{f}\mathfrak{w}$ is such that $g=\xi(\beta_g,\mathfrak{w})$.

Our aim in the following will be to construct elements $\theta\in L$ such that the ideal factorization of $(h_\theta,\chi)_{Q_0}$ can be computed.

Theorem 5.14 *Assume that* $\mathfrak{f}$ *is composite and* $(\mathfrak{f}, \mathfrak{p}\bar{\mathfrak{p}}) = 1$. *Then there exists an element* $\theta \in L$ *such that*

$$(h_\theta, \chi)_{Q_0} \sim \mathfrak{p}^m \tag{77}$$

for all abelian characters χ *of* G. *Moreover*

$$\theta \sim \mathfrak{p}^{\frac{1}{\Phi(\mathfrak{p}^r)} - \frac{1}{\Phi(\mathfrak{p}^{r+m})}}. \tag{78}$$

Remark 5.15 Up to minor modifications this is [Sch2, Satz 2.2].

Proof We set

$$\mathfrak{g} = \mathfrak{f}\mathfrak{p}^{r+m}, \quad \mathfrak{g}^* = \mathfrak{f}\mathfrak{p}^r$$

and define $\varphi_\mathfrak{g}$ and $\varphi_{\mathfrak{g}^*}$ as in (67) with $\mathfrak{l} = \mathfrak{f}$, $\mathfrak{c} = \mathfrak{p}^{r+m}$, $\mathfrak{c}^* = \mathfrak{p}^r$. We choose $\mu \in \mathbb{Z}$ as in part (iii) of Proposition 5.12. Then $(1-\mu)/\Phi(\mathfrak{p}^r) \in \mathbb{Z}$ and we can find $\kappa \in k(1)$ such that

$$\kappa \sim \mathfrak{p}^{(1-\mu)/\Phi(\mathfrak{p}^r)}.$$

We set

$$\theta = \frac{\varphi_\mathfrak{g}}{\varphi_{\mathfrak{g}^*}^\mu} \cdot \kappa.$$

Then $\theta \in L$ by Proposition 5.12. Furthermore it follows from Proposition (5.13) that

$$\begin{aligned} \varphi_\mathfrak{g} &\sim \frac{\varphi\left(l + g\frac{\nu_0}{l} \,|\, \mathfrak{l}\mathfrak{p}^{r+m}\right)}{\varphi\left(l \,|\, \mathfrak{l}\mathfrak{p}^{r+m}\right)} \sim \mathfrak{p}^{-\frac{1}{\Phi(\mathfrak{p}^{r+m})}}, \\ \varphi_{\mathfrak{g}^*} &\sim \frac{\varphi\left(l + g^*\frac{\nu_0}{l} \,|\, \mathfrak{l}\mathfrak{p}^{r}\right)}{\varphi\left(l \,|\, \mathfrak{l}\mathfrak{p}^{r}\right)} \sim \mathfrak{p}^{-\frac{1}{\Phi(\mathfrak{p}^{r})}} \end{aligned}$$

Hence $\theta \sim \mathfrak{p}^{-\frac{1}{\Phi(\mathfrak{p}^{r+m})} + \frac{\mu}{\Phi(\mathfrak{p}^r)} + \frac{1-\mu}{\Phi(\mathfrak{p}^r)}} = \mathfrak{p}^{\frac{1}{\Phi(\mathfrak{p}^r)} - \frac{1}{\Phi(\mathfrak{p}^{r+m})}}$, which proves (78).

In order to verify (77) we choose a set R of representatives of $\mathfrak{p}^{-m}l^3\mathfrak{f}\mathfrak{w}$ modulo $l^3\mathfrak{f}\mathfrak{w}$. Then

$$G = \{\xi(\beta, \mathfrak{w}) \mid \beta \in R\}$$

and from (76) we deduce

$$(h_\theta, \chi)_{Q_0} = \sum_{\beta \in R} \theta^{\sigma(1+\frac{\beta}{\rho_0})} \bar{\chi}(\xi(\beta, \mathfrak{w})).$$

From $\beta \in \mathfrak{p}^{-m}l^3\mathfrak{f}\mathfrak{w}$ and $\rho_0 \in \mathfrak{p}^{-r-m}\mathfrak{w}$ we easily deduce

$$\frac{l}{g} \cdot \frac{\beta}{\rho_0} \in \frac{l^4}{g}\mathfrak{f}\mathfrak{p}^r.$$

Considering the isomorphism

$$\begin{aligned} \mathfrak{p}^{-m} l^3 \mathfrak{f}\mathfrak{w} / l^3 \mathfrak{f}\mathfrak{w} &\longmapsto \frac{l^4}{g}\mathfrak{f}\mathfrak{p}^r / \frac{l^4}{g}\mathfrak{f}\mathfrak{p}^{r+m}, \\ \beta &\longmapsto \frac{l}{g} \cdot \frac{\beta}{\rho_0}, \end{aligned}$$

we obtain

$$(h_\theta, \chi)_{Q_0} = \sum_\xi \theta^{\sigma(1+\frac{g}{l}\xi)} \bar{\chi}(\xi), \tag{79}$$

where ξ runs over a set of representatives of $\frac{l^4}{g}\mathfrak{f}\mathfrak{p}^r / \frac{l^4}{g}\mathfrak{f}\mathfrak{p}^{r+m}$ and χ is interpreted as a character of this group in the obvious way. From (79) and Proposition 5.12 we deduce

$$(h_\theta, \chi)_{Q_0} = \left(\sum_\xi \frac{\varphi\left(\frac{l}{g} + \frac{\nu_0}{l} + \xi \,\middle|\, {\beta \atop 1}\right)}{\varphi\left(\frac{l}{g} + \xi \,\middle|\, {\beta \atop 1}\right)} \bar{\chi}(\xi) \right) \cdot \varphi_{\mathfrak{g}^*}^{-\mu} \cdot \kappa,$$

where we have to take into account that $\sigma(1+\frac{g}{l}\xi)$ acts trivially on $\varphi_{\mathfrak{g}^*}$, since $\frac{g}{l}\xi \in l^3\mathfrak{f}\mathfrak{p}^r$ and $\varphi_{\mathfrak{g}^*} \in k(l\mathfrak{f}\mathfrak{p}^r)$, if $2 \nmid l$ (resp. $\varphi_{\mathfrak{g}^*} \in k(2l\mathfrak{f}\mathfrak{p}^r)$, if $2 \mid l$).

By the homogenity of φ (and the usual misuse of notation) we can write

$$(h_\theta, \chi)_{Q_0} = \left(\sum_\xi \frac{\varphi\left(l + \frac{\nu_0 g}{l} + \xi \,|\mathfrak{f}\mathfrak{p}^{r+m}\right)}{\varphi\left(l + \xi \,|\mathfrak{f}\mathfrak{p}^{r+m}\right)} \bar{\chi}(\xi) \right) \cdot \varphi_{\mathfrak{g}^*}^{-\mu} \cdot \kappa,$$

where now ξ runs over a set of representatives of $l^4\mathfrak{f}\mathfrak{p}^r / l^4\mathfrak{f}\mathfrak{p}^{r+m}$. Recall now the definition of the function $h_\mathfrak{w}$ in (59). Since $\xi \in l^4\mathfrak{f}\mathfrak{p}^r$ and $2 \mid \nu_0$, if $2 \nmid l$, we easily find

$$\frac{1}{2} h_{\mathfrak{f}\mathfrak{p}^{r+m}}(\xi, \nu_0 \frac{g}{l}) \in 2\pi i \mathbb{Z}.$$

We apply Proposition 5.11 and therefore adopt the notation used there. Write $\mathfrak{f}\mathfrak{p}^{r+m} = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$, $\mathfrak{f}\mathfrak{p}^r = \mathbb{Z}\frac{\omega_1}{n_1} + \mathbb{Z}\frac{\omega_2}{n_2}$, $\chi(\frac{\omega_1}{n_1}) = e^{2\pi i \mu_1 / n_1}$, $\chi(\frac{\omega_2}{n_2}) = e^{2\pi i \mu_2 / n_2}$ and $\delta_\chi = \frac{1}{N_{k/\mathbb{Q}}(\mathfrak{p}^m)}(\nu_0 \frac{g}{l} + \mu_2\omega_1 - \mu_1\omega_2)$. Then Proposition 5.11 yields

$$(h_\theta, \chi)_{Q_0} = \zeta \cdot \sqrt[12]{\frac{\Delta(\mathfrak{f}\mathfrak{p}^r)}{\Delta(\mathfrak{f}\mathfrak{p}^{r+m})}} \cdot \varphi_{\mathfrak{g}^*}^{-\mu} \cdot \kappa \cdot \underbrace{\frac{\varphi\left(g\frac{\nu_0}{l} \,|\mathfrak{f}\mathfrak{p}^{r+m}\right) \varphi\left(l + \delta_\chi \,|\mathfrak{f}\mathfrak{p}^r\right)}{\varphi\left(\delta_\chi \,|\mathfrak{f}\mathfrak{p}^r\right) \varphi\left(l \,|\mathfrak{f}\mathfrak{p}^r\right)}}_{=:A}$$

with some root of unity ζ. We easily prove that $\mathfrak{f}$ divides $o\left(g\frac{\nu_0}{l} \,|\mathfrak{f}\mathfrak{p}^{r+m}\right)$, $o\left(l + \delta_\chi \,|\mathfrak{f}\mathfrak{p}^r\right)$, $o\left(\delta_\chi \,|\mathfrak{f}\mathfrak{p}^r\right)$ and that $o\left(l \,|\mathfrak{f}\mathfrak{p}^r\right) = \mathfrak{p}^r$. Since $\mathfrak{f}$ is composite we derive from Proposition 5.13 $A \sim \mathfrak{p}^{-\frac{1}{\Phi(\mathfrak{p}^r)}}$. [KL, Ch. 11,Th. 3.1] implies that $\sqrt[12]{\Delta(\mathfrak{f}\mathfrak{p}^r)/\Delta(\mathfrak{f}\mathfrak{p}^{r+m})} \sim \mathfrak{p}^m$. Collecting everything we get

$$(h_\theta, \chi)_{Q_0} \sim \mathfrak{p}^m \mathfrak{p}^{-\frac{\mu}{\Phi(\mathfrak{p}^r)} + \frac{1-\mu}{\Phi(\mathfrak{p}^r)} - \frac{1}{\Phi(\mathfrak{p}^r)}} = \mathfrak{p}^m$$

$\square$

5.6 Elliptic curves and Lubin-Tate theory

In this Section we keep all the notations of the previous sections.

In the sequel we will work out the connection between the relative Lubin-Tate theory presented in Section 4 and the global situation described in this section. Since we are mainly concerned with the relative extension $k(\mathfrak{f}\mathfrak{p}^{r+m})/k(\mathfrak{f}\mathfrak{p}^r)$, we may without loss of generality assume that $F = k(\mathfrak{f})$. Let $\mathfrak{P}$ be a prime ideal of F above $\mathfrak{p}$. Then $\mathfrak{P}$ is totally ramified in $k(\mathfrak{f}\mathfrak{p}^s)/F$ for all $s \geq 0$ and, for any intermediate field N in L/F, we write $\mathfrak{P}_N$ for the unique prime ideal of N above $\mathfrak{P}$. Let $\imath : \bar{\mathbb{Q}} \hookrightarrow \bar{\mathbb{Q}}_p$ be a field embedding defining the prime $\mathfrak{P}_L$. Via $\imath$ we will view elements of $\bar{\mathbb{Q}}$ as elements of $\bar{\mathbb{Q}}_p$ and usually omit the $\imath$ in our notation. Furthermore, for any finite extension N/F we write $\tilde{N}$ for the completion of $\imath(N)$.

We fix a minimal Weierstrass equation of E over the localization of $\mathcal{O}_F$ at $\mathfrak{P}$ and via $\imath$ we view E as an elliptic curve defined over $\tilde{F} = F_{\mathfrak{P}}$, denoted by $\tilde{E}$. Let $\hat{E}$ denote the formal group of $\tilde{E}$ with respect to the parameter $z = -\frac{x}{y}$. From Lemma 5.8 we know that $\hat{E}$ is a relative Lubin-Tate extension with respect to the unramified extension $F_{\mathfrak{P}}/k_{\mathfrak{p}}$. More precisely, $\hat{E}$ is the unique group law corresponding to

$$f(z) = \widehat{\lambda(\mathfrak{p})}(z) = \Lambda(\mathfrak{p})z + \dots . \tag{80}$$

Let N be a finite extension of F. From [Sil1, Ch. VII, Prop. 2.2] we know that the map

$$E_1(\tilde{N}) \longrightarrow \hat{E}(\mathfrak{p}_{\tilde{N}}), \quad P = (x,y) \longmapsto z(P) = -\frac{x}{y} \tag{81}$$

is a isomorphism, where E_1 denotes the kernel of reduction. Let $\theta : \mathcal{O}_k \to \mathrm{End}(E)$ be normalized. Via $\imath$ we can identify the rings $\mathrm{End}(E)$ and $\mathrm{End}(\tilde{E})$ and thus obtain a ring isomorphism $\tilde{\theta} : \mathcal{O}_k \to \mathrm{End}(\tilde{E})$. By general theory we know that $\tilde{\theta}(\alpha)(E_1(\tilde{L})) \subseteq E_1(\tilde{L})$, $\alpha \in \mathcal{O}_k$, (see [CT, diagram on p. 49]), hence $E_1(\tilde{L})$ is an $\mathcal{O}_k$-module. Furthermore $\hat{E}(\mathfrak{p}_{\tilde{L}})$ is also an $\mathcal{O}_k$-module by [dS, Prop. 1.5, p.9]. Namely, there is a ring isomorphism $\mathcal{O}_{\tilde{k}} \to \mathrm{End}(\hat{E})$, $\alpha \mapsto [\alpha]_f$, and hence a ring embedding $\mathcal{O}_k \hookrightarrow \mathrm{End}(\hat{E})$.

Lemma 5.16 *The map $E_1(\tilde{N}) \to \hat{E}(\mathfrak{p}_{\tilde{N}})$, $P \mapsto z(P)$, is an isomorphism of $\mathcal{O}_k$-modules for any finite extension $\tilde{N}/\tilde{F}$.*

Proof Let $P \in E_1(\tilde{N})$ and $\alpha \in \mathcal{O}_k$. Then we have to show that

$$z(\tilde{\theta}(\alpha)(P)) = [\alpha]_f\,(z(P))\,.$$

The isogeny $\tilde{\theta}(\alpha)$ induces an endomorphism $\widehat{\tilde{\theta}(\alpha)} \in \mathrm{End}(\hat{E})$ such that

$$\begin{array}{ccc} E_1(\tilde{N}) & \xrightarrow{\tilde{\theta}(\alpha)} & E_1(\tilde{N}) \\ \downarrow & & \downarrow \\ \hat{E}(\mathfrak{p}_{\tilde{N}}) & \xrightarrow{\widehat{\tilde{\theta}(\alpha)}} & \hat{E}(\mathfrak{p}_{\tilde{N}}) \end{array}$$

commutes. It remains to show that $\widehat{\tilde{\theta}(\alpha)} = [\alpha]_f$. To that end, by [dS, Prop. 1.5, p.9], it is enough to prove

$$\widehat{\tilde{\theta}(\alpha)}(z) \equiv \alpha z \text{ (mod deg 2)}.$$

This follows as in the proof of Lemma (5.8) from $(\omega \circ \tilde{\theta}(\alpha))(z) = \alpha\omega(z)$. □

Corollary 5.17 *(i) Let $\pi \in \mathcal{O}_{\tilde{k}}$ be any uniformizing parameter for $\mathfrak{p}$ and let $\omega \in \bar{\mathbb{Q}}_p$ be a primitive π^n-torsion point of $\hat{E}$. Then $P = z^{-1}(\omega)$ is a primitive $\mathfrak{p}^n$-torsion point of $E(\bar{\mathbb{Q}})$.*

(ii) Conversely, if $P \in E(\bar{\mathbb{Q}})$ is a primitive $\mathfrak{p}^n$-torsion point, then $z(P)$ is a primitive π^n-torsion point of $\hat{E}$ for any uniformizing parameter $\pi \in \mathcal{O}_{\tilde{k}}$.

Proof We first prove (i). We have to show that

$$\begin{aligned} \tilde{\theta}(\alpha)(P) &= 0_{\tilde{E}} \text{ for all } \alpha \in \mathfrak{p}^n, && (82)\\ \tilde{\theta}(\alpha)(P) &\neq 0_{\tilde{E}}, \text{ if } \mathfrak{p}^n \nmid \alpha. && (83)\end{aligned}$$

If $w_{\mathfrak{p}}(\alpha) = s$, then $\alpha/\pi^s \in \mathcal{O}_{\tilde{F}}{}^*$. By Lemma 5.16 the following equivalence holds:

$$\tilde{\theta}(\alpha)(P) = 0_E \iff [\alpha]_f(\omega) = [\frac{\alpha}{\pi^s}]_f \circ [\pi^s]_f(\omega) = 0.$$

Since $[\frac{\alpha}{\pi^s}]_f$ is an isomorphism, this implies both (82) and (83).

In order to prove the converse in (ii) we first note that $E[\mathfrak{p}^n] \subseteq E_1(\tilde{F}_n)$, where we denote by $\tilde{F}_n$ the field generated by the $\mathfrak{p}^n$-torsion points of $\hat{E}$ over $\tilde{F}$. This follows from $\hat{E}(\mathfrak{p}_{\tilde{F}_n}) \simeq E_1(\tilde{F}_n)$ and $|G_{f,n}| = N_{k/\mathbb{Q}}(\mathfrak{p}^n) = |E[\mathfrak{p}^n]|$ (see [dS, Ch. I, Prop. 1.7]), where $G_{f,n}$ is the set of all $\mathfrak{p}^n$-torsion points of $\hat{E}$.

We have to prove that $\omega = z(P)$ satisfies

$$[\pi^n]_f(\omega) = 0 \text{ and } [\pi^s]_f(\omega) \neq 0, 0 \leq s < n. \tag{84}$$

To that end we choose $\pi_1 \in \mathcal{O}_k$ such that $w_{\mathfrak{p}}(\pi_1) = 1$. Then $\pi = \pi_1 \cdot \varepsilon$ with a unit $\varepsilon \in \mathcal{O}_{\tilde{k}}^*$ and since $[\varepsilon]_f$ is an isomorphism we obtain $[\pi^s]_f(\omega) = 0 \iff [\pi_1^s]_f(\omega) = 0$ for $0 \leq s \leq n$. Now (ii) follows from Lemma 5.16. □

Corollary 5.17, together with [dS, Ch. I, Prop. 1.8] and Corollary 5.6, implies that for $s \geq 0$ the completion of $F(E[\mathfrak{p}^s]) = k(\mathfrak{f}\mathfrak{p}^s)$ is equal to the field $\tilde{F}_n = \tilde{F}(G_{f,n})$, where, as in Section 4 ,

$$G_{f,n} = \{\omega \in \hat{E}(\bar{\mathbb{Q}}_p) \mid [\pi^n]_f(\omega) = 0\}, \quad \pi \in \mathcal{O}_k \text{ such that } w_{\mathfrak{p}}(\pi) = 1,$$

is the set of all $\mathfrak{p}^n$-division points of $\hat{E}$. In particular we obtain

$$\tilde{L} = \tilde{F}_{r+m}, \quad \tilde{K} = \tilde{F}_r. \tag{85}$$

We fix an uniformizing parameter $\pi \in \mathcal{O}_k$ for $\mathfrak{p}$ and set

$$\begin{array}{rcl} \tilde{G} & = & G_{f,m} = \{\omega \in \hat{E}(\bar{\mathbb{Q}}_p) \mid [\pi^m]_f(\omega) = 0\}, \\ \tilde{\Gamma} & = & \{z(Q_0) +_f \omega \mid \omega \in \tilde{G}\}. \end{array}$$

Then we derive from Lemma (5.17) a group isomorphism

$$G \longmapsto \tilde{G}, \quad g \longmapsto z(g) \tag{86}$$

and a bijection

$$\Gamma \longmapsto \tilde{\Gamma}, \quad Q \longmapsto z(Q) \tag{87}$$

Let

$$\begin{array}{rclrcl} A & = & (\bar{K}G)^{\Omega_K}, & \tilde{A} & = & (\bar{\tilde{K}}\tilde{G})^{\Omega_{\tilde{K}}} \\ & = & (LG)^{\mathrm{Gal}(L/K)}, & & = & (\tilde{L}\tilde{G})^{\mathrm{Gal}(\tilde{L}/\tilde{K})}, \\ C & = & \mathrm{Map}(\Gamma, \bar{K})^{\Omega_K}, & \tilde{C} & = & \mathrm{Map}(\tilde{\Gamma}, \bar{\tilde{K}})^{\Omega_{\tilde{K}}} \\ & = & \mathrm{Map}(\Gamma, L)^{\mathrm{Gal}(L/K)} & & = & \mathrm{Map}(\tilde{\Gamma}, \tilde{L})^{\mathrm{Gal}(\tilde{L}/\tilde{K})}. \end{array} \tag{88}$$

Then

$$\Phi : \tilde{K} \otimes_K A \longmapsto \tilde{A}, \quad \alpha \otimes \sum_{g \in G} a_g g \longmapsto \sum_{g \in G} \alpha a_g z(g) \tag{89}$$

is an isomorphism of $\tilde{K}$-algebras and we will identify both algebras in the sequel.

Lemma 5.18 *The map*

$$\begin{array}{rcl} \Psi : \tilde{K} \otimes_K C & \longrightarrow & \tilde{C}, \\ \alpha \otimes h & \longmapsto & (z(Q) \mapsto \alpha h(Q)), \quad Q \in \Gamma \end{array}$$

is an isomorphism of $\tilde{A}$-algebras.

Proof Let $Q_1, \dots, Q_t$ be a set of orbit representatives of Γ modulo the action of $\mathrm{Gal}(L/K)$. For each $m \in \{1, \dots, t\}$ let $\tilde{K}_m$ denote the fixed field of $\mathrm{stab}_{\Omega_K}(Q_m) \le \Omega_K$, and let $z_{m,1}, \dots, z_{m,t_m}$ be an K-basis of $\tilde{K}_m$.(The notation $\tilde{K}_m$ does not mean completion for a short moment, but adapts the notation of Lemma 2.11.) For $1 \le m \le t$ and $1 \le n \le t_m$, let $c_{m,n} \in C$ be defined by

$$c_{m,n}(Q) := \begin{cases} \omega(z_{m,n}), & \text{if } Q = {}^{\omega}Q_m \text{ for some } \omega \in \Omega_L, \\ 0, & \text{otherwise,} \end{cases}$$

for $Q \in \Gamma$. Then, by Lemma 2.11(ii), the elements $c_{m,n}$, $1 \leqslant m \leqslant t$, $1 \leqslant n \leqslant t_m$, form an K-basis of C. Obviously this basis is mapped to a $\tilde{K}$-basis of $\tilde{C}$. Hence Ψ is an isomorphism of $\tilde{K}$-algebras.

Finally we have to show

$$\Psi\left((\alpha\otimes h)\left(\beta\otimes\sum_{g\in G}a_g g\right)\right)=\Psi(\alpha\otimes h)\cdot\sum_{g\in G}\beta a_g z(g)$$

for $h\in C$, $\alpha,\beta\in\tilde{K}$ and $\sum_{g\in G}a_g g\in A$. This is a straight forward consequence from the definitions: for the left hand side we compute

$$\left(\Psi\left((\alpha\otimes h)(\beta\otimes\sum_{g\in G}a_g g)\right)\right)(z(Q))=\sum_{g\in G}\alpha\beta a_g h(Q+_E g)$$

for the value at $z(Q), Q\in\Gamma$, and the right hand side yields

$$\begin{aligned}\left(\Psi(\alpha\otimes h)\cdot\sum_{g\in G}\beta a_g z(g)\right)(z(Q)) &= \sum_{g\in G}\beta a_g\Psi(\alpha\otimes h)\left(z(g)+_f z(Q)\right)\\ &= \sum_{g\in G}\beta a_g\Psi(\alpha\otimes h)\left(z(g+_E Q)\right)\\ &= \sum_{g\in G}\alpha\beta a_g h(g+_E Q).\end{aligned}$$

□

The preceeding discussion may be summarized in the following commutative diagram of $\tilde{A}$-modules

$$\begin{array}{ccc}\tilde{K}\otimes_K C & \xrightarrow{1\otimes\tau} & \tilde{K}\otimes_K L=\tilde{L}\\ {\scriptstyle\Psi}\downarrow & & \downarrow\\ \tilde{C} & \xrightarrow{\tilde{\tau}} & \tilde{L}\end{array}$$

where $\tau(h)=h(Q_0)$ and $\tilde{\tau}(\tilde{h})=\tilde{h}(z(Q_0))$ for $h\in C$ and $h'\in C'$.

Finally we have to take care of our resolvents.

Lemma 5.19 *Let $h\in C$ and put $\tilde{h}=\Psi(h)\in\tilde{C}$. Then*

$$(\tilde{h},\tilde{\chi})_{z(Q_0)}=(h,\chi)_{Q_0},$$

where χ and $\tilde{\chi}$ are related by $\chi=\tilde{\chi}\circ z$.

Proof This is just a straight forward computation:

$$\begin{aligned}(\tilde{h},\tilde{\chi})_{z(Q_0)} &= \sum_{g\in G}\tilde{h}(z(Q_0)+_f z(g))\tilde{\chi}(z(g))^{-1}\\ &= \sum_{g\in G}\tilde{h}(z(Q_0+_E g))\bar{\chi}(g)\\ &= \sum_{g\in G}h(Q_0+_E g)\bar{\chi}(g)\\ &= (h,\chi)_{Q_0}.\end{aligned}$$

□

5.7 Module structure

Recall the situation and notation as it is presented in Section 5.2. In addition, let $\mathcal{C}$ denote the integral closure of $\mathcal{O}_K$ in C and let $\mathcal{A}^{\mathrm{ass}}$ be its associated order in A.

Our aim is to study the $\mathcal{A}^{\mathrm{ass}}$-module structure of $\mathcal{C}$. The case $r = 0$ is already settled by Corollary 2.15. Namely, define a map $l \in C$ by

$$l(Q) = \begin{cases} 1, & \text{if } Q = 0_E, \\ 0, & \text{if } Q \neq 0_E, \end{cases}$$

and recall that $\mathcal{A}^\circ = (\mathcal{O}_{\bar{K}}G)^\Omega$. Then we have the following

Theorem 5.20 *Let $r = 0$. Then $\mathcal{A}^{\mathrm{ass}} = \mathcal{A}^\circ$ and $\mathcal{C}$ is free of rank one over $\mathcal{A}^{\mathrm{ass}}$. An explicit generator is given by the map l.*

Proof This is the assertion of Corollary 2.15. □

In the sequel we concentrate on the case $r \geq 1$. Recall that $L = k(\mathfrak{f}\mathfrak{p}^{r+m})$ and $K = k(\mathfrak{f}\mathfrak{p}^r)$. In order to control the ramication of primes outside $\mathfrak{p}$ we assume that the elliptic curve E/F and K satisfy the following hypothesis:

$$E \text{ attains everywhere good reduction over } K \tag{90}$$

This is in fact a mild condition, which, for a fixed elliptic curve E/F, excludes only finitely many extensions $K = k(\mathfrak{f}\mathfrak{p}^r)$. In Lemma 5.26 we will precisely describe those cases that do not satisfy (90).

Lemma 5.21 *Let $K = k(\mathfrak{f}\mathfrak{p}^r)$, $r \geq 1$, and let $\mathfrak{Q}$ be a prime ideal of $\mathcal{O}_K$ not dividing $\mathfrak{p}$. Then $\mathfrak{Q}$ is unramified in L/K, $L = k(\mathfrak{f}\mathfrak{p}^{r+m})$, for all $m \geq 1$ if and only if $\mathfrak{Q}$ is a prime of good reduction for E/K.*

Proof The criterion of Ogg-Néron-Shafarevich (see [dS, Ch. II, Th. 1.8]) implies that $\mathfrak{Q}$ is a prime of good reduction if and only if $K(E[\mathfrak{p}^\infty])/K$ is unramified at $\mathfrak{Q}$. Since $K(E[\mathfrak{p}^\infty]) = k(\mathfrak{f}\mathfrak{p}^\infty)$ by Proposition 5.3 the Lemma follows. □

We will completely determine $\mathcal{A}^{\mathrm{ass}}$ by its local components and thereby prove that it is an Hopf order, more precisely, the Cartier dual of the $\mathcal{O}_K$-Hopf order which represents the $\mathcal{O}_K$-group scheme of $\mathfrak{p}^m$-torsion points on E. Moreover we will show that $\mathcal{C}$ is locally free of rank 1 over $\mathcal{A}^{\mathrm{ass}}$. Finally we will prove that, under certain restrictions on $\mathfrak{f}$ and $\mathfrak{p}$, $\mathcal{C}$ is also globally free over $\mathcal{A}^{\mathrm{ass}}$.

Definition 5.22 We define an $\mathcal{O}_K$-module $\tilde{\mathcal{A}} \subseteq A$ by describing its localizations at each prime $\mathfrak{Q}$ of K. If $\mathfrak{Q} \nmid \mathfrak{p}$ let

$$\tilde{\mathcal{A}}_{\mathfrak{Q}} = (\mathcal{O}_{K_{\mathfrak{Q}}}G)^{\Omega_K}.$$

For $\mathfrak{Q} \mid \mathfrak{p}$ we choose a uniformizing parameter $\pi \in \mathcal{O}_k$ for $\mathfrak{p}$ and a minimal Weierstrass equation for E defined over the localization $\mathcal{O}_{K,\mathfrak{Q}}$. For $i \geq 0$ we define $\sigma_i \in A$ by

$$\sigma_i = \frac{1}{\pi^m} \sum_{g \in G} z(g)^i (g - g_0),$$

where

$$z(g) = \begin{cases} -\frac{x}{y}, & \text{if } g = (x,y) \neq 0_E, \\ 0, & \text{if } g = 0_E. \end{cases}$$

Then

$$\tilde{\mathcal{A}}_{\mathfrak{Q}} \quad = \quad \mathcal{O}_{K_{\mathfrak{Q}}} \cdot g_0 + \sum_{i=0}^{q^m-2} \mathcal{O}_K \cdot \sigma_i,$$

where $q = \mathrm{N}_{k/\mathbb{Q}}(\mathfrak{p})$.

Proposition 5.23 *$\tilde{\mathcal{A}}$ is a $\mathcal{O}_K$-Hopf order in A. More precisely, it is the Cartier dual of the $\mathcal{O}_K$-Hopf order which represents the $\mathcal{O}_K$-group scheme of $\mathfrak{p}^m$-torsion points on E.*

Proof Let $\mathcal{B}^{\mathrm{gs}}$ denote the $\mathcal{O}_K$-Hopf order which represents the $\mathcal{O}_K$-group scheme of $\mathfrak{p}^m$-torsion points on E. An explicit description of $\mathcal{B}^{\mathrm{gs}}$ is given in [T2, § 2]. For each prime $\mathfrak{Q}$ of $\mathcal{O}_K$ not dividing $\mathfrak{p}$, its localization $\mathcal{B}^{\mathrm{gs}}_{\mathfrak{Q}}$ is equal to $\mathrm{Map}(G, \mathcal{O}_{\bar{K}})^{\Omega_K}_{\mathfrak{Q}}$. For a prime $\mathfrak{Q} \mid \mathfrak{p}$ we have

$$\mathcal{B}^{\mathrm{gs}}_{\mathfrak{Q}} = \mathcal{O}_{K_{\mathfrak{Q}}}[[X]]/(f^{(m)}(X)),$$

where $f(z)$ is given by (80) and $f^{(m)}$ is defined in (25). Here we view, as in Section 3, $\mathcal{B}^{\mathrm{gs}}_{\mathfrak{Q}}$ as an $\mathcal{O}_{K_{\mathfrak{Q}}}$-order in $\mathrm{Map}(G, \bar{K})^{\Omega_K}_{\mathfrak{Q}}$ via the rule $b(X)(g) = b(z(g))$ for $b(X) \in \mathcal{O}_{K_{\mathfrak{Q}}}[[X]]$ and $g \in G$.

According to Lemma 2.3, we have a decomposition

$$B \simeq \prod_{i=1}^{r} K_i,$$

where in this situation each of the fields K_i is a subfield of L/K, and hence by (90) and Lemma 5.21 unramified at primes $\mathfrak{Q}$ not dividing $\mathfrak{p}$. Thus the assertion of the Theorem follows for $\mathfrak{Q} \nmid \mathfrak{p}$ from Lemma 2.4 and Corollary 2.5. For $\mathfrak{Q} \mid \mathfrak{p}$ it is an immediate consequence of Lemma 5.16 and Proposition 4.5. □

In the following we write again $\mathcal{A}^{\mathrm{gs}}$ for $\tilde{\mathcal{A}}$, reflecting the assertion of the previous proposition.

Theorem 5.24 *Let $r \geq 1$ and suppose that E/F and K satisfy (90). Then:*

(i) The associated order $\mathcal{A}^{\mathrm{ass}}$ is equal to $\mathcal{A}^{\mathrm{gs}}$.

(ii) $\mathcal{C}$ is a locally free $\mathcal{A}^{\mathrm{ass}}$-module of rank 1.

Proof Let first $\mathfrak{Q}$ be a prime ideal dividing $\mathfrak{p}$. By Lemma 5.18 the isomorphism Φ in (89) maps $\mathcal{A}_{\mathfrak{Q}}^{\mathrm{ass}}$ to the associated order of the integral closure $\tilde{\mathcal{C}}$ of $\mathcal{O}_{K_{\mathfrak{Q}}}$ in $\tilde{C}$. Hence the assertion of the Theorem follows from Proposition 5.23 and Corollary 4.10.

Next we will prove that $\mathcal{C}_{\mathfrak{Q}}$ is locally free over $\mathcal{A}_{\mathfrak{Q}}^{\mathrm{gs}}$ for primes $\mathfrak{Q}$ such that $\mathfrak{Q} \nmid \mathfrak{p}$. To achieve this we apply [CH, Th. 5.4].Let

$$I = \{\lambda \in \mathcal{A}_{\mathfrak{Q}}^{\mathrm{gs}} \mid \mu\lambda = \varepsilon(\mu)\lambda, \forall \mu \in \mathcal{A}_{\mathfrak{Q}}^{\mathrm{gs}}\}$$

denote the ideal of integrals in $\mathcal{A}_{\mathfrak{Q}}^{\mathrm{gs}}$. It is an easy exercise, using the basis described in Lemma 2.1, to show that $I = \mathcal{O}_{K_{\mathfrak{Q}}} \sum_{g\in G} g$. Since L/K is unramified at $\mathfrak{Q}$ by Lemma 5.21, it follows that $\mathcal{C}_{\mathfrak{Q}} \cdot I = \mathcal{O}_{K_{\mathfrak{Q}}}$, and this, in turn, proves local freeness by [CH, Prop. (5.4)].

To sum up, $\mathcal{C}$ is a locally free $\mathcal{A}^{\mathrm{gs}}$-module, hence $\mathcal{A}^{\mathrm{ass}} = \mathcal{A}^{\mathrm{gs}}$. □

As in the Lubin-Tate theory we consider the natural map

$$\begin{array}{rcl} \xi' : B & \longrightarrow & C, \\ f & \longmapsto & (Q \mapsto f(Q -_E Q_0)). \end{array}$$

From the explicit local description of $\mathcal{B}^{\mathrm{gs}}$ we derive

$$\mathcal{B}_L^{\mathrm{gs}} = \mathcal{O}_L \otimes_{\mathcal{O}_K} \mathcal{B}^{\mathrm{gs}}, \quad \mathcal{A}_L^{\mathrm{gs}} = \mathcal{O}_L \otimes_{\mathcal{O}_K} \mathcal{A}^{\mathrm{gs}}.$$

In the terminology of [T2] or [BT] the next proposition shows that $\mathcal{C}$ is a principal homogeneous space for $\mathcal{B}^{\mathrm{gs}}$.

Proposition 5.25 *The map ξ' induces an isomorphism*

$$\xi : \mathcal{O}_L \otimes_{\mathcal{O}_K} \mathcal{B}^{\mathrm{gs}} \longrightarrow \mathcal{O}_L \otimes_{\mathcal{O}_K} \mathcal{C}$$

of $\mathcal{A}_L^{\mathrm{gs}}$-modules.

Proof We show that ξ induces an isomorphism for the localizations at each prime $\mathfrak{Q}$ of $\mathcal{O}_L$. For a prime $\mathfrak{Q}$ dividing $\mathfrak{p}$ this follows from the corresponding result of the Lubin-Tate theory, namely Proposition 4.14. For primes $\mathfrak{Q}$ not dividing $\mathfrak{p}$ we set $\mathfrak{q} = \mathfrak{Q} \cap \mathcal{O}_K$. Then $\mathcal{B}^{\mathrm{gs}}$ is the unique maximal $\mathcal{O}_{K,\mathfrak{q}}$-order in B. By hypothesis (90) the extension L/K is unramified at $\mathfrak{q}$ and therefore $\mathcal{O}_{L,\mathfrak{q}} \otimes \mathcal{B}^{\mathrm{gs}}$ (resp. $\mathcal{O}_{L,\mathfrak{q}} \otimes \mathcal{C}$) is the maximal $\mathcal{O}_{L,\mathfrak{q}}$-order in B (resp. C). Now the result follows, since ξ is obviously an isomorphism on the field level. □

Before we discuss the question of global freeness we explicitly describe the triples $\mathfrak{f}, \mathfrak{p}, r$ for which the hypothesis (90) is not satisfied.

Lemma 5.26 *If $k \neq \mathbb{Q}(\sqrt{-3})$, then E/F and K do not satisfy (90) if and only if one of the following conditions holds:*

(a) $2 = \mathfrak{p}_2\bar{\mathfrak{p}}_2$ *is decomposed in* $k/\mathbb{Q}$, $\mathfrak{p} = \mathfrak{p}_2$, $r = 1$, $\mathfrak{f} = \mathfrak{q}^s, s \geq 1$.

(b) $2 = \mathfrak{p}_2\bar{\mathfrak{p}}_2$ *is decomposed in* $k/\mathbb{Q}$, $\mathfrak{p} = \mathfrak{p}_2$, $r = 1$, $\mathfrak{f} = \mathfrak{q}^s\bar{\mathfrak{p}}_2, s \geq 1$ *and* $(\mathfrak{q}, \bar{\mathfrak{p}}) = 1$.

(c) $2 = \mathfrak{p}_2$ *is inert in* $k/\mathbb{Q}$, $\mathfrak{p} = \mathfrak{p}_2$ *and* $r = 1$, $\mathfrak{f} = \mathfrak{q}^s, s \geq 1$.

(d) $2 = \mathfrak{p}_2^2$ *is ramified in* $k/\mathbb{Q}$, $\mathfrak{p} = \mathfrak{p}_2$, $r \in \{1, 2\}$ *and* $\mathfrak{f} = \mathfrak{q}^s, s \geq 1$.

If $k = \mathbb{Q}(\sqrt{-3})$, *then we have the following exclusions:*

(e) $\mathfrak{p} = (2)$, $r = 1$ *and* $\mathfrak{f} = \mathfrak{q}^s, s \geq 1$.

(f) $\mathfrak{p} = \mathfrak{p}_3$ *(where* $(3) = \mathfrak{p}_3^2$*),* $r = 1$ *and* $\mathfrak{f} = \mathfrak{q}^s, s \geq 1$.

Here $\mathfrak{q}$ *denotes always a prime of* k *with* $(\mathfrak{q}, \mathfrak{p}) = 1$.

Proof Since $\mathfrak{p} \nmid \mathfrak{f}$ the elliptic curve E/K has good reduction for all primes $\mathfrak{Q}$ of $\mathcal{O}_K$ dividing $\mathfrak{p}$. Let $\mathfrak{Q}$ be a prime of $\mathcal{O}_K$ not dividing $\mathfrak{p}$. By Lemma 5.21 it suffices to show that $k(\mathfrak{f}\mathfrak{p}^{r+m})/k(\mathfrak{f}\mathfrak{p}^r)$ is unramified at $\mathfrak{Q}$ for $m \geq 1$, except in the cases mentioned in the Lemma.

Let $\mathfrak{q} = \mathfrak{Q} \cap \mathcal{O}_k$. As before we write $L = k(\mathfrak{f}\mathfrak{p}^{r+m})$ and $K = k(\mathfrak{f}\mathfrak{p}^r)$. Then $\mathfrak{q}$ ramifies in L if and only if $\mathfrak{q} \mid \mathfrak{f}$. Hence we may assume that

$$\mathfrak{f} = \mathfrak{q}^s \mathfrak{f}', \quad (\mathfrak{f}', \mathfrak{q}) = 1, \quad s \geq 1.$$

We denote by $e_{L/k}, e_{K/k}, e_{L/K}$ the ramification indices of primes above $\mathfrak{q}$ in $L/k, K/k, L/K$, respectively. By class field theory (e.g., [Neu, Kap. VI, §7, Aufgabe 1] or [Ha2, Th. IVa]) we derive

$$\begin{aligned} e_{L/k} &= [k(\mathfrak{f}\mathfrak{p}^{r+m}) : k(\mathfrak{f}'\mathfrak{p}^{r+m})] = \frac{w(\mathfrak{f}\mathfrak{p}^{r+m})}{w(\mathfrak{f}'\mathfrak{p}^{r+m})} \Phi(\mathfrak{q}^s), \\ e_{K/k} &= [k(\mathfrak{f}\mathfrak{p}^{r}) : k(\mathfrak{f}'\mathfrak{p}^{r})] = \frac{w(\mathfrak{f}\mathfrak{p}^{r})}{w(\mathfrak{f}'\mathfrak{p}^{r})} \Phi(\mathfrak{q}^s), \end{aligned}$$

where Φ denotes the Euler function of the ring $\mathcal{O}_k$ and $w(\mathfrak{a})$ the order of $\{\zeta \in {\mathcal{O}_k}^* \mid \zeta \equiv 1 (\mathrm{mod}\ \mathfrak{a})\}$ for any integral ideal $\mathfrak{a}$ of $\mathcal{O}_k$. Hence we obtain

$$e_{L/K} = \frac{w(\mathfrak{f}\mathfrak{p}^{r+m}) w(\mathfrak{f}'\mathfrak{p}^r)}{w(\mathfrak{f}'\mathfrak{p}^{r+m}) w(\mathfrak{f}\mathfrak{p}^r)}. \tag{91}$$

If $k \neq \mathbb{Q}(\sqrt{-1}), \mathbb{Q}(\sqrt{-3})$, then we have

$$w(\mathfrak{a}) = \begin{cases} 2, & \text{if } \mathfrak{a} \mid (2), \\ 1, & \text{otherwise.} \end{cases} \tag{92}$$

For $k = \mathbb{Q}(\sqrt{-1})$ we set $(2) = \mathfrak{p}_2^2$. Then we have

$$w(\mathfrak{a}) = \begin{cases} 4, & \text{if } \mathfrak{a} \mid \mathfrak{p}_2, \\ 2, & \text{if } \mathfrak{a} = (2), \\ 1, & \text{otherwise.} \end{cases} \tag{93}$$

Finally, for $k=\mathbb{Q}(\sqrt{-3})$ we set $(3)=\mathfrak{p}_3^2$. Then

$$w(\mathfrak{a})=\begin{cases}6, & \text{if } \mathfrak{a}=(1),\\ 3, & \text{if } \mathfrak{a}=\mathfrak{p}_3,\\ 2, & \text{if } \mathfrak{a}=(2),\\ 1, & \text{otherwise.}\end{cases} \tag{94}$$

Now the assertion of the Lemma follows easiy from (91), (92), (93) and (94). For the convenience of the reader we record the ramification degrees $e_{L/K}$:

	$(a),(b)$	(c)	(d)	(e)	(f)
$k\neq\mathbb{Q}(\sqrt{-1}),\mathbb{Q}(\sqrt{-3})$	2	2	2	–	–
$k=\mathbb{Q}(\sqrt{-1})$	–	–	4, if $r=1, m\geq 2$ 2, if $r=m=1$ 2, if $r=2$	–	–
$k=\mathbb{Q}(\sqrt{-3})$	–	–	–	2	3

□

Due to the lack of appropriate resolvents we are not able to prove a complete result for the question of global freeness of $\mathcal{C}$ over $\mathcal{A}^{\mathrm{ass}}$. As a first global result we obtain

Theorem 5.27 *Assume that $r\geq 1$. If $\mathfrak{f}$ is composite and $(\mathfrak{f},\mathfrak{p}\bar{\mathfrak{p}})=1$, then $\mathcal{C}$ is free of rank one over its associated order $\mathcal{A}^{\mathrm{ass}}$. An explicit generator is given by the map h_θ constructed in the proof of Theorem 5.14.*

Remark 5.28 By Lemma 5.26 the assumptions of the theorem guarantee that hypothesis (90) is satisfied.

Proof Let $h_\theta\in\mathcal{C}$ be the map constructed in Theorem 5.14. Then

$$(h_\theta,\chi)_{Q_0}\sim\mathfrak{p}^m \tag{95}$$

for all abelian characters χ of G. We shall show that the global element h_θ generates $\mathcal{C}_{\mathfrak{Q}}$ at each prime $\mathfrak{Q}$ of $\mathcal{O}_K$.

Let L' be a splitting field for A and B. By Theorem 2.14 we have

$$[\mathcal{C}:h_\theta\cdot\mathcal{A}^\circ]^2_{\mathcal{O}_K}\,\mathcal{O}_{L'}=d_{B/K}\cdot d_{C/K}^{-1}\prod_{\chi\in G}(h_\theta,\chi)^2_{Q_0}. \tag{96}$$

Since B and C are unramified outside $\mathfrak{p}$ by Lemma 5.21 equation (95) implies that $\mathcal{C}_{\mathfrak{Q}}=h_\theta\cdot\mathcal{A}^{\mathrm{ass}}_{\mathfrak{Q}}$ for each prime $\mathfrak{Q}\nmid\mathfrak{p}$.

For primes $\mathfrak{Q}\mid\mathfrak{p}$ it follows from Lemma 5.19 and (95) that for $\tilde{h}_\theta=\Psi(h_\theta)$ we have

$$(\tilde{h}_\theta,\tilde{\chi})_{z(Q_0)}\sim\pi^m.$$

Thus, by Theorem 4.12 (a), $\tilde{h}_\theta$ generates $\tilde{\mathcal{C}}_{\mathfrak{Q}}$ over its associated order. But then Lemma 5.18 implies that $\mathcal{C}_{\mathfrak{Q}}$ is generated by h_θ over $\mathcal{A}_{\mathfrak{Q}}^{\mathrm{ass}}$. □

We now use the fact that the associated orders behave well under a change of the base field to deduce a more complete result from Theorem 5.27. Let w_k denote the number of roots of unity in k.

Theorem 5.29 *Assume that $r \geq 1$. If $(\mathfrak{f}, \mathfrak{p}\bar{\mathfrak{p}}) = 1$ and $(\mathfrak{p}, w_k) = 1$, then $\mathcal{C}$ is free of rank one over its associated order.*

Proof Let $\mathfrak{q}$ be an $\mathcal{O}_k$-prime ideal with $(\mathfrak{f}\mathfrak{p}\bar{\mathfrak{p}}, \mathfrak{q}) = 1$ and set $K' = k(\mathfrak{f}\mathfrak{q}\mathfrak{p}^r), L' = k(\mathfrak{f}\mathfrak{q}\mathfrak{p}^{r+m})$. Since the discriminants $d_{K'/K}$ and d_C are relatively prime, we have

$$\mathcal{O}_{K'} \otimes_{\mathcal{O}_K} \mathcal{C} \simeq \mathcal{C}_{K'}.$$

From this and Theorem 5.24 (or from the explicit local description of $\mathcal{A}^{\mathrm{ass}}$) we derive

$$\mathcal{A}_{K'}^{\mathrm{ass}} \simeq \mathcal{O}_{K'} \otimes_{\mathcal{O}_K} \mathcal{A}^{\mathrm{ass}}. \tag{97}$$

Let $\mathrm{cl}(\mathcal{A}^{\mathrm{ass}})$ (resp. $\mathrm{cl}(\mathcal{A}_{K'}^{\mathrm{ass}})$) denote the classgroup of locally free $\mathcal{A}^{\mathrm{ass}}$-modules (resp. $\mathcal{A}_{K'}^{\mathrm{ass}}$-modules). Because of (97) we have a restriction homomorphism

$$\mathrm{res} : \mathrm{cl}(\mathcal{A}_{K'}^{\mathrm{ass}}) \longrightarrow \mathrm{cl}(\mathcal{A}^{\mathrm{ass}}).$$

From Theorem 5.27 we know that the class $(\mathcal{C}_{K'})_{\mathcal{A}_{K'}^{\mathrm{ass}}}$ of $\mathcal{C}_{K'}$ in $\mathrm{cl}(\mathcal{A}_{K'}^{\mathrm{ass}})$ is trivial. On the other hand $\mathrm{res}((\mathcal{C}_{K'})_{\mathcal{A}_{K'}^{\mathrm{ass}}}) = [K' : K](\mathcal{C}_K)_{\mathcal{A}^{\mathrm{ass}}}$. Varying the extension K'/K we conclude that

$$d \cdot (\mathcal{C}_K)_{\mathcal{A}^{\mathrm{ass}}} = 0 \tag{98}$$

with $d = \gcd\{[K' : K] \mid K'/K \text{ as above }\}$. It follows easily from global class field theory that $d \mid w_k$ (see e.g. [ST, Lemma 3]). Hence we get $w_k \cdot (\mathcal{C}_K)_{\mathcal{A}}^{\mathrm{ass}} = 0$ in $\mathrm{cl}(\mathcal{A}^{\mathrm{ass}})$.

We now consider the base change induced by applying $\mathcal{O}_L \otimes_{\mathcal{O}_K} \_$. From the explicit local desription of the $\mathcal{O}_K$-order $\mathcal{B}^{\mathrm{gs}}$ we derive

$$\mathcal{O}_L \otimes_{\mathcal{O}_K} \mathcal{A}^{\mathrm{gs}} \simeq \mathcal{A}_L^{\mathrm{gs}}.$$

Hence we again have a restriction homomorphism

$$\mathrm{res} : \mathrm{cl}(\mathcal{A}_L^{\mathrm{gs}}) \longrightarrow \mathrm{cl}(\mathcal{A}^{\mathrm{gs}}).$$

We claim that $\mathcal{B}_L^{\mathrm{gs}}$ is a free $\mathcal{A}_L^{\mathrm{gs}}$-module with generator $\pi^m l$, l defined as in (23). Indeed, localizing at a prime $\mathfrak{Q}$ of $\mathcal{O}_L$ dividing $\mathfrak{p}$ this follows from Corollary 4.6. For primes $\mathfrak{Q}$ not dividing $\mathfrak{p}$ we have $\mathcal{B}_{L,\mathfrak{Q}}^{\mathrm{gs}} = \mathrm{Map}(G, \mathcal{O}_{L,\mathfrak{Q}})$ and $\mathcal{A}_{L,\mathfrak{Q}}^{\mathrm{gs}} = \mathcal{O}_{L,\mathfrak{Q}}G$. Thus the claim is immediate, since π is a unit at $\mathfrak{Q}$.

By Proposition 5.25 the $\mathcal{A}_L^{\mathrm{gs}}$-module $\mathcal{O}_L \otimes_{\mathcal{O}_k} \mathcal{C}$ is globally free and we therefore conclude

$$\mathrm{res}\left((\mathcal{O}_L \otimes_{\mathcal{O}_k} \mathcal{C})_{\mathcal{A}_L^{\mathrm{gs}}}\right) = N_{k/\mathbb{Q}}(\mathfrak{p}^m) \cdot (\mathcal{C}_K)_{\mathcal{A}}^{\mathrm{gs}} = 0.$$

Together with (98) this implies $(\mathcal{C}_K)_{\mathcal{A}^{\mathrm{gs}}} = 0$. Since $\mathcal{A}^{\mathrm{gs}}$ is commutative, the Eichler condition holds, and thus $\mathcal{C}$ is a free $\mathcal{A}^{\mathrm{gs}} = \mathcal{A}^{\mathrm{ass}}$-module. □

The next corollary describes consequences of Theorem 5.29 for the classical Galois module structure of rings of integers in abelian extensions of a quadratic imaginary number field.

Corollary 5.30 *Let r, m be integers with $1 \leq m \leq r$. Let $\mathfrak{f}$ be an integral $\mathcal{O}_k$-ideal with $w(\mathfrak{f}) = 1$. Let $\mathfrak{p}$ be an $\mathcal{O}_k$-prime ideal with $(\mathfrak{f}, \mathfrak{p}\bar{\mathfrak{p}}) = 1$ and $(\mathfrak{p}, w_k) = 1$ and set $K = k(\mathfrak{f}\mathfrak{p}^r), L = k(\mathfrak{f}\mathfrak{p}^{r+m})$. Then $\mathcal{O}_L$ is free over its associated order in $K\mathrm{Gal}(L/K)$.*

Proof By [dS, Ch. II, Lemma 1.4] there exists an elliptic curve E defined over $F = k(\mathfrak{f})$ with complex multiplication by $\mathcal{O}_k$ such that the associated Groessencharacter $\psi_{E/F}$ is of the form $\psi_{E/F} = \varphi \circ N_{F/k}$ with a Groessencharacter φ of k of infinity type $(1, 0)$ and conductor $\mathfrak{f}_\varphi = \mathfrak{f}$. Thus the assertion of the corollary follows from Theorem 5.29 and Lemma 5.10. □

Remark 5.31 The extensions $k(\mathfrak{f}\mathfrak{p}^{r+m})/k(\mathfrak{f}\mathfrak{p}^r)$ covered by Corollary 5.30 are not completely contained in the results of [CT] and [Sch2]. On the other hand our results do not completely include the results of [Sch2].

For the construction of the associated orders Schertz uses exactly our approach applied to the analytic Fueter model or the Deuring model of an elliptic curve. His results extending those of Corollary 5.30 are obtained by really tricky constructions of resolvent elements ([Sch2, Satz 2.1 and 2.2]) and some descent argument. However, it is clear from this work, that these methods can not be extended to treat the case $m > r$ for classical Galois module structure.

In the last part of this section we will use the results of Theorems 5.20, 5.24 and 5.27 to derive results in the composite case. Namely, let $\mathfrak{c}$ and $\mathfrak{m}^*$ be integral ideals of k and set $\mathfrak{m} = \mathfrak{c}\mathfrak{m}^*$. We assume that $(\mathfrak{f}, \mathfrak{c}) = 1$ and write

$$\mathfrak{c} = \prod_{i=1}^{s} \mathfrak{p}_i^{m_i}, \quad \mathfrak{m}^* = \prod_{i=1}^{s} \mathfrak{p}_i^{r_i}, \quad \mathfrak{m} = \prod_{i=1}^{s} \mathfrak{p}_i^{r_i+m_i}, \quad 0 \leq r_i, m_i, \quad r_i + m_i \geq 1.$$

We let $G = E[\mathfrak{c}]$ be the group of $\mathfrak{c}$-torsion points and choose primitive $\mathfrak{p}_i^{r_i+m_i}$-torsion points $Q_{i,0}$ for $i = 1, \ldots, s$. If we put

$$Q_0 = Q_{1,0} +_E \ldots +_E Q_{s,0},$$

then Q_0 is a primitive $\mathfrak{m}$-torsion point of E and we easily derive

$$G = \prod_{i=1}^{s} G_i, \tag{99}$$

$$\Gamma := \{Q_0 +_E g \mid g \in G\} = \prod_{i=1}^{s} \Gamma_i, \tag{100}$$

where

$$G_i := E[\mathfrak{p}_i^{m_i}], \quad \Gamma_i := \{Q_{i,0} +_E g \mid g \in G_i\}, \quad i = 1, \dots s.$$

Finally we write $K = F(E[\mathfrak{m}^*]) = k(\mathfrak{f}\mathfrak{m}^*)$, $L = F(E[\mathfrak{m}]) = k(\mathfrak{f}\mathfrak{m})$ and define

$$A = (\bar{K}G)^{\Omega_K}, \quad , B = \mathrm{Map}(G, \bar{K})^{\Omega_K}, \quad C = \mathrm{Map}(\Gamma, \bar{K})^{\Omega_K}.$$

For $i = 1, \dots, s$ set $\mathfrak{f}_i = \mathfrak{f}\mathfrak{m}^*/\mathfrak{p}_i^{r_i}$ and assume that either

$$\begin{array}{ll} & r_i = 0 \\ \text{or} & m_i = 0 \\ \text{or} & m_i, r_i \geq 1, \quad (\mathfrak{f}_i, \mathfrak{p}_i\bar{\mathfrak{p}}_i) = 1 \text{ and } (\mathfrak{p}_i, w_k) = 1 \\ \text{or} & m_i, r_i \geq 1, \quad \mathfrak{f}_i \text{ is composite and } (\mathfrak{f}_i, \mathfrak{p}_i\bar{\mathfrak{p}}_i) = 1. \end{array}$$

Let $\mathcal{B}^{\mathrm{gs}} \subseteq B$ denote the $\mathcal{O}_K$-Hopf order which represents the affine $\mathcal{O}_K$-group scheme of $\mathfrak{c}$-torsion on E. As before we write $\mathcal{A}^{\mathrm{gs}}$ for its Cartier dual in A.

Theorem 5.32 *Assume the notation and conditions as above. Then $\mathcal{C}$ is free over its associated order $\mathcal{A}^{\mathrm{ass}}$ in A. If, in addition, $r_i \geq 1$ for $i = 1, \dots, s$, then $\mathcal{A}^{\mathrm{ass}} = \mathcal{A}^{\mathrm{gs}}$.*

Remark 5.33 $\mathcal{A}^{\mathrm{ass}}$ and a generating element are explicitly given in the proof.

Proof Writing $A_i = (\bar{K}G_i)^{\Omega_K}$, $C_i = \mathrm{Map}(\Gamma_i, \bar{K})^{\Omega_K}$, it is easily verified that firstly

$$A \simeq A_1 \otimes_K \dots \otimes_K A_s,$$

and secondly that

$$\begin{array}{rcl} C_1 \otimes_K \dots \otimes_K C_s & \longrightarrow & C, \\ h_1 \otimes_K \dots \otimes_K h_s & \longmapsto & \big(Q_1 +_E \dots +_E Q_s \mapsto h_1(Q_1) \cdots h_s(Q_s)\big) \end{array} \tag{101}$$

is an isomorphism of A-modules.

By Theorem 5.20 or 5.27 there exists a map $h_i \in \mathcal{C}_i$ such that $\mathcal{C}_i = h_i \cdot \mathcal{A}_i^{\mathrm{ass}}$ for each $i \in \{1, \dots, s\}$, where $\mathcal{C}_i$ denotes the integral closure of $\mathcal{O}_K$ in C_i and $\mathcal{A}_i^{\mathrm{ass}}$ its associated order in A_i. Since the discriminants $d_{C_1/K}, \dots, d_{C_s/K}$ are mutually coprime, the isomorphism in (101) restricts to an isomorphism

$$\mathcal{C}_1 \otimes_{\mathcal{O}_K} \dots \otimes_{\mathcal{O}_K} \mathcal{C}_s \longrightarrow \mathcal{C}$$

of $\mathcal{A}_1^{\mathrm{ass}} \otimes_{\mathcal{O}_K} \dots \otimes_{\mathcal{O}_K} \mathcal{A}_s^{\mathrm{ass}}$-modules. Therefore

$$\mathcal{A}^{\mathrm{ass}} \simeq \mathcal{A}_1^{\mathrm{ass}} \otimes_{\mathcal{O}_K} \dots \otimes_{\mathcal{O}_K} \mathcal{A}_s^{\mathrm{ass}} \tag{102}$$

and a generating function is given by the image of $h_1 \otimes \dots \otimes h_s$ under the isomorphism in (101).

If $r_i \geq 1$ for $i = 1, \dots, s$, then (102) and Theorem 5.24 imply $\mathcal{A}^{\mathrm{ass}} = \mathcal{A}^{\mathrm{gs}}$.

$\square$

6 Kummer orders and Taylor's conjecture

In [T2], M.J. Taylor introduced the notion of a Kummer order with respect to the group law of an abelian variety. In this section we shall study the Galois module structure of these Kummer orders in the case when the variety is an elliptic curve.

We begin by describing the situation considered by Taylor. For more details the reader is referred to [T2] and [ST].

As always, let k denote a quadratic imaginary number field. Let M/k be a finite extension and E/M an elliptic curve with everywhere good reduction and admitting complex multiplication by $\mathcal{O}_k$. Let $\mathfrak{a}$ be a non-zero integral ideal and set

$$\begin{aligned} &G(\mathfrak{a}) = E[\mathfrak{a}], \quad A(\mathfrak{a}) = A_M(\mathfrak{a}) = (\bar{M}G(\mathfrak{a}))^{\Omega_M}, \\ &B(\mathfrak{a}) = B_M(\mathfrak{a}) = \mathrm{Map}(G(\mathfrak{a}), \bar{M})^{\Omega_M}. \end{aligned}$$

In the following we will define an M-algebra M_P for each $P \in E(M)$. If $\mathfrak{a} = (a)$ is principal, then M_P is given by

$$M_P = \mathrm{Map}(G_P(\mathfrak{a}), \bar{M})^{\Omega_M},$$

with $G_P(\mathfrak{a}) = \{P' \in E(\bar{M}) \mid [a](P') = P\}$. In the general case the definition is more involved. Since we will need it later we recall some details from [ST].

For integers $i \geq j \geq 0$ we fix an isomorphism of groups

$$\tau : G(\mathfrak{a}^i)/G(\mathfrak{a}^j) \longrightarrow G(\mathfrak{a}^{i-j}). \tag{103}$$

We always assume that τ is Ω_M-equivariant. The group $G(\mathfrak{a}^j)$ acts on $\bar{M}G(\mathfrak{a}^i)$ by translation and (103) induces an isomorphism

$$\begin{aligned} \tilde{\tau} : \left(\bar{M}G(\mathfrak{a}^i)\right)^{G(\mathfrak{a}^j)} &\longrightarrow \bar{M}G(\mathfrak{a}^{i-j}), \\ \textstyle\sum_{g \in G(\mathfrak{a}^i)} a_g g &\longmapsto \textstyle\sum_{g \in G(\mathfrak{a}^i)} a_g \tau(g). \end{aligned} \tag{104}$$

Note that $\tilde{\tau}$ is Ω_M-equivariant if τ has this property.

Next we choose a positive integer h such that $\mathfrak{a}^h = (a)$ is principal and set

$$M_P(\mathfrak{a}) = \left(\mathrm{Map}(G_P((a)), \bar{M})^{G(\mathfrak{a}^{h-1})}\right)^{\Omega_M}. \tag{105}$$

In the following we write $G = G(\mathfrak{a})$, $A = A(\mathfrak{a})$, $B = B(\mathfrak{a})$ and $M_P = M_P(\mathfrak{a})$. Then A acts on M_P via the rule

$$\left(f \cdot \sum_{g \in G((a))} a_g g\right)(P') = \sum_{g \in G((a))} a_g f(P' +_E g).$$

Let $\mathcal{B}^{\mathrm{gs}} \subseteq B$ be the $\mathcal{O}_M$-group scheme of $\mathfrak{a}$-torsion on E and denote by $\mathcal{A}^{\mathrm{gs}}$ its Cartier dual in A. Recall that $\mathcal{B}^{\mathrm{gs}}$, $\mathcal{A}^{\mathrm{gs}}$ are Hopf orders in B, A, respectively.

Let $\mathcal{O}_P = \mathcal{O}_P(M)$ be the integral closure of $\mathcal{O}_M$ in M_P and define the Kummer algebra $\tilde{\mathcal{O}}_P$ to be the largest $\mathcal{A}^{\mathrm{gs}}$-module contained in $\mathcal{O}_P$, i.e.,

$$\tilde{\mathcal{O}}_P = \tilde{\mathcal{O}}_P(M) = \{x \in \mathcal{O}_P \mid x\mathcal{A}^{\mathrm{gs}} \subseteq \mathcal{O}_P\}.$$

In [T2] it is proved that $\tilde{\mathcal{O}}_P$ is a locally free $\mathcal{A}^{\mathrm{gs}}$-module and moreover that

$$\psi : E(M) \longrightarrow \mathrm{cl}(\mathcal{A}^{\mathrm{gs}}), \quad P \longmapsto \left(\tilde{\mathcal{O}}_P\right)_{\mathcal{A}^{\mathrm{gs}}}$$

is a group homomorphism. Herein $\mathrm{cl}(\mathcal{A}^{\mathrm{gs}})$ denotes the classgroup of locally free $\mathcal{A}^{\mathrm{gs}}$-modules and $\left(\tilde{\mathcal{O}}_P\right)_{\mathcal{A}^{\mathrm{gs}}}$ the class of $\tilde{\mathcal{O}}_P$ in $\mathrm{cl}(\mathcal{A}^{\mathrm{gs}})$.

In [T2] the following conjecture was stated:

Conjecture 6.1 *For any non-zero $\mathcal{O}_k$-ideal (a), $a \in \mathcal{O}_k$,*

$$E(M)_{\mathrm{tor}} \subseteq \ker\psi.$$

In [ST] Conjecture 6.1 was generalized for arbitrary integral ideals and furthermore they proved

Theorem *Let $(\mathfrak{a}, w_k) = 1$, where w_k denotes the number of roots of unity in k. Then*

$$E(M)_{\mathrm{tor}} \subseteq \ker\psi.$$

□

Recently, A. Agboola proved an analogue of the Theorem of Srivastav and Taylor for elliptic curves without complex multiplication. Namely, let $p > 3$ be a rational prime and consider the conjecture for $\mathfrak{a} = (p^i), i \geq 1$. Then, by [Ag, Theorem 1],

$$E(M)_{\mathrm{tor}} \subseteq \ker\psi.$$

See also [Pa], where among other things, a group scheme theoretic proof of Agboola's Theorem is given. Finally we mention that Agboola's Theorem does not hold for $p = 2$ as the infinite series of counter-examples in [BK] shows.

In the sequel we will apply the results of Section 5.7 in order to derive results concerning Conjecture 6.1.

Let F be a finite abelian extension of k and let E/F be an elliptic curve with complex multiplication by $\mathcal{O}_k$. Assume further that $F(E_{\mathrm{tor}})/k$ is abelian. Let $\mathfrak{f}$ be defined as in (44). Let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_k$ such that $(\mathfrak{f}, \mathfrak{p}) = 1$. Let P be a primitive $\mathfrak{p}^r$-torsion point, $r \geq 1$, and let $\mathfrak{a} = \mathfrak{p}^m$, $m \geq 1$. Set $K = F(E(\mathfrak{f}\mathfrak{p}^r]) = k(\mathfrak{f}\mathfrak{p}^r)$.

Theorem 6.2 *Assume the above notation and suppose that E/F and K satisfy the hypothesis (90). Then, for $M = K$,*

$$\mathcal{A}^{\mathrm{gs}} = \mathcal{A}^{\mathrm{ass}}, \text{ and therefore } \mathcal{O}_P = \tilde{\mathcal{O}}_P.$$

Remarks 6.3 (i) The hypothesis (90) is almost always satisfied, except in the cases listed in Lemma 5.26.

(ii) During the proof of Theorem 6.2 we will show that there exists an isomorphism of A-modules

$$M_P \simeq C = \mathrm{Map}(\Gamma, \bar{M})^{\Omega_M},$$

where $\Gamma = \{Q_0 +_E g \mid g \in E[\mathfrak{p}^m]\}$ with an appropriate primitive $\mathfrak{p}^{r+m}$-torsion point Q_0. $\mathcal{A}^{\mathrm{ass}}$ can therefore be viewed as the associated order of the integral closure $\mathcal{C}$ of $\mathcal{O}_M$ in C or as the associated order of $\mathcal{O}_P$.

(iii) Theorem 6.2 generalizes [T2, Remark 2, p.431].

Proof of Theorem 6.2 The Theorem follows immediatedly from Theorem 5.23, if we can show that there exists an isomorphism of A-modules

$$M_P \simeq C = \mathrm{Map}(\Gamma, \bar{M})^{\Omega_M}$$

for an appropriate set $\Gamma = \{Q_0' +_E g' \mid g' \in E[\mathfrak{p}^m]\}$ with a primitive $\mathfrak{p}^{r+m}$-torsion point Q_0'.

Let $h \in \mathbb{N}$ be such that $(\mathfrak{p}^m)^h = (a)$ is principal and recall the definition of M_P in (103) – (105). We choose $b \in \mathcal{O}_k$ such that $(b) = (\mathfrak{p}^m)^{h-1} \cdot \mathfrak{b}$ with an integral $\mathcal{O}_k$-ideal $\mathfrak{b}$ such that $(\mathfrak{b}, \mathfrak{p}) = 1$ and specify an isomorphism τ as in (103) by

$$\begin{array}{rcl} \tau : G(\mathfrak{a}^h)/G(\mathfrak{a}^{h-1}) & \longrightarrow & G(\mathfrak{a}), \\ g + G(\mathfrak{a}^{h-1}) & \longmapsto & [b](g). \end{array}$$

Then the induced isomorphism

$$\tilde{\tau} : \left(\bar{M}G(\mathfrak{a}^h)\right)^{G(\mathfrak{a}^{h-1})} \longmapsto \bar{M}G(\mathfrak{a}) \tag{106}$$

is Ω_M-equivariant and we may therefore identify the Ω_M-invariants.

The set $G_P((a))$ is of the form

$$G_P((a)) = \{Q_0 +_E g \mid g \in G((a))\},$$

where Q_0 is a primitive $\mathfrak{p}^{r+mh}$-torsion point such that $[a](Q_0) = P$. We set $Q_0' = [b](Q_0)$ and note that Q_0' is a primitive $\mathfrak{p}^{r+m}$-torsion point. Let $\Gamma = \{Q_0' +_E g' \mid g' \in G(\mathfrak{a})\}$ and consider the natural map

$$\begin{array}{rcl} \Psi : \mathrm{Map}\big(G_P((a)), \bar{M}\big)^{G(\mathfrak{a}^{h-1})} & \longrightarrow & \mathrm{Map}(\Gamma, \bar{M}), \\ f & \longmapsto & f', \end{array}$$

where $f'(\gamma') = f(\gamma)$ with $\gamma \in G_P((a))$ such that $[b](\gamma) = \gamma'$. Ψ is well-defined since $[b](\gamma_1) = [b](\gamma_2)$ implies $\gamma_1 -_E \gamma_2 \in G(\mathfrak{a}^{h-1})$. The map Ψ is obviously bijective and also Ω_M-equivariant:

$$\begin{array}{rcl} (\Psi(f^\omega))\,(Q_0' +_E [b](g)) & = & f^\omega(Q_0 +_E g) = \omega\left(f(Q_0^{\omega^{-1}} +_E g^{\omega^{-1}})\right) \\ (\Psi(f)^\omega)\,(Q_0' +_E [b](g)) & = & \omega\left(\Psi(f)(Q_0'^{\,\omega^{-1}} +_E [b](g)^{\omega^{-1}})\right) = \omega\left(f(Q_0^{\omega^{-1}} +_E g^{\omega^{-1}})\right). \end{array}$$

Hence it remains to show that Ψ is an A-module homomorphism where we identify $\left(\left(\bar{M}G(\mathfrak{a}^h)\right)^{G(\mathfrak{a}^{h-1})}\right)^{\Omega_M}$ and $\left(\bar{M}G(\mathfrak{a})\right)^{\Omega_M}$ via (106). To that end we have to establish the equality

$$\Psi\left(f\left(\sum_{g\in G(\mathfrak{a}^h)} a_g g\right)\right) = \Psi(f)\cdot \sum_{g\in G(\mathfrak{a}^h)} a_g[b](g),$$

where $\sum_{g\in G(\mathfrak{a}^h)} a_g g \in \left(\bar{M}G(\mathfrak{a}^h)\right)^{G(\mathfrak{a}^{h-1})}$. Since $a_{g+_E g_1} = a_g$ for $g_1 \in G(\mathfrak{a}^{h-1})$ and $f(\gamma +_E g_1) = f(\gamma)$ we easily compute

$$\begin{aligned}\left(\Psi\big(f(\sum_{g\in G(\mathfrak{a}^h)} a_g g)\big)\right)(\gamma') &= \sum_{g\in G(\mathfrak{a}^h)} a_g f(\gamma +_E g)\\ &= |G(\mathfrak{a}^{h-1})| \sum_{g\in G(\mathfrak{a}^h)/G(\mathfrak{a}^{h-1})} a_g f(\gamma +_E g)\end{aligned}$$

and, since $[b](g_1) = 0_E$ for $g_1 \in G(\mathfrak{a}^{h-1})$,

$$\begin{aligned}\left(\Psi(f)\cdot \sum_{g\in G(\mathfrak{a}^h)} a_g[b](g)\right)(\gamma') &= \sum_{g\in G(\mathfrak{a}^h)} a_g \Psi(f)(\gamma' +_E [b](g))\\ &= \sum_{g\in G(\mathfrak{a}^h)/G(\mathfrak{a}^{h-1})} |G(\mathfrak{a}^{h-1})| a_g f(\gamma +_E g).\end{aligned}$$

□

Finally we apply Theorem 5.27 to exhibit an infinite class of elliptic curves E/M with everywhere good reduction for which Taylor's conjecture holds in full generality. To that end let $\mathfrak{f}$ be a composite $\mathcal{O}_k$-ideal such that $w(\mathfrak{f}) = 1$. By [dS, Ch. II, Lemma 1.4] there exists an elliptic curve E defined over $F = k(\mathfrak{f})$ with complex multiplication by $\mathcal{O}_k$ such that the associated Groessencharacter $\psi_{E/F}$ is of the form $\psi_{E/F} = \varphi \circ N_{F/k}$ with a Groessencharacter φ of k of infinity type $(1,0)$ and conductor $\mathfrak{f}_\varphi = \mathfrak{f}$.

Theorem 6.4 *Let $\mathfrak{f}$ be a composite integral $\mathcal{O}_k$-ideal with $w(\mathfrak{f}) = 1$ and $(\mathfrak{f}, w_k) = 1$. Let $E/k(\mathfrak{f})$ be an elliptic curve as above and let M be any extension of $k(\mathfrak{f})$ such that E/M has everywhere good reduction. Then Taylor's conjecture holds in full generality, i.e.,*

$$E(M)_{\mathrm{tor}} \subseteq \ker(\psi)$$

for all integral ideals $\mathfrak{a}$ of $\mathcal{O}_k$.

Proof From [ST, Theorem 1] we already know that the theorem holds for $\mathfrak{a}$ relatively prime with w_k. As it is shown in [ST, §2] it therefore suffices to prove

$P \in \ker \psi$ for $\mathfrak{a} = \mathfrak{p}^m$, $\mathfrak{p} \mid w_k$, $m \geq 1$ and P a torsion point with $\mathfrak{p}$-power $\mathcal{O}_k$-annihilator.

Suppose that $P \in E(M)$ is a primitive $\mathfrak{p}^r$-trosion point for some $r \geq 0$. By [T2, Proposition 2] we may assume that $r \geq 1$. Hence M contains the ray class field $K = F(E[\mathfrak{p}^r]) = k(\mathfrak{f}\mathfrak{p}^r)$ by Proposition 5.3. By Lemma 5.26 E/K has everywhere good reduction. Thus Theorem 5.27 and Theorem 6.2 imply that $\mathcal{C}_K \simeq \tilde{\mathcal{O}}_P$ is free over its associated order $\mathcal{A}_K^{\mathrm{ass}} = \mathcal{A}_K^{\mathrm{gs}}$. The result follows now by applying $\mathcal{O}_M \otimes_{\mathcal{O}_K} \_$, since both $\mathcal{A}_K^{\mathrm{gs}}$ and $\tilde{\mathcal{O}}_P$ behave well with respect to a change of fields (see [ST, (2.2a), (2.5), (2.6)]). $\square$

Part II
The conjecture of Chinburg-Stark for abelian extensions of a quadratic imaginary field

1 Introduction

This part is concerned with a strong version of Stark's conjecture [St] for abelian extensions of an imaginary quadratic number field.

Let N/K be a finite Galois extension of number fields with Galois group G. Let S be a finite G-stable set of places of N containing the set S_∞ of archimedean places. We write E_S for the $\mathbb{Z}G$-module of S-units of N. For $S = S_\infty$ we also set $E_N = E_{S_\infty}$.

Let $\mathbb{Z}S$ denote the free $\mathbb{Z}$-module on S, with G acting by permuting the primes in S. Let ΔS be the kernel of the augmentation map $\mathbb{Z}S \to \mathbb{Z}$ which sends every place $\mathfrak{p}$ in S to 1. Then the Dirichlet unit theorem implies that $\mathbb{Q}\otimes_{\mathbb{Z}} E_S \simeq \mathbb{Q}\otimes_{\mathbb{Z}} \Delta S$ as $\mathbb{Q}G$-modules. Therefore we may fix (but not canonically) a G-embedding $\varphi : \Delta S \to E_S$.

For any complex valued character χ of G we write $R_\varphi(\chi)$ for the Tate regulator associated to φ and χ in [Ta2] (see also Definition 2.4).

Let $L(s,\chi)$ denote the Artin L-function associated to χ with the Euler factors at places of S omitted. Let $c(\chi)$ denote the first non-zero coefficient in the Taylor expansion of $L(s,\chi)$ at $s = 0$. Thus $R_\varphi(\chi)$ and $c(\chi)$ are non-zero, possibly transcendental complex numbers and the idea of Stark's conjecture is that $R_\varphi(\chi)$ accounts precisely for the transcendental part of $c(\chi)$. Setting

$$A_\varphi(\chi) = \frac{R_\varphi(\chi)}{c(\chi)}$$

Tate's formulation of Stark's conjecture is as follows:

Stark's conjecture

$$A_\varphi(\chi)^\sigma = A_\varphi(\chi^\sigma) \text{ for all } \sigma \in \mathrm{Aut}_{\mathbb{Q}}(\mathbb{C}).$$

In particular, it is conjectured that $A_\varphi(\chi)$ is contained in the field $\mathbb{Q}(\chi)$ of character values of χ. Note that Stark's conjecture is known to be true for abelian extensions of $\mathbb{Q}$ and for abelian extensions of an imaginary quadratic number field (both cases are a consequence of [Ta2, Ch.IV, Prop.3.9]).

We fix a subfield F of $\mathbb{C}$ such that $F/\mathbb{Q}$ is a finite Galois extension and so that every representation of G is realizable over F. The field F is just an auxiliary field which is needed for housing the invariants that we will attach to N/K. For any number field M we write $\mathcal{O}_M$ for the ring of algebraic integers of M.

Let now S be large in the following sense: assume that S contains S_∞ and the set of all ramified primes in N/K, and that the S-class group cl_S is trivial. Then a strong version of Stark's conjecture, due to Chinburg [Ch1], asserts that the fractional $\mathcal{O}_F$-ideal generated by $A_\varphi(\chi)$ is an Euler characteristic $\mathcal{O}_F$-ideal $q_\varphi(\chi)$ (see Definition 2.2) constructed from the Galois cohomologies of ΔS and E_S. This was first proved by Tate [Ta2] for $\mathbb{Q}$-valued characters and recently by Ritter and Weiss (up to difficulties with the prime 2) for extensions N/K with $N/\mathbb{Q}$ abelian and all characters χ of $G = \mathrm{Gal}(N/K)$. We will refer to this strong form of Stark's conjecture as the conjecture of Chinburg-Stark.

If M is a number field let h_M denote the class number of M. For two fractional $\mathcal{O}_M$-ideals $\mathfrak{a}$ and $\mathfrak{b}$ and a rational prime l we write $\mathfrak{a} \sim_l \mathfrak{b}$ if and only if $(\mathfrak{a}/\mathfrak{b}, l) = 1$. Then the first main result of this paper reads as follows

Theorem 1.1 *Let N/k be an abelian extension of an imaginary quadratic number field k. Let l be a rational prime such that $l \nmid [N:k]h_k$. Let N/K be a subextension of N/k. Then*

$$q_\varphi(\chi) \sim_l A_\varphi(\check{\chi})\mathcal{O}_F$$

for all characters χ of $G = \mathrm{Gal}(N/K)$. Here $\check{\chi}$ denotes the contragredient of χ.

Since q_φ and A_φ are both functorial with respect to induction of characters it suffices to prove Theorem 1.1 for the extension N/k. The proof of Theorem 1.1 follows closely the strategy of Ritter and Weiss for their proof of $q_\varphi(\chi) = A_\varphi(\chi)$ in the cyclotomic case [RW2, Theorem A]. The starting point is a generalized Tate sequence of [RW1] associated to S

$$0 \longrightarrow E_S \longrightarrow A \longrightarrow B \longrightarrow \nabla \longrightarrow 0 \tag{1}$$

with A cohomologically trivial, B stably free and where ∇ originates from a unique extension

$$0 \longrightarrow \mathrm{cl}_S \longrightarrow \nabla \longrightarrow \bar{\nabla} \longrightarrow 0,$$

where $\bar{\nabla}$ is a known $\mathbb{Z}G$-lattice. For large sets S we have $\nabla = \Delta S$ and thus (1) generalizes the Tate sequence of [Ta1] which was originally used in the definition of q_φ (see [Ta2, Ch.II, Def.6.2]).

For arbitrary sets S (always assuming $S_\infty \subseteq S$) the invariant q_φ is attached to G-homomorphisms

$$\varphi : \nabla \longrightarrow E_S \oplus \mathbb{Z}G^r, \tag{2}$$

with finite kernel and cokernel. Here r denotes the number of G-orbits of ramified primes which are not in S. If we adapt A_φ to these φ (see Definition 2.5) then [RW2, Theorem B] asserts that the ratio

$$\mathfrak{a}(\chi) = \frac{A_\varphi(\check{\chi})}{q_\varphi(\chi)}$$

is independent of S and φ.

This result allows to work with the set $S = S_\infty$. To prove Theorem 1.1 it is necessary to construct an explicit G-homomorphism φ as in (2). In practice it is sometimes possible to define G-embeddings $\underline{\varphi} : \Delta S \to E_N$ by means of explicitly known units such as the cyclotomic and elliptic ones. In [RW2, Section 8] a recipe is given how to derive a G-map φ from a given $\underline{\varphi}$. Using this explicit construction of φ, Ritter and Weiss also compute an expression for $\mathfrak{a}(\chi)$ in terms of $\underline{\varphi}$, up to fractional $\mathcal{O}_F$-ideal factors which divide $|G|$. Therefore a main step towards a proof of the Chinburg-Stark conjecture is the construction of a G-embedding $\underline{\varphi}$. This will be done in Section 5.

In order to be able to approach the conjecture of Chinburg-Stark prime by prime we shall interprete the ideal $\mathfrak{a}(\chi)$ l-adically. Let $\bar{\mathbb{Q}}$ denote a fixed algebraic closure of $\mathbb{Q}$. Fix a rational prime l and denote by $\mathbb{C}_l$ a fixed completion of an algebraic closure of the l-adic rationals $\mathbb{Q}_l$. Choose an embedding $i_l : \bar{\mathbb{Q}} \to \mathbb{C}_l$ and write F_l for the completion of $i_l(F)$ in $\mathbb{C}_l$. Let $\mathcal{O}_l$ denote the valuation ring of F_l. If χ_l is a $\mathbb{C}_l$-character of G, then $\chi_l = i_l \circ \chi$ for a unique F-character χ and we define $\mathfrak{a}^{(l)}(\chi_l) = i_l(\mathfrak{a}(\chi))\mathcal{O}_l$.

Our aim is to show that $\mathfrak{a}(\chi)$ is prime to l for all characters χ of G. By a variant of [We, Chapter 14, Prop. 10] it is enough to prove that $\mathfrak{a}^{(l)}(\psi)^{-1}$ is integral whenever ψ is a non-trivial $\mathbb{Q}_l$-irreducible character of a subextension N'/K' of N/k with $([N' : K'], l) = 1$ and $[K' : k] = l^t, t \geq 0$. We may therefore assume the following situation

$$\begin{tikzcd}
& N \arrow[dl, dash, "l'"'] \arrow[dr, dash, "l^t"] & \\
K \arrow[dr, dash, "l^t"'] & & K_0 \arrow[dl, dash, "l'"] \\
& k &
\end{tikzcd}$$

with $(l, l') = 1$, $t \geq 0$ and ψ a non-trivial $\mathbb{Q}_l$-irreducible character of $G = \mathrm{Gal}(N/K)$.

Corollary 1.2 *Let N/k be an abelian p-extension of an imaginary quadratic number field k. Let l be a rational prime such that $l = p$ or $l \nmid h_k$. Let N/K be a subextension of N/k. Then*

$$q_\varphi(\chi) \sim_l A_\varphi(\check{\chi})\mathcal{O}_F$$

for all characters χ of $G = \mathrm{Gal}(N/K)$. In particular, $q_\varphi(\chi) = A_\varphi(\check{\chi})\mathcal{O}_F$, if $h_k = 1$.

Proof For primes $l \neq p$ the assertion follows from Theorem 1.1. For $l = p$ the result is immediate from the above discussion. □

Let ψ be a non-trivial $\mathbb{Q}_l$-character of $G = \mathrm{Gal}(N/K)$. The computations of Section 5 and 6 reduce the problem of proving the integrality of $\mathfrak{a}^{(l)}(\psi)^{-1}$ essentially to the problem of establishing a divisibility result of the form

$$\ell_{\mathbb{Z}_l}\left((\mathbb{Z}_l \otimes_{\mathbb{Z}} \mathrm{cl}_N)^{\psi}\right) \mid \ell_{\mathbb{Z}_l}\left((\mathbb{Z}_l \otimes_{\mathbb{Z}} (E_N/\mathcal{C}_N))^{\psi}\right). \tag{3}$$

Here, for a torsion $\mathbb{Z}_l$-module X, $\ell_{\mathbb{Z}_l}(X)$ denotes the usual $\mathbb{Z}_l$-order ideal of X (see e.g. [CR, page 86]). Writing e_ψ for the idempotent associated to ψ, the $\mathbb{Z}_l G$-submodule $X^\psi = e_\psi X$ is the ψ-eigenspace of the $\mathbb{Z}_l G$-module X. Finally, $\mathcal{C}_N$ denotes the group of elliptic units defined by Rubin in [Ru2]. In [Ru2], $\mathcal{C}_N$ is only defined for extensions N containing the Hilbert class field $k(1)$. In fact it suffices to require that N contains the Hilbert-l-class field $k(1)_l$. This is the reason for the restriction to primes $l \nmid h_k$ in Theorem 1.1.

Using Kolyvagin's Euler system method [Ko], the divisibility assertion (3) is proved in [Ru2, Section 3] under the additional assumption $l \nmid [N : k]$. This assumption is responsible for the restriction to primes $l \nmid [N : k]$ in Theorem 1.1.

At this point we should compare Theorem 1.1 to the result of Ritter and Weiss. The essential reason why they can prove an almost complete result for abelian extensions N of $\mathbb{Q}$ is that the main conjecture of Iwasawa theory for totally real fields is known to be true by famous work of A.Wiles [Wi]. Indeed, their problems with the prime 2 are only due to the present state of the main conjecture. It should also be remarked that for the proof of their main theorem it is not enough to know the main conjecture over $\mathbb{Q}$, but also for certain totally real fields.

Using Rubin's work [Ru2] on the "main conjectures" for imaginary quadratic fields we can prove a kind of a complementary result to Theorem 1.1.

Theorem 1.3 *Let k be an imaginary quadratic number field with class number $h_k = 1$. Let l be a prime and let K_0/k be abelian with $l \nmid [K_0 : k]$. Let K_∞/K_0 be a $\mathbb{Z}_l$-extension such that K_∞/k is abelian. Assume that every $\mathcal{O}_k$-prime ideal $\mathfrak{p}$ which divides l and ramifies in K_∞/K_0 does not split in K_0/k. Let N/K_0 be a finite subextension of K_∞/K_0 and assume that l does not divide the number of roots of unity in N. Then*

$$q_\varphi(\chi) \sim_l A_\varphi(\check{\chi})$$

for all characters χ of $G = \mathrm{Gal}(N/k)$.

To illustrate Theorem 1.3 we consider an example.

Example Let k be an imaginary quadratic number field with class number $h_k = 1$. Let $l \neq 2$ be a rational prime that splits in $k/\mathbb{Q}$ and write $l = \mathfrak{p}\bar{\mathfrak{p}}$, $\mathfrak{p} \neq \bar{\mathfrak{p}}$. For $n \geq 0$ we set $K_n = k(\mathfrak{p}^{n+1})$. Then K_∞/K_0 is a $\mathbb{Z}_l$-extension, which is obviously abelian over k. If we consider $N = K_n$, $n \geq 1$, then $q_\varphi(\chi) \sim_l A_\varphi(\check{\chi})$ for all characters χ of $\mathrm{Gal}(N/k)$.

We conclude this introductory Section with a brief outline of the structure of this part. In Sections 2 and 3 we recall the necessary definitions and results from [RW2]. Section 5 is devoted to the construction of an embedding $\underline{\varphi} : \Delta S \to E_N$. The construction of $\underline{\varphi}$ is motivated by the construction of Ramachandra units (see [Wa, Ch.8]) with cyclotomic units replaced by elliptic units. The relevant results on elliptic units are collected in Section 4. In Section 6 we construct another group $\mathcal{C}_{\mathrm{Ha}}$ of explicit units and compute the index of $\mathrm{im}(\underline{\varphi})$ in $\mathcal{C}_{\mathrm{Ha}}$. The group $\mathcal{C}_{\mathrm{Ha}}$ is independent of $\underline{\varphi}$ and contained in $\mathcal{C}_N$. The knowledge of the index $[\mathcal{C}_{\mathrm{Ha}} : \mathrm{im}(\underline{\varphi})]$ allows therefore to reduce the proof of Theorem 1.1 to the divisibility assertion (3). This is achieved in Section 7, where the main theorems are proved. Finally, in Section 8, we discuss the implications of our results for the Galois module structure of units.

2 Preliminary results

Let N/K be a finite Galois extension of number fields and write $G = \mathrm{Gal}(N/K)$. Let S be a finite G-stable set of primes of N containing the set S_∞ of archimedian primes.

In this section we briefly recall the construction of Ritter and Weiss [RW2] of a q-index and an A-number for such a set S. Originally these invariants were only defined when S is *large*, i.e., when S contains S_∞ and all ramified primes and the S-class group cl_S is trivial (see [Ta2] and [Ch1]). The definitions were based on a so-called Tate sequence [Ta1] for large sets S which gives a cohomological connection between E and ΔS. The new definitions use the generalized Tate sequence of [RW1] which we shall describe first.

Let $\mathfrak{P}$ be a prime of N and put $\mathfrak{p} = \mathfrak{P} \cap \mathcal{O}_K$. We write $N_\mathfrak{P}/K_\mathfrak{p}$ for the localization of N/K. Let $G_\mathfrak{P}$ denote the decomposition group, $I_\mathfrak{P}$ the inertia group and $\phi_\mathfrak{P}$ the Frobenius automorphism of the corresponding residue class extension. In addition, set $\bar{G}_\mathfrak{P} = G_\mathfrak{P}/I_\mathfrak{P}$, $e_\mathfrak{P} = |I_\mathfrak{P}|$ and $f_\mathfrak{P} = |\bar{G}_\mathfrak{P}|$. For any group H we write ΔH for the kernel of the augmentation map.

Definition 2.1 [GW] The inertial lattice $W_\mathfrak{P}$ attached to $N_\mathfrak{P}/K_\mathfrak{p}$ is the free $\mathbb{Z}$-module on the basis

$$w_g = (g-1, 1 + \phi_\mathfrak{P} + \ldots + \phi_\mathfrak{P}^{a(g)-1}) \in \Delta G_\mathfrak{P} \oplus \mathbb{Z}\bar{G}_\mathfrak{P}, \quad g \in G_\mathfrak{P},$$

where $\bar{g} = (g \bmod I_\mathfrak{P}) = \phi_\mathfrak{P}^{a(g)}$ and $1 \le a(g) \le f_\mathfrak{P}$. The $G_\mathfrak{P}$-action is induced by the natural action of $G_\mathfrak{P}$ on $\Delta G_\mathfrak{P} \oplus \mathbb{Z}\bar{G}_\mathfrak{P}$.

The projection on the first summand induces a short exact sequence

$$0 \longrightarrow \mathbb{Z} \longrightarrow W_\mathfrak{P} \longrightarrow \Delta G_\mathfrak{P} \longrightarrow 0$$

with $1 \mapsto w_1$, which implies $\mathbb{Q} \otimes_\mathbb{Z} W_\mathfrak{P} = \mathbb{Q}G_\mathfrak{P}$. Dualizing this sequence yields

$$0 \longrightarrow \Delta G_\mathfrak{P}^\circ \longrightarrow W_\mathfrak{P}^\circ \xrightarrow{\imath_\mathfrak{P}} \mathbb{Z} \longrightarrow 0$$

where $\imath_{\mathfrak{P}}(f) = f(w_1)$ for $f \in W_{\mathfrak{P}}^{\circ} = Hom_{\mathbb{Z}}(W_{\mathfrak{P}}, \mathbb{Z})$. For later reference we define a map $\rho_{\mathfrak{P}} \in W_{\mathfrak{P}}^{\circ}$ by

$$\rho_{\mathfrak{P}}(g) = \begin{cases} 1, & \text{if } g = 1, \\ 1 + e_{\mathfrak{P}}, & \text{if } 1 \neq g \in I_{\mathfrak{P}}, \\ e_{\mathfrak{P}}, & \text{if } g \notin I_{\mathfrak{P}}. \end{cases} \tag{4}$$

We fix a choice $*$ of G-orbit representatives in the set of all primes of N and for a G-stable subset S we write S_* for the intersection of $*$ and S. Furthermore we set

$$\begin{aligned} S^{\mathrm{ram}} &= \{\mathfrak{P} \text{ ramified in } N/K, \mathfrak{P} \notin S\}, \\ {}^{\circ}W &= {}^{\circ}W_S = \bigoplus_{\mathfrak{P} \in S_*^{\mathrm{ram}}} \mathrm{ind}_{G_{\mathfrak{P}}}^{G} W_{\mathfrak{P}}^{\circ}, \end{aligned}$$

and finally

$$\bar{\nabla} = \bar{\nabla}_S = \ker(\mathbb{Z}S \oplus {}^{\circ}W \xrightarrow{\imath'} \mathbb{Z}),$$

where $\imath'$ is the augmentation on $\mathbb{Z}S$ and $\mathrm{ind}_{G_{\mathfrak{P}}}^{G} \imath_{\mathfrak{P}}$ followed by the augmentation map $\mathrm{ind}_{G_{\mathfrak{P}}}^{G} \mathbb{Z} \longrightarrow \mathbb{Z}$ on $\mathrm{ind}_{G_{\mathfrak{P}}}^{G} W_{\mathfrak{P}}^{\circ}$ for $\mathfrak{P} \in S_*^{\mathrm{ram}}$.

The main result of [RW1] is a Tate sequence associated to S

$$0 \longrightarrow E_S \longrightarrow A \longrightarrow B \longrightarrow \nabla \longrightarrow 0$$

with A cohomologically trivial, B stably free and where ∇ originates from a unique extension

$$0 \longrightarrow \mathrm{cl}_S \longrightarrow \nabla \longrightarrow \bar{\nabla} \longrightarrow 0$$

which is explicitly described in [RW1]. Note that the torsion submodule of ∇ is the S-class group cl_S and that for a large set S we have $\nabla = \Delta S$.

We are now in position to give the definitions of the q-index and the A-number. Let $r = r_S$ be the number of G-orbits of ramified primes of N/K which are not in S, i.e., $r = |S_*^{\mathrm{ram}}|$. Then the invariants are associated to G-homomorphisms

$$\varphi : \nabla \longrightarrow \tilde{E} = E_S \oplus \mathbb{Z}G^r$$

with finite kernel and cokernel (in [RW2] such maps are called isogenies).

We fix a subfield F of $\mathbb{C}$ such that $F/\mathbb{Q}$ is finite Galois with group $\Gamma = \mathrm{Gal}(F/\mathbb{Q})$ and large enough that every representation of G can be realized over F. For a character χ of G we choose a FG-module $V = V_\chi$ affording χ and an $\mathcal{O}_F G$-lattice M such that $F \otimes_{\mathcal{O}_F} M = V$. We write $\hat{G}$ for the trace element $\sum_{g \in G} g$. Motivated by Tate's definition of the q-index we consider the composite map

$$\varphi_M : \mathrm{Hom}_{\mathcal{O}_F}(M, \nabla)_G \xrightarrow{\hat{G}} \mathrm{Hom}_{\mathcal{O}_F}(M, \nabla)^G \xrightarrow{\varphi} \mathrm{Hom}_{\mathcal{O}_F}(M, \tilde{E})^G.$$

Here and in all what follows we adopt the convention that whenever it is clear from the context any $\mathbb{Z}G$-lattice is to be replaced by the appropriate base change which makes the notations meaningful. Above this simply means that ∇ and $\tilde{E}$ have to be read as $\mathcal{O}_F \otimes_{\mathbb{Z}} \nabla$ and $\mathcal{O}_F \otimes_{\mathbb{Z}} \tilde{E}$.

Recall that for a finitely generated torsion $\mathcal{O}_F$-module X the $\mathcal{O}_F$-order ideal $\ell_{\mathcal{O}_F}(X)$ is defined as the product $\mathfrak{p}_1 \cdots \mathfrak{p}_t$ if $\mathcal{O}_F/\mathfrak{p}_1, \dots, \mathcal{O}_F/\mathfrak{p}_t$ are the composition factors of X.

Definition 2.2 [RW2]

$$q_\varphi(\chi) = \frac{\ell_{\mathcal{O}_F}(\operatorname{coker}(\varphi_M))}{\ell_{\mathcal{O}_F}(\ker(\varphi_M))}$$

For reasons of completeness we include the following

Lemma 2.3 *[RW2, Lemma 3]*

a) $q_\varphi(\chi)$ does not depend on the choices of F, V and M.

b) If χ is irreducible, then $q_\varphi(\chi)$ is a fractional $\mathcal{O}_F$-ideal which is generated by a fractional ideal of the field $\mathbb{Q}(\chi)$ of character values of χ.

c) $q_\varphi(\chi)^\gamma = q_\varphi(\chi^\gamma)$ for $\gamma \in \Gamma$.

Next we come to the definition of the generalized A-number of [RW2], which involves two main ingredients. The first one will be denoted by $c(\chi)$ and is defined to be the leading coefficient in the Taylor expansion of the Artin L-function for χ with the Euler factors at $\mathfrak{P} \in S$ removed. The second one is a generalized Stark-Tate regulator $R_\varphi(\chi)$ which we shall introduce next. We write $|\cdot|_{\mathfrak{P}}$ for the absolute values attached to places $\mathfrak{P}$ of N normalized in the usual way. Let

$$\begin{array}{rcl} \lambda : \mathbb{R} \otimes_{\mathbb{Z}} E_S & \longrightarrow & \mathbb{R} \otimes_{\mathbb{Z}} \Delta S, \\ u & \longmapsto & \sum\limits_{\mathfrak{P} \in S} \log |u|_{\mathfrak{P}} \mathfrak{P} \end{array}$$

denote the usual Dirichlet isomorphism. Our aim is to define a generalized Dirichlet map

$$\tilde{\lambda} : \mathbb{R} \otimes_{\mathbb{Z}} \tilde{E} \longrightarrow \mathbb{R} \otimes_{\mathbb{Z}} \nabla.$$

To that end let $\tilde{\lambda}$ be any $\mathbb{R}G$-homomorphism such that the diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathbb{R} \otimes_{\mathbb{Z}} E_S & \longrightarrow & \mathbb{R} \otimes_{\mathbb{Z}} \tilde{E} & \longrightarrow & \mathbb{R}G^r & \longrightarrow & 0 \\ & & \lambda \downarrow & & \tilde{\lambda} \downarrow & & \tilde{\rho} \downarrow & & \\ 0 & \longrightarrow & \mathbb{R} \otimes_{\mathbb{Z}} \Delta S & \longrightarrow & \mathbb{R} \otimes_{\mathbb{Z}} \bar{\nabla} & \longrightarrow & \mathbb{R} \otimes_{\mathbb{Z}} \mathcal{W} & \longrightarrow & 0 \end{array} \tag{5}$$

commutes. Here, for the definition of $\tilde{\rho}$, we view $\mathbb{Z}G^r$ as $\bigoplus_{\mathfrak{P} \in S_*^{\mathrm{ram}}} \operatorname{ind}_{G_{\mathfrak{P}}}^G \mathbb{Z}G_{\mathfrak{P}}$ and set $\tilde{\rho}(1_{\mathfrak{P}}) = -\log(N\mathfrak{P}) \otimes \rho_{\mathfrak{P}}$ with $\rho_{\mathfrak{P}}$ as in (4).

Let $\check{V}$ be a $\mathbb{C}G$-module affording the contragredient $\check{\chi}$ of χ and denote by $[\tilde{\lambda}\varphi \mid \mathrm{Hom}_{\mathbb{C}G}(\check{V}, \nabla)]$ the endomorphism of $\mathrm{Hom}_{\mathbb{C}G}(\check{V}, \nabla)$ which maps a homomorphism f to the composite $\tilde{\lambda} \circ \varphi \circ f$.

By [RW2, Lemma 4] the determinant of $[\tilde{\lambda}\varphi \mid \mathrm{Hom}_{\mathbb{C}G}(\check{V}, \nabla)]$ does not depend on the choice of $\tilde{\lambda}$ making diagram (5) commute.

Definition 2.4 [RW2]

$$R_\varphi(\chi) = \det[\tilde{\lambda}\varphi \mid \mathrm{Hom}_{\mathbb{C}G}(\check{V}, \nabla)]$$

Finally we define the generalized A-number of [RW2].

Definition 2.5 [RW2]

$$A_\varphi(\chi) = \frac{R_\varphi(\chi)}{c_S(\chi)\left(\prod_{\mathfrak{P}\in S_*^{\mathrm{ram}}} e_{\mathfrak{P}} \log(N\mathfrak{P})\right)^{\chi(1)}}.$$

When S is large Chinburg [Ch1] conjectured that

$$q_\varphi(\chi) = A_\varphi(\check{\chi})\mathcal{O}_F \tag{6}$$

for all characters χ of G. This was first proved by Tate [Ta2] for $\mathbb{Q}$-valued characters and by Ritter and Weiss [RW2, Theorem A] (up to certain problems with the prime 2) for extensions N/K with $N/\mathbb{Q}$ abelian and all characters χ of $G = \mathrm{Gal}(N/K)$.

In [RW2] the proof of the above conjecture is based on the following

Theorem 2.6 *[RW2, Theorem B] The ratio* $\mathfrak{a}(\chi) = \frac{A_\varphi(\check{\chi})\mathcal{O}_F}{q_\varphi(\chi)}$ *is independent of* φ *and* S.

This Theorem allows to work with small sets S; in particular we can take $S = S_\infty$.

3 Some reductions

We write $\mathfrak{a}_{N/K}(\chi)$ instead of $\mathfrak{a}(\chi)$ if we want to emphasize the dependence on N/K. The next proposition, which lists some basic properties of the ratio $\mathfrak{a}(\chi)$, is a direct consequence of work of Tate [Ta2] and Chinburg [Ch1] and Theorem 2.6.

Proposition 3.1 *[RW2, Proposition 9]*

a) $\mathfrak{a}_{N/K}$ *is additive, i.e.,* $\mathfrak{a}_{N/K}(\chi_1 + \chi_2) = \mathfrak{a}_{N/K}(\chi_1)\mathfrak{a}_{N/K}(\chi_2)$ *for all characters* χ_1, χ_2 *of* G.

b) $\mathfrak{a}_{N/K}(1) = \mathcal{O}_F$.

c) Let H *be a subgroup of* G. *Then for any character* ψ *of* H *we have*

$$\mathfrak{a}_{N/N^H}(\psi) = \mathfrak{a}_{N/K}(ind_H^G \psi).$$

d) Let H be a normal subgroup of G and $\bar{\chi}$ a character of $\bar{G} = G/H$. Then we have

$$\mathfrak{a}_{N^H/K}(\bar{\chi}) = \mathfrak{a}_{N/K}(\mathit{infl}_{\bar{G}}^{G}\bar{\chi}).$$

In practice it is in special cases possible to exhibit a G-embedding $\underline{\varphi} : \Delta S \longrightarrow E_N$ by means of explicitly known units such as the cyclotomic and elliptic units (e.g. [RW2, Section 10] or Section 5). It is therefore of great importance to give an expression for $\mathfrak{a}(\chi)$ in terms of $\underline{\varphi}$. In [RW2, Section 8] a canonical homomorphism $\varphi : \nabla \to \tilde{E}$ with finite kernel and cokernel is constructed, starting out from a given G-embedding $\underline{\varphi} : \Delta S \to E_N$. This map is then used to prove another result of Ritter and Weiss, which we will state after introducing the necessary notation.

Define $\mathcal{O}' = \mathcal{O}_F[\frac{1}{|G|}]$. For G abelian and an irreducible character χ of G we write e_χ for the χ-idempotent

$$e_\chi = \frac{1}{|G|} \sum_{g \in G} \chi(g) g^{-1} \in \mathcal{O}' G.$$

If X is a $\mathcal{O}'G$-module we let $X^\chi = e_\chi X$ denote its χ-isotypic component. Recall also that cl_S is the S-class group of N.

Proposition 3.2 *[RW2, Proposition 10] Let G be abelian and let χ be an irreducible character of G. Let $V = V_\chi$ be a $\mathbb{C}G$-module affording χ. Then*

$$\mathfrak{a}(\chi)\mathcal{O}' = \frac{\det\left(\lambda\underline{\varphi} \mid \mathrm{Hom}_{\mathbb{C}G}(V, \Delta S)\right)}{c_S(\check{\chi})} \cdot \frac{\ell_{\mathcal{O}'}(\mathrm{cl}_S^\chi)}{\ell_{\mathcal{O}'}\left(\mathit{coker}(\underline{\varphi})^\chi\right)}.$$

In the final part of this section we are concerned with certain l-adic reductions that will allow to approach Conjecture (6) prime by prime. To that end we assume that Stark's conjecture holds, so that by Lemma 2.3 $\mathfrak{a}(\chi)$ is a fractional $\mathcal{O}_F$-ideal satisfying $\mathfrak{a}(\chi)^\gamma = \mathfrak{a}(\chi^\gamma)$ for $\gamma \in \Gamma$.

We view all our number fields as subfields of a fixed algebraic closure $\bar{\mathbb{Q}}$ of the rationals. For a rational prime l denote by $\mathbb{C}_l$ a fixed completion of an algebraic closure of the l-adic rationals $\mathbb{Q}_l$ and choose once and for all an embedding $i_l : \bar{\mathbb{Q}} \to \mathbb{C}_l$. Write F_l for the completion of $i_l(F)$ in $\mathbb{C}_l$. If χ_l is a $\mathbb{C}_l$-character of G, then $\chi_l = i_l \circ \chi$ for some F-character χ and we define $\mathfrak{a}^{(l)}(\chi_l) = i_l(\mathfrak{a}(\chi))\mathcal{O}_l$, where $\mathcal{O}_l$ is the valuation ring in F_l.

Proposition 3.3 *[We, Proposition 10]*

a) $\mathfrak{a}^{(l)}$ is independent of the choice of i_l.

(b) Let N/K be abelian. Suppose that $\mathfrak{a}^{(l)}_{N'/K'}(\chi_l)$ (resp. $\mathfrak{a}^{(l)}_{N'/K'}(\chi_l)^{-1}$) is integral, whenever χ_l is a non-trivial $\mathbb{Q}_l$-irreducible character of a cyclic subextension N'/K' of N/K which has degree prime to l and so that K'/K is a cyclic l-extension. Then $\mathfrak{a}_{N/K}(\chi)$ is relatively prime to l for all χ of $G = \mathrm{Gal}(N/K)$.

Proof The proof is similar to the proof of [We, Prop. 10]. Therefore we only give a sketch of a proof, referring the reader to the details in [We].

Since $\mathfrak{a}_{N/K}$ is functorial with respect to inflation we may assume that N/K is cyclic. For any finite group H we write $R_{\mathbb{Q}_l}(H)$ for the ring of virtual $\mathbb{Q}_l$-characters.

The proof of [We, Lemma 19] shows the surjectivity of the map

$$\bigoplus_{N'/K'} R_{\mathbb{Q}_l}(\mathrm{Gal}(N'/K')) \stackrel{\mathrm{ind}\circ\mathrm{inf}}{\longrightarrow} R_{\mathbb{Q}_l}(G),$$

N'/K' as in the statement of the Proposition. By Proposition 3.1 this implies that $\mathfrak{a}_{N/K}(\psi)$ (resp. $\mathfrak{a}_{N/K}(\psi)^{-1}$) is integral for all $\mathbb{Q}_l$-irreducible characters ψ of G. The regular representation is the sum of the irreducibles. From $\mathfrak{a}_{N/K}(\mathrm{ind}_1^G 1) = (1)$ (Proposition 3.1) we therefore conclude $\mathfrak{a}_{N/K}(\psi) = (1)$ for all $\mathbb{Q}_l$-irreducible characters of G.

The rest of the proof is the same as the proof of [We, Prop.10]. $\square$

4 Elliptic units

The aim of this section is to define the elliptic units in abelian extensions of an imaginary quadratic number field k and to summarice the relevant arithmetical properties. Our main references are [Co1, Appendix], [Ru1, Appendix] and [dS, II,2].

Most of the properties that we shall need have long been known for the 12th powers. In order to deal with the 12th roots we first recall some definitions and results of [Co1, Appendix].

Let F be a field of characteristic 0 and let E be an elliptic curve defined over F. Let E'/F be another curve and let $\phi : E \longrightarrow E'$ be an isogeny of elliptic curves which is also defined over F. We shall always assume that $(|\ker(\phi)|, 6) = 1$.

We choose a generalized Weierstrass equation for E over F,

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \quad a_i \in F, \tag{7}$$

and let x_E be the x-coordinate function given by this model.

Following Coates we set

$$\zeta_\phi(P_E) = \prod_R (x_E(P_E) - x_E(R))^{-1}, \tag{8}$$

where R runs over any set of representatives of $\ker(\phi) \setminus \{0_E\}$ modulo $\{\pm 1\}$. This is a well-defined F-rational function on E, for which the following holds:

Proposition 4.1 *[Co1, Appendix, Prop.1] There exists a unique $c_E(\phi) \in F^*$ such that, for all $\beta \in \mathrm{End}_F(E)$ with $\ker(\beta) \cap \ker(\phi) = \{0_E\}$, we have*

$$\frac{\zeta_\phi(\beta(P_E))}{\prod_{R\in\ker(\beta)} \zeta_\phi(P_E +_E R)} = c_E(\phi)^{\deg(\beta)-1}.$$

Next we define a F-rational function

$$\gamma_\phi(P_E) = c_E(\phi)\zeta_\phi(P_E).$$

Note that $\gamma_\phi(P_E)$ does not depend on the choice of a generalized Weierstrass equation for E over F.

Lemma 4.2 *Suppose that F is an algebraic extension of a field k and let $\sigma \in \mathrm{Gal}(\bar{k}/k)$. Then*

$$\gamma_\phi(P_E)^\sigma = \gamma_{\phi^\sigma}(P_E^\sigma).$$

Proof By the definition of ζ_ϕ we have

$$\begin{aligned}
\zeta_\phi^\sigma(P_E^\sigma) &= \prod_{R\in(\ker(\phi)\setminus\{0\})/\{\pm 1\}} (x_E^\sigma(P_E^\sigma) - (x_E(R))^\sigma)^{-1} \\
&= \prod_{R\in(\ker(\phi)\setminus\{0\})/\{\pm 1\}} (x_E^\sigma(P_E^\sigma) - x_E^\sigma(R^\sigma))^{-1} \qquad (9)\\
&= \prod_{R\in(\ker(\phi^\sigma)\setminus\{0\})/\{\pm 1\}} (x_E^\sigma(P_E^\sigma) - (x_E^\sigma(R)))^{-1} = \zeta_{\phi^\sigma}(P_E^\sigma).
\end{aligned}$$

Next we claim that

$$c_E(\phi)^\sigma = c_{E^\sigma}(\phi^\sigma).$$

To prove the claim we have to show that for all $\beta \in \mathrm{End}_F(E)$

$$(c_E(\phi)^\sigma)^{\deg(\beta^\sigma)-1} = \frac{\zeta_{\phi^\sigma}\left(\beta^\sigma(P_E^\sigma)\right)}{\prod_{R\in\ker(\phi^\sigma)} \zeta_{\phi^\sigma}\left(P_E^\sigma +_{E^\sigma} R\right)}.$$

But this follows immediately from (9) and the defining equation for $c_E(\phi)$, since the right hand side equals

$$\left(\frac{\zeta_\phi\left(\beta(P_E)\right)}{\prod_{R\in\ker(\phi)} \zeta_\phi\left(P_E +_E R\right)}\right)^\sigma$$

The lemma is now a consequence of the claim and (9). □

Let $\lambda : E \to A$ be an isogeny of elliptic curves defined over F such that $\ker(\lambda) \cap \ker(\phi) = \{0_E\}$. To any such λ we associate a new isogeny

$$\psi : A \longrightarrow A' = A/\lambda(\ker(\phi)) \qquad (10)$$

by taking the canonical projection map (see e.g. [Sil1, Ch. III, Prop. 4.12]).

Proposition 4.3 *[Co1, Appendix, Theorem 3 and Theorem 4]*
(a) For all isogenies $\lambda : E \to A$ as above, we have

$$\gamma_\psi(\lambda(P_E)) = \prod_{R\in\ker(\lambda)} \gamma_\phi(P_E +_E R).$$

(b) For all $\beta \in \mathrm{End}_F(E)$ with $\ker(\beta) \cap \ker(\phi) = \{0_E\}$ we have

$$\gamma_\phi(\beta(P_E)) = \prod_{R \in \ker(\beta)} \gamma_\phi(P_E +_E R).$$

Corollary 4.4 *Let $\lambda : E \to A$ be an F-isogeny such that $\ker(\lambda) \cap \ker(\phi) = \{0_E\}$ and let ψ be the associated isogeny as in (10). Let $t_A = -x_A/y_A$ and $t_E = -x_E/y_E$ be local parameters at zero and write*

$$t_A(\lambda(P_E)) = \Lambda t_E + \text{ higher powers of } t_E$$

with $\Lambda \in F^*$. Then we have

$$\prod_{R \in \ker(\lambda)\setminus\{0_E\}} \gamma_\phi(R) = \frac{c_A(\psi)}{c_E(\phi)} \cdot \Lambda^{\deg(\phi)-1}.$$

Remark By [Sil1, III, Th. 4.10(c)] the isogeny λ is unramified. Therefore the element $\Lambda \in F^*$ satisfying the hypothesis of the Corollary always exists.

Proof Proposition 4.3 (a) implies

$$\begin{aligned} \prod_{R \in \ker(\lambda)\setminus\{0_E\}} \gamma_\phi(R) &= \left.\frac{\gamma_\psi(\lambda(P_E))}{\gamma_\phi(P_E)}\right|_{P_E=0_E} \\ &= \frac{c_A(\psi)}{c_E(\phi)} \cdot \left.\frac{\zeta_\psi(\lambda(P_E))}{\zeta_\phi(P_E)}\right|_{P_E=0_E}. \end{aligned}$$

If we expand ζ_ψ and ζ_ϕ in terms of the local parameters at zero we obtain

$$\begin{aligned} \zeta_\psi(P_A) &= t_A^{\deg(\psi)-1} + \text{ higher powers of } t_A, \\ \zeta_\phi(P_E) &= t_E^{\deg(\phi)-1} + \text{ higher powers of } t_E. \end{aligned}$$

Since $\ker(\lambda) \cap \ker(\phi) = \{0_E\}$, we have $\deg(\psi) = \deg(\phi)$, and thus the expansion of $\zeta_\psi(\lambda(P_E))/\zeta_\phi(P_E)$ at zero is given by

$$\frac{\zeta_\psi(\lambda(P_E))}{\zeta_\phi(P_E)} = \Lambda^{\deg(\phi)-1} + \text{ higher powers of } t_E.$$

Hence $\left.\frac{\zeta_\psi(\lambda(P_E))}{\zeta_\phi(P_E)}\right|_{P_E=0_E} = \Lambda^{\deg(\phi)-1}$ and the proof is complete. □

We shall now give an expression of the 12th powers of $c_E(\phi)$ in terms of the discriminants of E and E'. We fix a generalized Weierstrass model

$$E' : y^2 + a_1' xy + a_3' y = x^3 + a_2' x^2 + a_4' x + a_6', \quad a_i' \in F, \tag{11}$$

and let $\Delta(E')$ (resp. $\Delta(E)$) be the discriminant of this equation (resp. of (7)). Let

$$\omega_E = \frac{dx_E}{2y_E + a_1 x_E + a_3}, \quad \omega_{E'} = \frac{dx_{E'}}{2y_{E'} + a_1' x_{E'} + a_3'}$$

be the standard differentials associated with (7) and (11). Since ω_E is a F-basis of the one-dimensional space of holomorphic F-rational differentials, we may define a number $\delta(E,E') \in F^*$ by

$$\omega_{E'} \circ \phi = \delta(E,E')\omega_E.$$

Proposition 4.5 *[Co1, Appendix, Theorem 8]*

$$c_E(\phi)^{12} = \frac{\Delta(E)^{\deg(\phi)}}{\Delta(E')\delta(E,E')^{12}}.$$

In the second part of this section we shall rephrase the above results in terms of analytic functions. For that purpose we introduce a special class of elliptic curves defined over an abelian extension F of our imaginary quadratic number field k. For a detailed discussion of these curves the reader is referred to [dS, II, 1.4] or [GS].

In the following we assume that the elliptic curve E satisfies the hypothesis

$$\begin{array}{rl} (i) & E \text{ has complex multiplication by } \mathcal{O}_k, \\ (ii) & F(E_{\mathrm{tor}})/k \text{ is abelian.} \end{array} \tag{12}$$

The condition (ii) is equivalent to the existence of a Groessencharacter φ of k of type $(1,0)$ such that

$$\psi_{E/F} = \varphi \circ N_{F/k},$$

where $\psi_{E/F}$ denotes the unique Groessencharacter of F associated to E. Denoting the conductors of φ and F/k by $\mathfrak{f}_\varphi$ and $\mathfrak{f}_{F/k}$, respectively, we define an integral $\mathcal{O}_k$-ideal $\mathfrak{f} = \mathrm{lcm}(\mathfrak{f}_\varphi, \mathfrak{f}_{F/k})$. This ideal depends only on E/F and not on the choice of φ.

If $\mathfrak{a}$ is an integral ideal of k we let $w(\mathfrak{a})$ be the number of roots of unity in k congruent to 1 modulo $\mathfrak{a}$. We write $k(\mathfrak{a})$ for the ray class field of conductor $\mathfrak{a}$. If N/k is an abelian extension and $\mathfrak{a}$ an integral ideal relatively prime to $\mathfrak{f}_{N/k}$ we write $\sigma(\mathfrak{a})$ or $(\mathfrak{a}, N/k)$ for the corresponding Artin automorphism. Furthermore we denote by $E[\mathfrak{a}]$ the finite subgroup of $E(\bar{F})$ consisting of all points P which are annihilated by all elements $\alpha \in \mathfrak{a}$.

Let now $\mathfrak{a}$ be an integral $\mathcal{O}_k$-ideal with $(\mathfrak{a}, \mathfrak{f}) = 1$. By [dS, II, Proposition 1.5] there exists a unique isogeny

$$\lambda(\mathfrak{a}) : E \longrightarrow E^{\sigma(\mathfrak{a})}, \tag{13}$$

defined over F, of degree $N\mathfrak{a}$ and characterized by

$$P^{\sigma(\mathfrak{a})} = \lambda(\mathfrak{a})(P)$$

for all $P \in E[\mathfrak{c}]$, where $\mathfrak{c}$ is any integral ideal of k relatively prime to $\mathfrak{a}$.

Let $\omega = \omega_E$ be a F-rational holomorphic differential on E and define $\Lambda(\mathfrak{a}) \in F^*$ by

$$\omega^{\sigma(\mathfrak{a})} \circ \lambda(\mathfrak{a}) = \Lambda(\mathfrak{a})\omega. \tag{14}$$

Whenever E is given by a generalized Weierstrass equation we assume that Λ is associated with the standard differential.

Let $[\ ]: \mathcal{O}_k \to \mathrm{End}_F(E)$ be normalized such that $\omega \circ [\alpha] = \alpha\omega$ for all $\alpha \in \mathcal{O}_k$. We recall from [dS, II, 1.5] that if $(\mathfrak{a}, F/k) = 1$, then

$$\Lambda(\mathfrak{a}) \in k^*, \quad \lambda(\mathfrak{a}) = [\Lambda(\mathfrak{a})], \quad \Lambda(\mathfrak{a}) = \varphi(\mathfrak{a}).$$

We view all our number fields as subfields of the complex number field $\mathbb{C}$. Let L be the period lattice of ω and

$$\begin{aligned} \xi(\cdot, L) : \mathbb{C}/L &\longrightarrow E(\mathbb{C}), \\ z + L &\longmapsto \begin{cases} [0,1,0], & \text{if } z \in L, \\ \left[\wp(z) - \frac{a_1^2+4a_2}{12}, \frac{\wp'(z)-a_1\wp(z)}{2} + \frac{a_1^3+4a_1a_3-12a_3}{24}, 1\right], & \text{if } z \notin L. \end{cases} \end{aligned}$$

the corresponding analytic uniformization. Here, as usual, $\wp$ denotes the Weierstrass function associated to the complex lattice L and $\wp'$ its derivative.

For an integral ideal $\mathfrak{a}$ with $(\mathfrak{a}, \mathfrak{f}) = 1$ the period lattice of $\omega^{\sigma(\mathfrak{a})}$ on $E^{\sigma(\mathfrak{a})}$ is given by $L_{\mathfrak{a}} = \Lambda(\mathfrak{a})\mathfrak{a}^{-1}L$ and we have the commuting diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathfrak{a}^{-1}L/L & \longrightarrow & \mathbb{C}/L & \xrightarrow{\cdot\Lambda(\mathfrak{a})} & \mathbb{C}/L_{\mathfrak{a}} & \longrightarrow & 0 \\ & & \big\downarrow & & {\scriptstyle \xi(\cdot,L)}\big\downarrow & & {\scriptstyle \xi(\cdot,L_{\mathfrak{a}})}\big\downarrow & & \\ 0 & \longrightarrow & \ker\lambda(\mathfrak{a}) & \longrightarrow & E(\mathbb{C}) & \xrightarrow{\lambda(\mathfrak{a})} & E^{\sigma(\mathfrak{a})}(\mathbb{C}) & \longrightarrow & 0 \end{array} \tag{15}$$

To conclude the collection of facts about this special class of elliptic curves we finally recall

Proposition 4.6 *[dS, II, Prop. 1.6] Let $\mathfrak{g}$ be an integral $\mathcal{O}_k$ ideal such that $\mathfrak{f} \mid \mathfrak{g}$. Then $k(\mathfrak{g}) = F(E[\mathfrak{g}])$.*

We now express the elliptic units obtained from special values of the function γ_ϕ by means of complex analytic functions and derive their basic arithmetical properties. For that purpose let $\mathfrak{b}$ be an integral $\mathcal{O}_k$-ideal such that $w(\mathfrak{b}) = 1$. By [dS, II, Lemma 1.4] there exists a Groessencharacter φ of k of type $(1,0)$ and conductor $\mathfrak{b}$ and an elliptic curve E defined over $F = k(\mathfrak{b})$ satisfying (12) and such that $\psi_{E/F} = \varphi \circ N_{F/k}$. We fix a generalized Weierstrass equation for E and let L denote the period lattice associated to the standard invariant differential. Let $\mathfrak{a}$ be an integral $\mathcal{O}_k$-ideal such that $(\mathfrak{a}, 6\mathfrak{b}) = 1$ and consider the isogeny

$$\phi = \lambda(\mathfrak{a}) : E \longrightarrow E^{\sigma(\mathfrak{a})}.$$

Then, for any $z \in \mathbb{C}$, we define

$$\begin{aligned} \theta_0(z, \mathfrak{a}) &:= \gamma_\phi(\xi(z, L)) \\ &= c_E(\phi) \cdot \prod_u \frac{1}{\wp(z \mid L) - \wp(u \mid L)}, \end{aligned} \tag{16}$$

where u runs over a set of non-zero representatives of $\mathfrak{a}^{-1}L/L$ modulo $\{\pm 1\}$. The 12th power of $\theta_0(z,\mathfrak{a})$ is the function $\theta(z,L,\mathfrak{a})$ considered in [dS, II, 2.3]. Indeed, by Proposition 4.5 and the definition of $\Lambda(\mathfrak{a})$,

$$\begin{aligned}\theta_0(z,\mathfrak{a})^{12} &= \frac{\Delta(L)^{N\mathfrak{a}}}{\Delta(L_\mathfrak{a})\Lambda(\mathfrak{a})^{12}}\prod_u \frac{1}{(\wp(z \mid L)-\wp(u \mid L))^{12}}\\ &= \frac{\Delta(L)^{N\mathfrak{a}}}{\Delta(\mathfrak{a}^{-1}L)}\prod_u \frac{1}{(\wp(z \mid L)-\wp(u \mid L))^{12}},\end{aligned}$$

where now Δ also denotes the discriminant function for complex lattices (see e.g. [Sil1, VI, Prop.3.6]). Note also that $\theta_0(z,\mathfrak{a})^{12}$ can be expressed in terms of an important normalization of the Weierstrass σ-function which we shall define next. We choose a $\mathbb{Z}$-basis ω_1,ω_2 of L such that $\mathrm{Im}(\omega_1/\omega_2) > 0$ and write $\eta(\tau), \mathrm{Im}(\tau) > 0$, for the Dedekind η-function. Let η_1,η_2 denote the basic quasi-periods of the Weierstrass ζ-function and for any $z = a_1 + a_2 \in \mathbb{C}, a_1, a_2 \in \mathbb{R}$, put $z^* = a_1\eta_1 + a_2\eta_2$. Writing $\sigma\left(z\,|L\right)$ for the Weierstrass σ-function attached to the lattice L we define (see e.g. [Sch2] or [KL, page 29])

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

This function is non-meromorphic as a function of z and it is not a function of lattices but depends on the choice of a basis ω_1,ω_2. Its 12th power is often called the fundamental theta function associated to L [dS, II,2.3]

$$\theta(z,L) = \Delta(L)e^{-6zz^*}\sigma\left(z\,|L\right)^{12} = \varphi\left(z\left|\begin{matrix}\omega_1\\ \omega_2\end{matrix}\right.\right)^{12}.$$

Indeed, the 12-th power is a function of lattices and we will also write $\varphi\left(z\,|L\right)^{12}$.

The following relation between φ and θ_0 will be of great importance since certain sums of values of φ arise in the Kronecker limit formula and its applications to L-series. We have [dS, II, 2.3]

$$\theta_0(z,\mathfrak{a})^{12} = \frac{\varphi^{12N(\mathfrak{a})}(z \mid L)}{\varphi^{12}(z \mid \mathfrak{a}^{-1}L)}. \tag{17}$$

For later reference we recall some fundamental properties of the function φ.

Lemma 4.7 *(a) The function* $\varphi\left(z\left|\begin{smallmatrix}\omega_1\\ \omega_2\end{smallmatrix}\right.\right)$ *is homogeneous of degree* 0*, i.e.,* $\varphi\left(\lambda z\left|\begin{smallmatrix}\lambda\omega_1\\ \lambda\omega_2\end{smallmatrix}\right.\right) = \varphi\left(z\left|\begin{smallmatrix}\omega_1\\ \omega_2\end{smallmatrix}\right.\right)$ *for all* $\lambda \in \mathbb{C}^*$.

(b) Let L *be a complex lattice and* $z \in \mathbb{C}\setminus L$. *Let* $N \in \mathbb{N}$ *be minimal with* $Nz \in L$. *Then* φ^{12N} *does not depend on the choice of a basis of* L *and furthermore*

$$\varphi^{12N}(z+\omega \mid L) = \varphi^{12N}(z \mid L)$$

for all $\omega \in L$.

(c) Let L be a complex lattice with complex multiplication by $\mathcal{O}_k$. Let $\mathfrak{g} \neq (1)$ be an integral $\mathcal{O}_k$-ideal and let τ be a primitive $\mathfrak{g}$-torsion point of $\mathbb{C}/L$. Then

$$\varphi^{12N(\mathfrak{g})}(\tau \mid L) \in k(\mathfrak{g}).$$

(d) Let $L, \mathfrak{g}$ and τ be as in (c). Let $\mathfrak{c}$ be an integral $\mathcal{O}_k$-ideal with $(\mathfrak{g}, \mathfrak{c}) = 1$. Then

$$\varphi^{12N(\mathfrak{g})}(\tau \mid L)^{\sigma(\mathfrak{c})} = \varphi^{12N(\mathfrak{g})}(\tau \mid \mathfrak{c}^{-1}L).$$

Proof (a) This is almost immediate from the definition (see e.g. [KL, pages 27–29]).

(b) This is a consequence of [KL, page 28, K 2].

(c) The lattice L can be written in the form $L = \Omega\mathfrak{a}$ with an integral $\mathcal{O}_k$-ideal $\mathfrak{a}$ and $\Omega \in \mathbb{C}^*$. Since τ is a primitive $\mathfrak{g}$-torsion point there exists an integral $\mathcal{O}_k$-ideal $\mathfrak{b}$ such that $\mathfrak{g}\tau = \mathfrak{b}\mathfrak{a}\Omega$, $(\mathfrak{b}, \mathfrak{g}) = 1$. By (a) we derive $\varphi^{12N}(\tau \mid L) = \varphi^{12N}(1 \mid \mathfrak{g}\mathfrak{b}^{-1})$. Now (c) follows from [KL, Ch.11, Th.1.1].

(d) This is also a consequence of [KL, Ch.11, Th.1.1]. ☐

The next proposition summarizes important arithmetical properties of special values of the function θ_0. In particular, it implies that these elements can be used to construct an Euler system in the sense of [Ru2].

Proposition 4.8 *(a) Let $\mathfrak{g}$ be an integral $\mathcal{O}_k$-ideal with $\mathfrak{b} \mid \mathfrak{g}$ and let τ be a primitive $\mathfrak{g}$-torsion point of $\mathbb{C}/L$. Then $\theta_0(\tau, \mathfrak{a}) \in k(\mathfrak{g})$.*

(b) Let $\mathfrak{g}$ and τ be as in (a) and let $\mathfrak{c}$ be an integral $\mathcal{O}_k$-ideal prime to $\mathfrak{g}$. Then

$$\theta_0(\tau, \mathfrak{a})^{\sigma(\mathfrak{c})} = \gamma_{\phi^{\sigma(\mathfrak{c})}}(\xi(\Lambda(\mathfrak{c})\tau, L_{\mathfrak{c}})).$$

If, in addition, one has $(\mathfrak{c}, F/k) = 1$, then

$$\theta_0(\tau, \mathfrak{a})^{\sigma(\mathfrak{c})} = \theta_0(\Lambda(\mathfrak{c})\tau, \mathfrak{a}).$$

(c) Let $\mathfrak{g}$ and τ be as in (a). If $\mathfrak{g}$ is composite (i.e., divisible by at least two distinct prime $\mathcal{O}_k$-ideals), then $\theta_0(\tau, \mathfrak{a})$ is a unit. If $\mathfrak{g} = \mathfrak{p}^n$ is the power of a prime $\mathcal{O}_k$-ideal $\mathfrak{p}$, then

$$\theta_0(\tau, \mathfrak{a})\mathcal{O}_{k(\mathfrak{g})} = \left(\mathfrak{p}\mathcal{O}_{k(\mathfrak{g})}\right)^{(N\mathfrak{a}-1)/\Phi(\mathfrak{p}^n)},$$

where Φ is the Euler function of the ring $\mathcal{O}_k$. Thus $\theta_0(\tau, \mathfrak{a})^{\sigma-1}$ is a unit for all $\sigma \in \mathrm{Gal}(k(\mathfrak{g})/k)$.

(d) Let $\mathfrak{g}$ and τ be as in (a). Let $\mathfrak{p}$ be a prime $\mathcal{O}_k$-ideal such that $\mathfrak{p} \nmid \mathfrak{g}$. Let τ_1 be a primitive $\mathfrak{p}$-torsion point of $\mathbb{C}/L$. Then

$$N_{k(\mathfrak{p}\mathfrak{g})/k(\mathfrak{g})}\theta_0(\tau + \tau_1, \mathfrak{a}) = \theta_0(\tau, \mathfrak{a})^{\sigma(\mathfrak{p})-1}.$$

(e) Let $\mathfrak{p}, \mathfrak{g}, \tau, \tau_1$ be as in (d). Then

$$\theta_0(\tau + \tau_1, \mathfrak{a}) \equiv \theta_0(\tau, \mathfrak{a})$$

modulo all primes of $k(\mathfrak{p}\mathfrak{g})$ above $\mathfrak{p}$.

Proof

(a) Since γ_ϕ is defined over F, the special value $\theta_0(\tau,\mathfrak{a}) = \gamma_\phi(\xi(\tau,L))$ is contained in $F(E[\mathfrak{g}])$, which equals $k(\mathfrak{g})$ by Proposition 4.6.

(b) The first assertion is an immediate consequence of Lemma 4.2 and the commutative diagram (15). Indeed, writing $\sigma = \sigma(\mathfrak{c})$ we have

$$\begin{aligned} \theta_0(\tau,\mathfrak{a})^\sigma &= \gamma_\phi(\xi(\tau,L))^\sigma \\ &= \gamma_\phi^\sigma\,(\xi(\tau,L)^\sigma) \\ &= \gamma_{\phi^\sigma}\,(\xi(\Lambda(\mathfrak{c})\tau, L_\mathfrak{c}))\,. \end{aligned}$$

The second statement follows then from $\phi^\sigma = \phi$ and $L_\mathfrak{c} = L$.

(c) The prime factorization of special values of $\varphi\,(z\,|L)^{12}$ is originally due to Ramachandra [Ra]. The assertion in (c) follows immediately from (17) and [Sch1, Satz 3].

(d) By class field theory and part (b) we obtain

$$N_{k(\mathfrak{p}\mathfrak{g})/k(\mathfrak{g})}\theta_0(\tau+\tau_1,\mathfrak{a}) = \prod_\alpha \theta_0(\tau+\tau_1,\mathfrak{a})^{\sigma(\alpha)} = \prod_\alpha \theta_0(\alpha\tau+\alpha\tau_1,\mathfrak{a}),$$

where α runs through a set of representatives of $(\mathcal{O}_k/\mathfrak{p}\mathfrak{g})^*$ with $\alpha \equiv 1 \pmod{\mathfrak{g}}$. Thus

$$\begin{aligned} N_{k(\mathfrak{p}\mathfrak{g})/k(\mathfrak{g})}\theta_0(\tau+\tau_1,\mathfrak{a}) &= \prod_{\beta\in\mathfrak{p}^{-1}L/L,\beta\not\equiv 0} \theta_0(\tau+\beta,\mathfrak{a}) \\ &= \frac{\prod_{\beta\in\mathfrak{p}^{-1}L/L}\gamma_\phi(\xi(\tau+\beta,L))}{\gamma_\phi(\xi(\tau,L))}. \end{aligned}$$

We now apply Proposition 4.3(a) for the isogeny

$$\lambda = \lambda(\mathfrak{p}) : E \longrightarrow E^{\sigma(\mathfrak{p})}.$$

Note that we can take $\phi^{\sigma(\mathfrak{p})}$ for the associated isogeny $\psi : E^{\sigma(\mathfrak{p})} \to E^{\sigma(\mathfrak{p})}/\lambda(\ker(\phi))$. Hence we find

$$\begin{aligned} N_{k(\mathfrak{p}\mathfrak{g})/k(\mathfrak{g})}\theta_0(\tau+\tau_1,\mathfrak{a}) &= \frac{\gamma_{\phi^{\sigma(\mathfrak{p})}}(\xi(\Lambda(\mathfrak{p})\tau,L_\mathfrak{p}))}{\gamma_\phi(\xi(\tau,L))} \\ &\overset{(b)}{=} \theta_0(\tau,\mathfrak{a})^{\sigma(\mathfrak{p})-1}. \end{aligned}$$

(e) Since $\theta_0(\tau+\tau_1,\mathfrak{a})$ is a unit it suffices to show that $\theta_0(\tau,\mathfrak{a})/\theta_0(\tau+\tau_1,\mathfrak{a}) \equiv 1$. Using the equality [La1, Ch.18, §1, Th.2]

$$\wp\,(z_1\,|L) - \wp\,(z_2\,|L) = -\frac{\sigma\,(z_1+z_2\,|L)\,\sigma\,(z_1-z_2\,|L)}{\sigma^2(z_1\mid L)\sigma^2(z_2\mid L)}, z_1,z_2\in\mathbb{C},$$

we obtain

$$\frac{\wp(\tau+\tau_1)-\wp(\tau)}{\wp(\tau)-\wp(u)} = \frac{\varphi(2\tau+\tau_1)\varphi(\tau_1)\varphi(u)^2}{\varphi^2(\tau+\tau_1)\varphi(\tau+u)\varphi(\tau-u)}, \tag{18}$$

where we omit the lattice L in our notation. From the definition (16) of θ_0 we derive

$$\begin{aligned} \frac{\theta_0(\tau, \mathfrak{a})}{\theta_0(\tau+\tau_1, \mathfrak{a})} &= \prod_u \frac{\wp(\tau+\tau_1)-\wp(u)}{\wp(\tau)-\wp(u)} \\ &= \prod_u \left(1 + \frac{\wp(\tau+\tau_1)-\wp(\tau)}{\wp(\tau)-\wp(u)}\right) \end{aligned}$$

By (18) and [Sch1, Satz 3] each of the factors is congruent 1 modulo all primes above $\mathfrak{p}$. This concludes the proof. □

5 The Ramachandra unit lattice

Let k be an imaginary quadratic number field and let N be an abelian extension of k. Our ultimate goal is to prove Conjecture (6) (or at least some approximation to it) for all abelian extensions N/k and all characters χ of $\mathrm{Gal}(N/k)$. By Proposition 3.1 we may assume firstly, that N/k is cyclic, and secondly, that χ is a faithful linear character of $\mathrm{Gal}(N/k)$. Moreover, Stark's conjecture holds for abelian extensions of an imaginary quadratic number field and we can therefore apply the results of Proposition 3.3.

Fix a rational prime l. The idea is to prove (6) prime by prime by applying Proposition 3.3(b). Thus it suffices to consider the following situation

$$\begin{tikzcd} & N \arrow[dl, dash, "l'"'] \arrow[dr, dash, "l^t"] & \\ K \arrow[dr, dash, "l^t"'] & & K_0 \arrow[dl, dash, "l'"] \\ & k & \end{tikzcd} \tag{19}$$

where $G = \mathrm{Gal}(N/K)$ has order l' prime to l and $[K:k] = l^t$ with $t \geq 0$. We also write H for the group $\mathrm{Gal}(N/k)$.

Let $\mathfrak{f}$ be any multiple of the conductor $\mathfrak{f}_{N/k}$ of N. Write

$$\mathfrak{f} = \prod_{i=1}^{s} \mathfrak{p}_i^{e_i}$$

and assume that $\Phi(\mathfrak{p}^{e_i}) > 2$ for $i = 1, \ldots, s$. We choose an $\mathcal{O}_k$-prime ideal $\mathfrak{b}$ such that

$$\begin{aligned} &w(\mathfrak{b}) = 1, \quad (\mathfrak{b}, 6\mathfrak{f}) = 1, \\ &\psi(\sigma(\mathfrak{b})) \neq 1 \text{ for all non-trivial linear characters } \psi \text{ of } H. \end{aligned} \tag{20}$$

Since N/k is cyclic, there are infinitely many primes $\mathfrak{b}$ satisfying (20) by the Chebotarev density theorem.

Let $\mathfrak{a}$ be another auxiliary integral $\mathcal{O}_k$-ideal such that $(\mathfrak{a}, 6\mathfrak{b}\mathfrak{f}) = 1$. Let φ be a Groessencharacter of k of type $(1,0)$ and of conductor $\mathfrak{b}$ and let E be an elliptic curve defined over $F = k(\mathfrak{b})$ satisfying (12) and such that $\psi_{E/F} = \varphi \circ N_{K/k}$. Fix a Weierstrass model for E and a period lattice L associated to the standard invariant differential. If necessary we replace E by one of its conjugates so that we can assume without loss of generality that $L = \Omega\mathcal{O}_k$ with $\Omega \in \mathbb{C}^*$. Recall also the definition of the function $\theta_0(z, \mathfrak{a})$ in (16).

Motivated by the cyclotomic case (see e.g. [Wa, page 147]) we write $\mathfrak{n}_I = \prod_{i \in I} \mathfrak{p}_i^{e_i}$ for each subset I of $\{1, \dots, s\}$. We fix a primitive $\mathfrak{b}$-torsion point τ of $\mathbb{C}/L$ and for each $j \in \{1, \dots, s\}$ a primitive $\mathfrak{p}_j^{e_j}$-torsion point τ_j. Finally, for a subset $J \subseteq \{1, \dots, s\}$ we set $\tau_J = \tau + \sum_{j \in J} \tau_j$ and

$$\theta_J = \theta_0(\tau_J, \mathfrak{a}).$$

From Proposition 4.8(a) we deduce $\theta_0(\tau_J, \mathfrak{a}) \in k(\mathfrak{b}\mathfrak{n}_J)$.

Definition 5.1

$$\theta_N = N_{k(\mathfrak{f}\mathfrak{b})/N}\left(\prod_{J \subseteq \{1,\dots,s\}} \theta_0(\tau_J, \mathfrak{a})\right).$$

Note that in contrast to the cyclotomic case (see [RW2, §10]) it is here necessary to include the set $J = \emptyset$ in order to include the so-called unramified units.

Henceforth we assume that $S = S_\infty$. As before we view all our number fields as subfields of $\mathbb{C}$. This defines an archemedian place $\mathfrak{p}_\infty$ of S and for all $\alpha \in N^*$ we have $|\alpha|_{\mathfrak{p}_\infty} = |\alpha|^2$ with $|\cdot|$ denoting the usual complex value. Note that $\mathbb{Z}S = \mathbb{Z}H\mathfrak{p}_\infty$. Hence there is a unique H-homomorphism $\mathbb{Z}S \to N^*$ mapping $\mathfrak{p}_\infty$ to θ_N. By Proposition 4.8(c) this homomorphism restricts to a map

$$\underline{\varphi} : \Delta S \longrightarrow E_N, \quad (h-1)\mathfrak{p}_\infty \longmapsto \theta_N^{h-1}, \quad h \in H. \tag{21}$$

Actually, we should now proof that $\mathrm{im}(\underline{\varphi})$ is a unit lattice of full rank. However, this will follow immediately from the expression we shall compute for $\det(\lambda\underline{\varphi} \mid \mathrm{Hom}_{\mathbb{C}G}(V, \Delta S))/c_S(\check{\chi})$ (see Proposition 5.3), where χ is any non-trivial linear character of G.

Definition 5.2 For any non-trivial linear character ψ of H we set

$$g(\psi) = \prod_{\mathfrak{p}_i \mid \mathfrak{f}, \mathfrak{p}_i \nmid \mathfrak{f}_\psi} \left(\Phi(\mathfrak{p}_i^{e_i}) + \psi(\mathfrak{p}_i)^{e_i - 1}(\psi(\mathfrak{p}_i) - 1)\right),$$

where ψ is interpreted as a Dirichlet character via the Artin map.

By our choice of $\mathfrak{f}$ we obtain $g(\psi) \neq 0$ for all non-trivial linear characters ψ of H.

Proposition 5.3 *Let χ be a non-trivial linear character of G with representation space V. Then*

$$\frac{\det(\lambda\underline{\varphi} \mid \mathrm{Hom}_{\mathbb{C}G}(V, \Delta S))}{c_S(\check{\chi})} = \zeta_\chi \prod_{\psi|\chi} (-g(\psi)(\psi(\mathfrak{b}) - 1)(N(\mathfrak{a}) - \psi(\mathfrak{a}))) ,$$

where ψ runs through all characters of H extending χ and ζ_χ is a root of unity.

The proof of Proposition 5.3 will occupy the rest of this section. We start by computing $\det(\lambda\underline{\varphi} \mid \mathrm{Hom}_{\mathbb{C}G}(V, \Delta_S))$. We take $V = \mathbb{C}Ge_\chi$ and derive

$$\begin{aligned} \mathrm{Hom}_{\mathbb{C}G}(V, \Delta S) &\simeq e_\chi \mathbb{C}S = \sum_{\psi|\chi} e_\psi \mathbb{C}S \\ &= \sum_{\psi|\chi} e_\psi \mathbb{C}H\mathfrak{p} = \sum_{\psi|\chi} e_\psi \mathbb{C}\mathfrak{p}_\infty . \end{aligned}$$

Thus the set $\{e_\psi \mathfrak{p}_\infty \mid \psi \text{ extends } \chi\}$ can be viewed as a $\mathbb{C}$-basis of $\mathrm{Hom}_{\mathbb{C}G}(V, \Delta S)$. Computing the matrix representation of $\lambda\underline{\varphi}$ with respect to this basis we obtain

$$\begin{aligned} \lambda\underline{\varphi}(e_\psi\mathfrak{p}_\infty) &= \lambda\underline{\varphi}\left(\frac{1}{|H|}\sum_{h\in H}\psi(h^{-1})(h\mathfrak{p}_\infty - \mathfrak{p}_\infty)\right), \quad \text{since } \psi \neq 1 \\ &= \lambda\left(\frac{1}{|H|}\sum_{h\in H}\psi(h^{-1})\theta_N^{h^{-1}}\right) \\ &= \frac{1}{|H|}\sum_{h\in H}\psi(h^{-1})\sum_{h'\in H}\log|\theta_N^{h^{-1}}|_{h'\cdot\mathfrak{p}_\infty} h'\cdot\mathfrak{p}_\infty \\ &= \frac{1}{|H|}\sum_{h\in H}\psi(h^{-1})\sum_{h'\in H}\log|\theta_N^{(h-1)h'^{-1}}|_{\mathfrak{p}_\infty} h'\cdot\mathfrak{p}_\infty \\ &= \frac{1}{|H|}\sum_{h\in H}\psi(h^{-1})\sum_{h'\in H}\log|\theta_N^{hh'^{-1}}|_{\mathfrak{p}_\infty} h'\cdot\mathfrak{p}_\infty, \text{ since } \psi \neq 1 \\ &= \frac{1}{|H|}\sum_{h'\in H}\sum_{l\in H}\psi(h'^{-1}l^{-1})\log|\theta_N^{l}|_{\mathfrak{p}_\infty} h'\cdot\mathfrak{p}_\infty, \quad l = hh'^{-1} \\ &= \left(\sum_{h\in H}\psi(h^{-1})\log|\theta_N^{h}|_{\mathfrak{p}_\infty}\right) e_\psi\mathfrak{p}_\infty . \end{aligned}$$

Therefore $\lambda\underline{\varphi}$ is represented by a diagonal matrix with determinant

$$\det(\lambda\underline{\varphi} \mid \mathrm{Hom}_{\mathbb{C}G}(V, \Delta S)) = \prod_{\psi|\chi} 2\sum_{h\in H}\psi(h^{-1})\log|\theta_N^h|. \tag{22}$$

We will express the sums $\sum_{h\in H}\psi(h^{-1}\log|\theta_N^h|$ in terms of the Dirichlet L-series $L(s,\psi)$ at $s = 1$. By the definition of θ_N we obtain

$$\sum_{h\in H}\psi(h^{-1})\log|\theta_N^h| = \sum_{g\in\mathrm{Gal}(k(\mathfrak{f}\mathfrak{b})/k)}\psi(g^{-1})\sum_{J\subseteq\{1,\dots,s\}}\log|\theta_0(\tau_J,\mathfrak{a})|, \tag{23}$$

where we view ψ as a character of $\mathrm{Gal}(k(\mathfrak{f}\mathfrak{b})/k)$ by inflation. By (17) the above expression is equal to

$$\frac{1}{12}\sum_{g\in\mathrm{Gal}(k(\mathfrak{f}\mathfrak{b})/k)}\psi(g^{-1})\sum_{J\subseteq\{1,\dots,s\}}\log\left|\left(\frac{\varphi^{12N(\mathfrak{a})}(\tau_J\mid L)}{\varphi^{12}(\tau_J\mid\mathfrak{a}^{-1}L)}\right)^g\right|. \tag{24}$$

Since $\varphi^{12N(\mathfrak{n}_J\mathfrak{b})}(\tau_J\mid\mathfrak{a}^{-1}L)=\varphi^{12N(\mathfrak{n}_J\mathfrak{b})}(\tau_J\mid L)^{\sigma(\mathfrak{a})}$ by Lemma 4.7(d) the expression (24) becomes

$$\frac{N(\mathfrak{a})-\psi(\mathfrak{a})}{12}\sum_{J\subseteq\{1,\dots,s\}}\frac{1}{N(\mathfrak{n}_J\mathfrak{b})}\times$$
$$\sum_{g\in\mathrm{Gal}(k(\mathfrak{f}\mathfrak{b})/k)}\psi(g^{-1})\log\left|\left(\varphi^{12N(\mathfrak{b}\mathfrak{n}_J)}(\tau_J\mid L)\right)^g\right|. \tag{25}$$

Since τ_J is a primitive $\mathfrak{n}_J\mathfrak{b}$-torsion point of $\mathbb{C}/L$, there exists an integral $\mathcal{O}_k$-ideal $\mathfrak{c}_J$ such that

$$\mathfrak{n}_J\mathfrak{b}\tau_J=\mathfrak{c}_J\Omega,\quad(\mathfrak{c}_J,\mathfrak{n}_J\mathfrak{b})=1.$$

By Lemma 4.7(a) and (d) we derive

$$\begin{aligned}\varphi^{12N(\mathfrak{n}_J\mathfrak{b})}(\tau_J\mid L)&=\varphi^{12N(\mathfrak{n}_J\mathfrak{b})}(1\mid\mathfrak{n}_J\mathfrak{b}\mathfrak{c}_J^{-1})\\&=\varphi^{12N(\mathfrak{n}_J\mathfrak{b})}(1\mid\mathfrak{n}_J\mathfrak{b})^{\sigma(\mathfrak{c}_J)}.\end{aligned}$$

Therefore the expression in (25) becomes

$$\frac{N(\mathfrak{a})-\psi(\mathfrak{a})}{12}\sum_{J\subseteq\{1,\dots,s\}}\frac{\psi(\mathfrak{c}_J)}{N(\mathfrak{n}_J\mathfrak{b})}\times$$
$$\sum_{g\in\mathrm{Gal}(k(\mathfrak{f}\mathfrak{b})/k)}\psi(g^{-1})\log\left|\left(\varphi^{12N(\mathfrak{n}_J\mathfrak{b})}(1\mid\mathfrak{n}_J\mathfrak{b})\right)^g\right|. \tag{26}$$

Following [Ro] we define for integral $\mathcal{O}_k$-ideals $\mathfrak{g},\mathfrak{g}_1$ with $\mathfrak{g}\mid\mathfrak{g}_1$ and each abelian character ψ of $\mathrm{Gal}(k(\mathfrak{g})/k)$

$$S_{\mathfrak{g}}(\psi,\mathfrak{g}_1)=\sum_{C\in\mathrm{cl}(\mathfrak{g}_1)}\psi(C^{-1})\log|\varphi_{\mathfrak{g}}(C)|, \tag{27}$$

where $\mathrm{cl}(\mathfrak{g}_1)$ denotes the ray class group modulo $\mathfrak{g}_1$ and ψ is viewed as a character of $\mathrm{cl}(\mathfrak{g}_1)$ by inflation. For the definition of the invariant $\varphi_{\mathfrak{g}}(C)$ we choose an integral ideal $\mathfrak{c}$ in the class C and set

$$\varphi_{\mathfrak{g}}(C)=\begin{cases}\varphi^{12N(\mathfrak{g})}(1\mid\mathfrak{g}\mathfrak{c}^{-1}), & \text{if } \mathfrak{g}\neq(1),\\ \left|\frac{N(\mathfrak{c}^{-1})^6\Delta(\mathfrak{c}^{-1})}{(2\pi)^{12}}\right|, & \text{if } \mathfrak{g}=(1).\end{cases}$$

Note that this definition does not depend on the choice of $\mathfrak{c}\in C$ ([Ro, pp. 15/16]).

By Lemma 4.7(d) and (26) we can therefore write

$$\begin{aligned}&\sum_{h\in H}\psi(h^{-1})\log|\theta_N^h|\\ =\ &\frac{N(\mathfrak{a})-\psi(\mathfrak{a})}{12}\sum_{J\subseteq\{1,\ldots,s\}}\frac{\psi(\mathfrak{c}_J)}{N(\mathfrak{n}_J\mathfrak{b})}S_{\mathfrak{n}_J\mathfrak{b}}(\psi,\mathfrak{f}\mathfrak{b}).\end{aligned}$$

Lemma 5.4 *[Wa, §8, Lemma 8.4] If* $\mathfrak{f}_\psi\nmid\mathfrak{n}_J\mathfrak{b}$, *then* $S_{\mathfrak{n}_J\mathfrak{b}}(\psi,\mathfrak{f}\mathfrak{b})=0$.

Lemma 5.5 *[Wa, §8, Lemma 8.5] If* $\mathfrak{f}_\psi\mid\mathfrak{n}_J\mathfrak{b}$, *then*

$$S_{\mathfrak{n}_J\mathfrak{b}}(\psi,\mathfrak{f}\mathfrak{b})=\Phi(\mathfrak{n}_I)S_{\mathfrak{n}_J\mathfrak{b}}(\psi,\mathfrak{n}_J\mathfrak{b}),$$

where $I=\{1,\ldots,s\}$.

Proofs The proofs are analogous to the proofs of [Wa, §8, Lemma 8.4 and 8.5] using the fact that $\varphi^{12N(\mathfrak{n}_J\mathfrak{b})}(1\mid\mathfrak{n}_J\mathfrak{b})\in k(\mathfrak{n}_J\mathfrak{b})$ by Lemma 4.7(c). □

By the above Lemmas we obtain

$$\begin{aligned}&\sum_{h\in H}\psi(h^{-1})\log|\theta_N^h|\\ =\ &\frac{N(\mathfrak{a})-\psi(\mathfrak{a})}{12}\sum_{\substack{J,\,\mathfrak{f}_\psi\mid\mathfrak{n}_J\\ I=\{1,\ldots,s\}\setminus J}}\frac{\psi(\mathfrak{c}_J)}{N(\mathfrak{n}_J\mathfrak{b})}\Phi(\mathfrak{n}_I)S_{\mathfrak{n}_J\mathfrak{b}}(\psi,\mathfrak{n}_J\mathfrak{b}).\end{aligned}\tag{28}$$

Lemma 5.6 *[Ro, Corollaire 2] If* $\mathfrak{f}_\psi\mid\mathfrak{n}_J\mathfrak{b}$, *then*

$$S_{\mathfrak{n}_J\mathfrak{b}}(\psi,\mathfrak{n}_J\mathfrak{b})=\frac{N(\mathfrak{n}_J\mathfrak{b})w(\mathfrak{n}_J\mathfrak{b})}{N(\mathfrak{f}_\psi)w(\mathfrak{f}_\psi)}(1-\psi(\mathfrak{b})^{-1})\left(\prod_{\substack{j\in J\\ \mathfrak{p}_j\nmid\mathfrak{f}_\psi}}(1-\psi(\mathfrak{p}_j)^{-1})\right)S_{\mathfrak{f}_\psi}(\psi,\mathfrak{f}_\psi).$$

Substituting the equality of Lemma 5.6 into (28) we have

$$\begin{aligned}&\sum_{h\in H}\psi(h^{-1})\log|\theta_N^h|\\ =\ &\frac{N(\mathfrak{a})-\psi(\mathfrak{a})}{12N(\mathfrak{f}_\psi)w(\mathfrak{f}_\psi)}\sum_{\substack{J,\,\mathfrak{f}_\psi\mid\mathfrak{n}_J\\ I=\{1,\ldots,s\}\setminus J}}\left[\psi(\mathfrak{c}_J)\prod_{\substack{j\in J\\ \mathfrak{p}_j\nmid\mathfrak{f}_\psi}}\psi(\mathfrak{p})^{-e_j}\right](1-\psi(\mathfrak{b})^{-1})\times\\ &\Phi(\mathfrak{n}_I)\left(\prod_{\substack{j\in J\\ \mathfrak{p}_j\nmid\mathfrak{f}_\psi}}\psi(\mathfrak{p})^{e_j-1}(\psi(\mathfrak{p}_j)-1)\right)S_{\mathfrak{f}_\psi}(\psi,\mathfrak{f}_\psi).\end{aligned}\tag{29}$$

Lemma 5.7 *The value*

$$\zeta_\psi = \psi(\mathfrak{c}_J) \prod_{\substack{j \in J \\ \mathfrak{p}_j \nmid \mathfrak{f}_\psi}} \psi(\mathfrak{p}_j)^{-e_j}$$

does not depend on J as long as $\mathfrak{f}_\psi \mid \mathfrak{n}_J$.

Proof Let $J_1 \subseteq \{1, \ldots, s\}$ be minimal with $\mathfrak{f}_\psi \mid \mathfrak{n}_J$. Then $\tau_J = \tau_{J_1} + \nu$ with a torsion point ν of order prime to $\mathfrak{f}_\psi$.From the definition of $\mathfrak{c}_J$ and $\mathfrak{c}_{J_1}$ we derive

$$\begin{aligned} \psi(\mathfrak{c}_J) \prod_{\substack{j \in J \\ \mathfrak{p}_j \nmid \mathfrak{f}_\psi}} \psi(\mathfrak{p}_j)^{-e_j} &= \psi(\frac{\tau_J}{\Omega}\mathfrak{b} \prod_{\mathfrak{p}_j \mid \mathfrak{f}_\psi} \mathfrak{p}_j^{e_j}), \\ \psi(\mathfrak{c}_{J_1}) \prod_{\substack{j \in J_1 \\ \mathfrak{p}_j \nmid \mathfrak{f}_\psi}} \psi(\mathfrak{p}_j)^{-e_j} &= \psi(\frac{\tau_{J_1}}{\Omega}\mathfrak{b} \prod_{\mathfrak{p}_j \mid \mathfrak{f}_\psi} \mathfrak{p}_j^{e_j}). \end{aligned}$$

Hence it suffices to show that τ_J/τ_{J_1} belongs to the principle ray class modulo $\mathfrak{f}_\psi$. But this follows from $\frac{\tau_J}{\tau_{J_1}} - 1 = \frac{\nu}{\tau_{J_1}}$, since ν has order prime to $\mathfrak{f}_\psi$. □

Lemma 5.8

$$\sum_{\substack{J, \mathfrak{f}_\psi \mid \mathfrak{n}_J \mathfrak{b} \\ I = \{1, \ldots, s\} \setminus J}} \Phi(\mathfrak{n}_I) \prod_{\substack{j \in J \\ \mathfrak{p}_j \nmid \mathfrak{f}_\psi}} \psi(\mathfrak{p}_j)^{e_j - 1}(\psi(\mathfrak{p}_j) - 1) = g(\psi).$$

Proof For fixed ψ let $K = \{i \in \{1, \ldots, s\} \mid \mathfrak{p}_i \nmid \mathfrak{f}_\psi\}$. By expanding the product for $g(\psi)$ given in Definition 5.2 we find

$$g(\psi) = \sum_{I \in K} \Phi(\mathfrak{n}_I) \prod_{j \in K \setminus I} \psi(\mathfrak{p}_j)^{e_j - 1}(\psi(\mathfrak{p}_j) - 1).$$

A subset $I \subseteq \{1, \ldots, s\}$ occurs in the sum if and only if $\mathfrak{f}_\psi \mid \mathfrak{n}_J \mathfrak{b}$ with $J = \{1, \ldots, s\} \setminus I$. Thus the Lemma follows easily from

$$j \in J \text{ and } \mathfrak{p}_j \nmid \mathfrak{f}_\psi \iff j \in K \setminus I.$$

□

Applying the results of Lemma 5.7 and 5.8 to the expression in (29) we get

$$\begin{aligned} & \sum_{h \in H} \psi(h^{-1}) \log |\theta_N^h| \\ = \; & \frac{N(\mathfrak{a}) - \psi(\mathfrak{a})}{12 N(\mathfrak{f}_\psi) w(\mathfrak{f}_\psi)} \zeta_\psi (1 - \psi(\mathfrak{b})^{-1}) g(\psi) S_{\mathfrak{f}_\psi}(\psi, \mathfrak{f}_\psi). \end{aligned} \tag{30}$$

Our next aim is to compute $c_S(\check{\chi})$ in terms of the $S_{\mathfrak{f}_\psi}(\psi, \mathfrak{f}_\psi)$ with ψ extending χ. By the formal properties of Artin L-series [Ta2, Ch.0, 4.2] we have

$$L(s, \chi) = L(s, \mathrm{ind}_G^H \chi) = \prod_{\psi \mid \chi} L(s, \psi).$$

Since ψ is abelian and $S = S_\infty$ the Artin L-function $L(s,\psi)$ is equal to the primitive Dirichlet L-function attached to ψ

In the following we write d_k for the discriminant of $k/\mathbb{Q}$, $\mathfrak{d}_k$ for the different ideal and Tr for the trace from k to $\mathbb{Q}$.

Definition 5.9 [Ro, 2.4] Let $\mathfrak{g}$ be an integral $\mathcal{O}_k$-ideal and ψ a character of $\mathrm{cl}(\mathfrak{g})$. Let γ be an element of k^* such that $\gamma\mathfrak{d}_k\mathfrak{g}$ is integral and prime to $\mathfrak{g}$. Then we define a Gauss sum $\tau(\psi,\mathfrak{g})$ by

$$\tau(\psi,\mathfrak{g}) = \sum_{\lambda\in\mathcal{O}_k/\mathfrak{g}} \bar{\psi}(\lambda\gamma\mathfrak{d}_k\mathfrak{g})e^{2\pi i \mathrm{Tr}(\lambda\gamma)}.$$

If ψ is primitive, we simply write $\tau(\psi)$.

Note that $\tau(\psi,\mathfrak{g})$ does not depend on the choice of γ.

By [Ro, Théorème 3] the values $L(1,\psi)$ and $S_{\mathfrak{f}_\psi}(\psi,\mathfrak{f}_\psi)$ are closely related, namely

$$L(1,\psi) = -\frac{2\pi}{6N(\mathfrak{f}_\psi)w(\mathfrak{f}_\psi)\tau(\psi)\sqrt{|d_k|}}S_{\mathfrak{f}_\psi}(\psi,\mathfrak{f}_\psi). \tag{31}$$

We will now use the functional equation for $L(s,\psi)$ to compute the value $c_S(\check{\psi})$. The completed Artin L-function is given by

$$\Lambda(s,\psi) = \frac{(|d_k|N(\mathfrak{f}_\psi))^{s/2}\cdot 2}{(2\pi)^s}\Gamma(s)L(s,\psi)$$

(see e.g. [Ta2, Ch.0, §6]). The function $\Lambda(s,\psi)$ satisfies the functional equation

$$\Lambda(1-s,\psi) = W(\psi)\Lambda(s,\check{\psi}) \tag{32}$$

with the Artin root number $W(\psi)$. Computing the limit for $s\to 0$ on both sides of (32) we obtain

$$|d_k|^{1/2}N(\mathfrak{f}_\psi)^{1/2}\pi^{-1}L(1,\psi) = 2W(\psi)c_S(\check{\psi}),$$

since $L(s,\psi)$ has a zero of order 1 at $s=0$, $\Gamma(1)=1$ and $\lim_{s\to 0} s\Gamma(s) = 1$.

Together with (31) and $W(\psi) = N(\mathfrak{f}_\psi)^{1/2}/\tau(\psi)$ ([Ta2, page 19]) this implies

$$c_S(\check{\psi}) = -\frac{S_{\mathfrak{f}_\psi}(\psi,\mathfrak{f}_\psi)}{6N(\mathfrak{f}_\psi)w(\mathfrak{f}_\psi)}. \tag{33}$$

Now, from (22), (30) and (33), we derive

$$\frac{\det(\lambda\underline{\varphi}\mid \mathrm{Hom}_{\mathbb{C}G}(V,\Delta S))}{c_S(\check{\chi})} = \prod_{\psi|\chi}\left(-(N(\mathfrak{a})-\psi(\mathfrak{a}))(\psi(\mathfrak{b})-1)g(\psi)\zeta_\psi\right),$$

which concludes the proof of Proposition 5.3.

6 A unit lattice à la Hasse

In this section we will define another G-stable unit group, denoted by $\mathcal{C}_{\mathrm{Ha}}$, and compute the index of $\mathrm{im}(\underline{\varphi})^\chi$ in ${\mathcal{C}_{\mathrm{Ha}}}^\chi$ for each abelian faithful character χ of G.

Recall the situation and notation summarized at the beginning of Section 5. In addition, let σ be a generator of $G = \mathrm{Gal}(N/K)$.

For each abelian character ϕ of $\mathrm{Gal}(N/K_0)$ we denote by $\mathbb{Q}(\phi)$ the field of character values of ϕ. We define the division of ϕ by

$$[\phi] := \{\phi^g \mid g \in \mathrm{Gal}(\mathbb{Q}(\phi)/\mathbb{Q})\},$$

thus dividing the group $\widehat{\mathrm{Gal}}(N/K_0)$ of abelian characters of $\mathrm{Gal}(N/K_0)$ into equivalence classes. Obviously this equivalence relation does not depend on the choice of ϕ within a class.

In the sequel we write

$$\mathrm{Gal}(N/K_0) =<\rho> \text{ with } \rho^{l^t} = 1$$

and define a generator ϕ_0 of $\widehat{\mathrm{Gal}}(N/K_0)$ by

$$\phi_0(\rho) = \zeta_{l^t},$$

where ζ_{l^t} is a fixed primitive l^t-th root of unity. Then the divisions of $\widehat{\mathrm{Gal}}(N/K_0)$ are given by

$$D_i = [\phi_0^{l^{t-i}}] = \{\phi_0^{l^{t-i}j} \mid j = 1, \dots, l^i, (j,l) = 1\}, \quad i = 0, \dots, t,$$

and we easily compute

$$|D_i| = \begin{cases} l^{i-1}(l-1), & \text{if } 1 \le i \le t, \\ 1, & \text{if } i = 0. \end{cases}$$

In the following let χ be a linear faithful character of G. The characters ψ of H extending χ are given by $\chi\phi$, $\phi \in \widehat{\mathrm{Gal}}(N/K_0)$. We set

$$\ker(D_i) = \ker(\phi), \quad \mathfrak{f}_i = \mathfrak{f}_{\chi\phi}, \quad N_i = N^{\ker(D_i)}$$

for any $\phi \in D_i$, $i = 0, \dots, t$, and note again that these definitions do not depend on the choice of $\phi \in D_i$. Moreover we have $\mathfrak{f}_{N_i} = \mathfrak{f}_i$. Finally we fix a primitive $\mathfrak{f}_i\mathfrak{b}$-torsion point ν_i of $\mathbb{C}/L$ for each $i \in \{0, \dots, t\}$.

The next definition is motivated by [Ha1, §13 and 18].

Definition 6.1

(a) For $i \in \{0, \dots, t\}$ we define

$$\theta_i = N_{k(\mathfrak{f}_i\mathfrak{b})/N_i}(\theta_0(\nu_i, \mathfrak{a})).$$

(b) Let $\mathcal{C}_{\mathrm{Ha}}$ be the subgroup of E_N generated by the elements

$$\theta_i^{(\sigma-1)\sigma^v\rho^w}, \quad i = 0, \dots, t, \quad v \in \mathbb{Z}, \quad w = 0, \dots, |D_i| - 1.$$

We remark that the elements $\theta_i^{\sigma-1}$ are units by Proposition 4.8(c). Of course, $\mathcal{C}_{\mathrm{Ha}}$ is not a unit group of full rank, since χ is fixed and does not run over all non-trivial irreducible characters of G. But the result of Proposition 6.2 will show that the "χ-part of $\mathcal{C}_{\mathrm{Ha}}$" is a full sublattice of the "χ-part of E_N".

From now on we view χ as an l-adic character. Let F be a Galois extension of $\mathbb{Q}$ such that each representation of G can be realized over F. As in Section 3 we fix an embedding $i_l : \bar{\mathbb{Q}} \to \mathbb{C}_l$ and write F_l for the completion of $i_l(F)$ in $\mathbb{C}_l$. The valuation ring of F_l will be denoted by $\mathcal{O}_l$.

In order to state the next proposition we need the notion of a generalized index ideal. Let R be a Dedekind domain with quotient field M. Let X, Y be two full R-lattices on a M-vector space V. For each prime ideal $\mathfrak{p}$ of R we define $[X : Y]_{\mathfrak{p}} := (det(l_{\mathfrak{p}}))R_{\mathfrak{p}}$, where $l_{\mathfrak{p}}$ is any automorphism of $M_{\mathfrak{p}} \otimes_M V$ with $l_{\mathfrak{p}}(R_{\mathfrak{p}} \otimes_R Y) = R_{\mathfrak{p}} \otimes_R X$. Then $[X : Y]_{\mathfrak{p}} = R_{\mathfrak{p}}$ for almost all primes $\mathfrak{p}$ and we can therefore define an R-ideal $[X : Y]_R$ by requiring $([X : Y]_R)_{\mathfrak{p}} = [X : Y]_{\mathfrak{p}}$ for all primes $\mathfrak{p}$ of R. We also recall the following relation

$$[X : Y]_R = \frac{\ell_R(X/X \cap Y)}{\ell_R(Y/X \cap Y)}.$$

Proposition 6.2 *Let χ be a faithful abelian character of G. Then*

$$\left[(\mathcal{O}_l \otimes_{\mathbb{Z}} \mathcal{C}_{\mathrm{Ha}})^{\chi} : (\mathcal{O}_l \otimes_{\mathbb{Z}} im(\underline{\varphi}))^{\chi}\right]_{\mathcal{O}_l} = \left(\prod_{\psi} g(\psi)\right) \mathcal{O}_l,$$

where ψ runs through all characters of H extending χ.

The rest of this section will be devoted to the proof of Proposition 6.2.

Let ζ be a primitive $|H|$-th root of unity and set $R = \mathcal{O}_l[\zeta]$. Let M be the field of fractions of R.

We will show that

$$\left[(R \otimes_{\mathbb{Z}} \mathcal{C}_{\mathrm{Ha}})^{\chi} : (R \otimes_{\mathbb{Z}} \mathrm{im}(\underline{\varphi}))^{\chi}\right]_R = \left(\prod_{\psi|\chi} g(\psi)\right) R, \tag{34}$$

which immediately implies Proposition 6.2 since $\prod_{\psi|\chi} g(\psi) \in \mathcal{O}_l$. The computations leading to (34) will take place in $M \otimes_{\mathbb{Z}} (k^{\mathrm{ab}})^*$.

In analogy to (27) we define for integral $\mathcal{O}_k$-ideals $\mathfrak{g}, \mathfrak{g}_1$ with $\mathfrak{g} \mid \mathfrak{g}_1$ and an abelian character ψ of $\mathrm{Gal}(k(\mathfrak{g})/k)$

$$S'_{\mathfrak{g}}(\psi, \mathfrak{g}_1) = \sum_{C \in \mathrm{cl}(\mathfrak{g}_1)} \psi(C^{-1}) \otimes \varphi'_{\mathfrak{g}}(C),$$

where

$$\varphi'_{\mathfrak{g}} = \begin{cases} \varphi_{\mathfrak{g}}(C), & \text{if } \mathfrak{g} \neq (1), \\ \frac{\Delta(\mathfrak{c}^{-1})}{\Delta(\mathfrak{b}\mathfrak{c}^{-1})}, & \text{if } \mathfrak{g} = (1) \text{ and } \mathfrak{c} \in C. \end{cases}$$

Note that we have to adapt the definition of $\varphi'_{(1)}$ since $N(\mathfrak{c})^{-1}\Delta(\mathfrak{c}^{-1})/(2\pi)^{12}$ (without the absolut value) is not a class invariant. However, we have the relation

$$\sum_{g\in\mathrm{Gal}(k(1)/k)} \psi(g^{-1})\log\left|\left(\frac{\Delta(\mathcal{O}_k)}{\Delta(\mathfrak{b})}\right)^g\right| = (1-\psi(\mathfrak{b})^{-1})S_{(1)}(\psi,(1)). \tag{35}$$

The strategy for our proof of (34) is as follows: we will exhibit an R-basis $\alpha_1,\dots,\alpha_{l^t}$ of $(R\otimes_{\mathbb{Z}}\mathrm{im}(\underline{\varphi}))^\chi$ and an R-basis $\beta_1,\dots,\beta_{l^t}$ of $(R\otimes_{\mathbb{Z}}\mathcal{C}_{\mathrm{Ha}})^\chi$ and express both basis in terms of the $S'_{\mathfrak{f}_\psi}(\psi,\mathfrak{f}_\psi),\psi\mid\chi$,

$$\begin{pmatrix}\alpha_1\\ \vdots\\ \alpha_{l^t}\end{pmatrix} = A_1\begin{pmatrix}\vdots\\ S'_{\mathfrak{f}_\psi}(\psi,\mathfrak{f}_\psi)\\ \vdots\end{pmatrix}_{\psi|\chi}, \qquad \begin{pmatrix}\beta_1\\ \vdots\\ \beta_{l^t}\end{pmatrix} = A_2\begin{pmatrix}\vdots\\ S'_{\mathfrak{f}_\psi}(\psi,\mathfrak{f}_\psi)\\ \vdots\end{pmatrix}_{\psi|\chi}$$

with matrices $A_1,A_2\in\mathrm{Gl}_{l^t}(M)$. Then

$$\left[(R\otimes_{\mathbb{Z}}\mathcal{C}_{\mathrm{Ha}})^\chi : (R\otimes_{\mathbb{Z}}\mathrm{im}(\underline{\varphi}))^\chi\right]_R = \det(A_1A_2^{-1})R. \tag{36}$$

Since $(R\otimes_{\mathbb{Z}}\mathrm{im}(\underline{\varphi}))^\chi \simeq (R\otimes_{\mathbb{Z}}\Delta S)^\chi = e_\chi RH\mathfrak{p}_\infty$, an R-basis of $(R\otimes_{\mathbb{Z}}\mathrm{im}(\underline{\varphi}))^\chi$ is given by the elements $e_\chi(1\otimes\theta_N^h)$ with h running through a set of representatives of H/G.

From $e_\chi=\sum_{\psi|\chi}e_\psi$ and the definition of θ_N we obtain

$$e_\chi(1\otimes\theta_N^h) = \sum_{\psi|\chi}\psi(h)\,e_\psi \underbrace{\sum_{g\in\mathrm{Gal}(k(\mathfrak{f}\mathfrak{b})/N)}\ \sum_{J\subseteq\{1,\dots,s\}} 1\otimes\theta_0(\tau_J,\mathfrak{a})^g}_{(*)}.$$

For (*) we compute

$$\frac{1}{|H|}\sum_{g\in\mathrm{Gal}(k(\mathfrak{f}\mathfrak{b})/k)}\psi(g^{-1})\sum_{J\subseteq\{1,\dots,s\}}1\otimes\theta_0(\tau_J,\mathfrak{a})^g.$$

This expression is analogous to the right hand side of (23). We define

$$a_1(\psi) = \begin{cases}\frac{1}{|H|}\frac{N(\mathfrak{a})-\psi(\mathfrak{a})}{12N(\mathfrak{f}_\psi)w(\mathfrak{f}_\psi)}(1-\psi(\mathfrak{b})^{-1})\zeta_\psi g(\psi), & \text{if } \mathfrak{f}_\psi\neq(1),\\ \frac{1}{|H|}\frac{N(\mathfrak{a})-\psi(\mathfrak{a})}{12w(1)}\zeta_\psi g(\psi), & \text{if } \mathfrak{f}_\psi=(1),\end{cases}$$

with $g(\psi)$ defined in Defintion 5.2 and ζ_ψ as in Lemma 5.6.

Note that the Lemmas 5.4,5.5 and 5.7 also hold for S replaced by S', up to a slight difference in the case $\mathfrak{f}_\psi=(1)$ which reflects the definition of $\varphi'_{(1)}$. As in Section 5 we can prove

$$e_\chi(1\otimes\theta_N^h) = \sum_{\psi|\chi}\psi(h)a_1(\psi)S'_{\mathfrak{f}_\psi}(\psi,\mathfrak{f}_\psi). \tag{37}$$

We will now describe an R-basis of $(R\otimes_{\mathbb{Z}}\mathcal{C}_{\mathrm{Ha}})^\chi$ and compute the matrix A_2. Since $e_\chi(1\otimes\theta_i^{(\sigma-1)\sigma^v\rho^w}) = (\chi(\sigma)-1)\chi(\sigma)^v e_\chi(1\otimes\theta_i^{\rho^w})$ and $(\chi(\sigma)-1)\chi(\sigma)^v \in {\mathcal{O}_l}^*$, the set

$$\{e_\chi(1\otimes\theta_i^{\rho^w}) \mid i = 0,\dots,t, w = 0,\dots,|D_i|-1\}$$

constitutes an R-basis of $(R\otimes_{\mathbb{Z}}\mathcal{C}_{\mathrm{Ha}})^\chi$. The set of characters ψ extending χ is given by $\{\chi\phi \mid \phi\in\widehat{\mathrm{Gal}}(N/K_0)\}$. From the definition of θ_i and $\widehat{\mathrm{Gal}}(N/K_0) = \cup_{j=0}^t D_j$ we conclude

$$\begin{aligned} e_\chi(1\otimes\theta_i^{\rho^w}) &= \sum_{j=0}^t\sum_{\phi\in D_j}\phi(\rho^w)\frac{1}{|H|}\sum_{h\in H}(\chi\phi)(h^{-1})\otimes\theta_i^h \\ &= \sum_{j=0}^t\sum_{\phi\in D_j}\phi(\rho^w)\frac{1}{|H|}\sum_{h\in H/\ker(D_i)}\ \sum_{g\in\ker(D_i)}(\chi\phi)((hg)^{-1})\otimes\theta_i^{hg}. \end{aligned}$$

Since $\mathrm{Gal}(N/K_0)$ is cyclic, we have a filtration

$$1 = \ker(D_t)\subset\ker(D_{t-1})\subset\ldots\subset\ker(D_1)\subset\ker(D_0) = \mathrm{Gal}(N/K_0).$$

By definition θ_i is contained in $N_i = N^{ker(D_i)}$. Hence we compute further

$$\begin{aligned} &\sum_{h\in H/\ker(D_i)}\ \sum_{g\in\ker(D_i)}(\chi\phi)((hg)^{-1})\otimes\theta_i^{hg} \\ &= \sum_{h\in H/\ker(D_i)}(\chi\phi)(h^{-1})\left(\sum_{g\in\ker(D_i)}(\chi\phi)(g^{-1})\right)\otimes\theta_i^h \\ &= \begin{cases} 0, & \text{if } i<j, \\ l^{t-i}\sum_{h\in H/\ker(D_i)}(\chi\phi)(h^{-1})\otimes\theta_i^h, & \text{if } i\geq j. \end{cases} \end{aligned} \tag{38}$$

From (38) and the definition of θ_i we derive

$$e_\chi(1\otimes\theta_i^{\rho^w}) = \sum_{j=0}^i\sum_{\phi\in D_j}\phi(\rho^w)\frac{l^{t-i}}{|H|}\sum_{g\in\mathrm{Gal}(k(\mathfrak{f}_i\mathfrak{b})/k)}(\chi\phi)(g^{-1})\otimes\theta_0(\nu_i,\mathfrak{a})^g. \tag{39}$$

The equation (17) implies

$$\begin{aligned} &\sum_{g\in\mathrm{Gal}(k(\mathfrak{f}_i\mathfrak{b})/k)}(\chi\phi)(g^{-1})\otimes\theta_0(\nu_i,\mathfrak{a})^g \\ &= \frac{N(\mathfrak{a})-(\chi\phi)(\mathfrak{a})}{12N(\mathfrak{f}_i\mathfrak{b})}\sum_{g\in\mathrm{Gal}(k(\mathfrak{f}_i\mathfrak{b})/k)}(\chi\phi)(g^{-1})\otimes\left(\varphi^{12N(\mathfrak{f}_i\mathfrak{b})}(\nu_i\mid L)\right)^g. \end{aligned}$$

Since ν_i is a primitive $\mathfrak{f}_i\mathfrak{b}$-torsion point of $\mathbb{C}/L$ there exists an integral $\mathcal{O}_k$-ideal $\mathfrak{c}_i$ such that

$$\left(\frac{\nu_i}{\Omega}\right) = \mathfrak{c}_i(\mathfrak{f}_i\mathfrak{b})^{-1}, \quad (\mathfrak{c}_i,\mathfrak{f}_i\mathfrak{b}) = 1.$$

By the homogeneity of $\varphi^{12N(\mathfrak{f}_i\mathfrak{b})}$ and Lemma 4.7(d) we conclude

$$\begin{aligned}\varphi^{12N(\mathfrak{f}_i\mathfrak{b})}(\nu_i \mid L) &= \varphi^{12N(\mathfrak{f}_i\mathfrak{b})}(1 \mid \mathfrak{f}_i\mathfrak{b}\mathfrak{c}_i^{-1}) \\ &= \varphi^{12N(\mathfrak{f}_i\mathfrak{b})}(1 \mid \mathfrak{f}_i\mathfrak{b})^{\sigma(\mathfrak{c}_i)}.\end{aligned}$$

Hence we obtain for $0 \leq j \leq i$ and $\phi \in D_j$

$$\begin{aligned}& \sum_{g\in \mathrm{Gal}(k(\mathfrak{f}_i\mathfrak{b})/k)} (\chi\phi)(g^{-1}) \otimes \theta_0(\nu_i, \mathfrak{a}) \\ =\ & \frac{N(\mathfrak{a}) - (\chi\phi)(\mathfrak{a})}{12N(\mathfrak{f}_i\mathfrak{b})}(\chi\phi)(\mathfrak{c}_i) \times \\ & \sum_{g\in \mathrm{Gal}(k(\mathfrak{f}_i\mathfrak{b})/k)} (\chi\phi)(g^{-1}) \otimes \varphi^{12N(\mathfrak{f}_i\mathfrak{b})}(1 \mid \mathfrak{f}_i\mathfrak{b})^g \\ =\ & \frac{N(\mathfrak{a}) - (\chi\phi)(\mathfrak{a})}{12N(\mathfrak{f}_i\mathfrak{b})}(\chi\phi)(\mathfrak{c}_i) S'_{\mathfrak{f}_i\mathfrak{b}}(\chi\phi, \mathfrak{f}_i\mathfrak{b}) \end{aligned} \tag{40}$$

By the analogon of Lemma 5.7 (adapted to the definition of $\varphi'_{(1)}$ we obtain for $\phi \in D_j$ with $0 \leq j \leq i$

$$\frac{1}{|H|} \sum_{g\in \mathrm{Gal}(k(\mathfrak{f}_i\mathfrak{b})/k)} (\chi\phi)(g^{-1}) \otimes \theta_0(\nu_i, \mathfrak{a}) = a_2^{(i)}(\chi\phi) S'_{\mathfrak{f}_{\chi\phi}}(\chi\phi, \mathfrak{f}_{\chi\phi}), \tag{41}$$

where

$$\begin{aligned}& a_2^{(i)}(\chi\phi) \\ =\ & \begin{cases} \frac{1}{|H|}\frac{N(\mathfrak{a})-(\chi\phi)(\mathfrak{a})}{12N(\mathfrak{f}_j)w(\mathfrak{f}_j)}(\chi\phi)(\mathfrak{c}_i)(1-(\chi\phi)(\mathfrak{b})^{-1})\prod_{\mathfrak{p}\mid\mathfrak{f}_i,\mathfrak{p}\nmid\mathfrak{f}_j}(1-(\chi\phi)(\mathfrak{p})^{-1}), \\ \text{if } \mathfrak{f}_j \neq (1), \\ \frac{1}{|H|}\frac{N(\mathfrak{a})-(\chi\phi)(\mathfrak{a})}{12w(1)}(\chi\phi)(\mathfrak{c}_i)\prod_{\mathfrak{p}\mid\mathfrak{f}_i}(1-(\chi\phi)(\mathfrak{p})^{-1}), \\ \text{if } \mathfrak{f}_j = (1). \end{cases}\end{aligned}$$

Hence we obtain from (39) and (41) for $i = 0, \ldots, t$ and $w = 0, \ldots, |D_i| - 1$

$$e_\chi(1 \otimes \theta_i^{\rho^w}) = \sum_{j=0}^{i} \sum_{\phi\in D_j} \phi(\rho^w) l^{t-i} a_2^{(i)}(\chi\phi) S'_{\mathfrak{f}_{\chi\phi}}(\chi\phi, \mathfrak{f}_{\chi\phi}). \tag{42}$$

We are now in position to compute the matrices A_1 and A_2. On the one hand we derive from (37)

$$\begin{pmatrix} \vdots \\ e_\chi(1 \otimes \theta_N^h) \\ \vdots \end{pmatrix}_{h\in \mathrm{Gal}(N/K_0)} = A_1 \begin{pmatrix} \vdots \\ S'_{\mathfrak{f}_{\chi\phi}}(\psi, \mathfrak{f}_\psi) \\ \vdots \end{pmatrix}_{\psi\mid\chi},$$

where

$$A_1 = (\psi(h))_{\substack{h\in \mathrm{Gal}(N/K_0) \\ \psi\mid\chi}} \cdot \mathrm{diag}\,(a_1(\psi))_{\psi\mid\chi}.$$

On the other hand (42) implies

$$\begin{pmatrix} \vdots \\ e_\chi(1\otimes\theta_i^{\rho^w}) \\ \vdots \end{pmatrix}_{i=0,\dots,t,w=0,\dots,|D_i|-1} = A_2 \begin{pmatrix} \vdots \\ S'_{\mathfrak{f}_{\chi\phi}}(\chi\phi,\mathfrak{f}_{\chi\phi}) \\ \vdots \end{pmatrix}_{j=0,\dots,t,\phi\in D_j},$$

where A_2 is a block matrix of the form

$$A_2 = \begin{pmatrix} M_{00} & 0 & 0 & \dots & 0 \\ M_{10} & M_{11} & 0 & \dots & 0 \\ \vdots & & \ddots & & \\ M_{t0} & & \dots & & M_{tt} \end{pmatrix}.$$

Each block M_{ij} is a $|D_i|\times|D_j|$-matrix given by

$$\begin{aligned} M_{ij} &= l^{t-i}\left(a_2^{(i)}(\chi\phi)\phi(\rho^w)\right)_{\substack{w=0,\dots,|D_i|-1\\ \phi\in D_j}} \\ &= l^{t-i}\left(\phi(\rho^w)\right)_{\substack{w=0,\dots,|D_i|-1\\ \phi\in D_j}}\cdot \operatorname{diag}\left(a_2^{(i)}(\chi\phi)\right)_{\phi\in D_j}. \end{aligned}$$

The determinant of A_1 is easily computed. We have

$$\det(A_1) = l^{\frac{1}{2}tl^t}\cdot\prod_{\psi|\chi} a_1(\psi). \tag{43}$$

Lemma 6.3

$$\prod_{i=0}^{t}\det\left(l^{t-i}\phi(\rho^w)\right)_{\substack{w=0,\dots,|D_i|-1\\ \phi\in D_i}} = \pm l^{\frac{1}{2}tl^t}.$$

Proof Recall that $D_i = \{\phi_0^{l^{t-i}j} \mid j=1,\dots,l^i,(j,l)=1\}$. It follows that $(\det(\phi(\rho^w)_{w,\phi})^2$ equals the field discriminant of $\mathbb{Q}(\zeta_{l^i})/\mathbb{Q}$. By [Wa, Ch.2, Prop. 2.1] we therefore derive

$$\begin{aligned} &\prod_{i=0}^{t}\det\left(l^{t-i}\phi(\rho^w)\right)_{\substack{w=0,\dots,|D_i|-1\\ \phi\in D_i}} \\ = &\prod_{i=0}^{t} l^{(t-i)|D_i|}\cdot d^{1/2}_{\mathbb{Q}(\zeta_{l^i})/\mathbb{Q}} \\ = &\pm l^t\prod_{i=1}^{t} l^{(t-i)l^{i-1}(l-1)}\cdot l^{l^{i-1}(li-i-1)/2}. \end{aligned}$$

An elementary computation shows that this is equal to $\pm l^{\frac{1}{2}tl^t}$. $\square$

Lemma 6.3 implies that

$$\det(A_2) = \pm l^{\frac{1}{2}tl^t} \cdot \prod_{i=0}^{t} \prod_{\phi \in D_i} a_2^{(i)}(\chi\phi). \tag{44}$$

Now (34) (and thus also Proposition 6.2) is an immediate consequence of (36), (43), (44) and the definition of $a_1(\psi)$ and $a_2^{(i)}(\chi\phi)$.

7 Proofs of the main results

We assume the situation described at the beginning of Section 5. From Proposition 3.2, Proposition 5.3 and Proposition 6.2 we conclude

$$\mathfrak{a}^{(l)}(\chi) = \left(\prod_{\psi|\chi} (N(\mathfrak{a}) - \psi(\mathfrak{a}))(\psi(\mathfrak{b}) - 1) \right) \frac{\ell_{\mathcal{O}_l}(\mathrm{cl}_N^\chi)}{\ell_{\mathcal{O}_l}((E_N/\mathcal{C}_{\mathrm{Ha}})^\chi)}. \tag{45}$$

Since χ is a faithful abelian character of G the hypothesis (20) implies that $\psi(\mathfrak{b})$ is a non-trivial root of unity of order dividing l'. Therefore $\psi(\mathfrak{b}) - 1 \sim_l 1$.

Lemma 7.1 *(a) Suppose that either $l \nmid w_N$ or $K_0 \neq k(\zeta_l)$. Then there exists an integral $\mathcal{O}_k$-ideal $\mathfrak{a}$ such that*

$$\prod_{\psi|\chi} (N(\mathfrak{a}) - \psi(\mathfrak{a})) \sim_l \ell_{\mathcal{O}_l}(\mu_N^\chi) \sim_l 1.$$

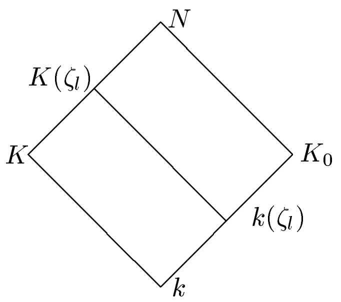
(b) If $K_0 = k(\zeta_l)$, then

$$\ell_{\mathcal{O}_l}(\mu_N^\chi) \mid \prod_{\psi|\chi} (N(\mathfrak{a}) - \psi(\mathfrak{a}))$$

for all integral $\mathcal{O}_k$-ideals $\mathfrak{a}$.

Proof (a) If $l \nmid w_N$ then obviously $\ell_{\mathcal{O}_l}(\mu_N^\chi) = 1$. For the choice of the integral ideal $\mathfrak{a}$ we consider the tower of fields $k \subseteq N \subseteq N(\zeta_l)$ and take $\mathfrak{a}$ such that $(\mathfrak{a}, N(\zeta_l)/k) \neq 1$ and $(\mathfrak{a}, N/k) = 1$. Then $\psi(\mathfrak{a}) = 1$ and since $\zeta_l^{(\mathfrak{a}, N(\zeta_l)/k)} = \zeta_l^{N(\mathfrak{a})}$ we obtain $N(\mathfrak{a}) - \psi(\mathfrak{a}) = N(\mathfrak{a}) - 1 \not\equiv 0 (\mathrm{mod}\ l)$.

If $l \mid w_N$, but $K_0 \neq k(\zeta_l)$, then we have the following diagram of fields



with $N \neq K(\zeta_l)$. We choose $\mathfrak{a}$ such that $(\mathfrak{a}, N/k) \in \mathrm{Gal}(N/K(\zeta_l)) \setminus \{1\}$. Then $N(\mathfrak{a}) - \psi(\mathfrak{a}) = N(\mathfrak{a}) - \chi(\mathfrak{a}) = N(\mathfrak{a}) - 1 + 1 - \chi(\mathfrak{a})$. Since $(\mathfrak{a}, N/k)$ acts trivially on ζ_l we have $N(\mathfrak{a}) \equiv 1 (\mathrm{mod}\ l)$. The character value $\chi(\mathfrak{a})$ is a root of unity of order prime to l and therefore $(1 - \chi(\mathfrak{a}), l) = 1$, which implies the assertion.

(b) The set of characters $\psi \mid \chi$ is given by $\chi\phi, \phi \in \mathrm{Gal}(N/K_0)$. On writing $\sigma(\mathfrak{a}) = \sigma_1\sigma_2$ with $\sigma_1 \in G,\ \sigma_2 \in \mathrm{Gal}(N/K_0)$ we compute

$$\prod_{\psi \mid \chi} (N(\mathfrak{a}) - \psi(\mathfrak{a})) = \prod_{\phi \in \mathrm{Gal}(N/K_0)} (N(\mathfrak{a}) - \chi(\sigma_1)\phi(\sigma_2)\phi(\mathfrak{a}))$$
$$= \prod_{j=0}^{l^t-1} (N(\mathfrak{a}) - \chi(\sigma_1)\zeta_{l^t}^j) = N(\mathfrak{a})^{l^t} - \chi(\sigma_1)^{l^t}.$$

We write $w_N = l^s \cdot k$ with $(l, k) = 1,\ t \geq s - 1$. Since $\mu_N^\chi = e_\chi(\mathcal{O}_l \otimes_{\mathbb{Z}} \mu_N)$ is cyclic generated by $e_\chi(1 \otimes \zeta_{l^s})$ it suffices to show that $N(\mathfrak{a})^{l^t} - \chi(\sigma_1)^{l^t}$ annihilates $e_\chi(1 \otimes \zeta_{l^s})$. On the one hand we have $\sigma_1^{l^t} e_\chi(1 \otimes \zeta_{l^s}) = \chi(\sigma_1)^{l^t} e_\chi(1 \otimes \zeta_{l^s})$. On the other hand $\sigma_1^{l^t} e_\chi(1 \otimes \zeta_{l^s}) = \frac{1}{|G|} \sum_{g \in G} \chi(g^{-1}) \otimes \zeta_{l^s}^{\sigma_1^{l^t} g} = \frac{1}{|G|} \sum_{g \in G} \chi(g^{-1}) \otimes \left(\zeta_{l^s}^{N(\mathfrak{a})^{l^t}}\right)^g = N(\mathfrak{a})^{l^t} e_\chi(1 \otimes \zeta_{l^s})$. Hence $N(\mathfrak{a})^{l^t} - \chi(\mathfrak{a})^{l^t}$ annihilates $e_\chi(1 \otimes \zeta_{l^s})$. $\square$

In the sequel we assume that l is fixed and satisfies either

$$l \nmid w_N \text{ or } (l \mid w_N \text{ and } K_0 \neq k(\zeta_l)). \tag{46}$$

Then Lemma 7.1(a) implies that

$$\mathfrak{a}^{(l)}(\chi) = \frac{\ell_{\mathcal{O}_l}(\mathrm{cl}_N^\chi)}{\ell_{\mathcal{O}_l}((E_N/(\mu_N \times \mathcal{C}_{\mathrm{Ha}}))^\chi)}. \tag{47}$$

In order to show that this quotient equals (1) (or to derive at least some divisibility result) we will employ the Euler system method as presented by Rubin in [Ru2, §1-3].

We fix a power M of l and unfortunately have to impose the additional hypothesis

$$N \text{ contains the Hilbert-}l\text{-class field } k(1)_l. \tag{48}$$

We define $\mathcal{L} = \mathcal{L}_{N,M}$ to be the set of primes $\mathfrak{l}$ of k not dividing w_k and satisfying

(i) $\mathfrak{l}$ splits completely in N/k

(ii) $N(\mathfrak{l}) \equiv 1 (\mathrm{mod}\ M)$.

Lemma 7.2 *For $\mathfrak{l} \in \mathcal{L}$ there exists a unique extension $N[\mathfrak{l}]$ of N of degree M in $Nk(\mathfrak{l})$. Further $N[\mathfrak{l}]/N$ is cyclic, totally ramified at all primes above $\mathfrak{l}$ and unramified at all primes not dividing $\mathfrak{l}$.*

Proof The proof is just an adaption of the proof of [Ru2, Lemma 1.1] (see also [BH, page ???]).

For each $\mathfrak{l} \in \mathcal{L}$ there exists a unique cyclic extension $C/k(1)$ such that $M = [C : k(1)]$ and $C \subseteq k(\mathfrak{l})$. Let C' be the unique cyclic subextension of $C/k(1)_l$ with $[C' : k(1)_l] = M$. If we set $N[\mathfrak{l}] = NC'$, then the assertions of the Lemma follow from global class field theory. $\square$

We write $\mathcal{S} = \mathcal{S}_{N,M}$ for the set of squarefree integral ideals of k which are divisible only by primes $\mathfrak{l} \in \mathcal{L}$. For $\mathfrak{g} \in \mathcal{S}$ with $\mathfrak{g} = \prod_{i=1}^n \mathfrak{l}_i$ we set $N[\mathfrak{g}] = N[\mathfrak{l}_1] \cdots N[\mathfrak{l}_n]$. Note that for $\mathfrak{l}_1, \mathfrak{l}_2 \in \mathcal{L}$, $\mathfrak{l}_1 \neq \mathfrak{l}_2$, the extensions $N[\mathfrak{l}_1]/N$ and $N[\mathfrak{l}_2]/N$ are linearly disjoint.

For an integral $\mathcal{O}_k$-ideal $\mathfrak{c}$ we write $\mathcal{S}(\mathfrak{c})$ for the subset of $\mathcal{S}$ consisting of ideals $\mathfrak{g} \in \mathcal{S}$ with $(\mathfrak{c}, \mathfrak{g}) = 1$. Furthermore we let $\mathcal{U}_M(\mathfrak{c}) = \mathcal{U}(\mathfrak{c})$ denote the set of functions $\alpha : \mathcal{S}(\mathfrak{c}) \to \bar{N}^*$ such that the following axioms hold:

- ES(i) $\quad \alpha(\mathfrak{g}) \in N[\mathfrak{g}]^*$ for all $\mathfrak{g} \in \mathcal{S}(\mathfrak{c})$.
- ES(ii) $\quad \alpha(\mathfrak{g})$ is a global unit if $\mathfrak{g} \neq (1)$.
- ES(iii) $\quad N_{N[\mathfrak{g}]/N[\mathfrak{g}/\mathfrak{l}]}(\alpha(\mathfrak{g})) = \alpha(\mathfrak{g}/\mathfrak{l})^{\sigma(\mathfrak{l})-1}$, if $\mathfrak{l} \mid \mathfrak{g}$.
- ES(iv) $\quad \alpha(\mathfrak{g}) \equiv \alpha(\mathfrak{g}/\mathfrak{l})^{(N(\mathfrak{l})-1)/M}$ modulo all primes above $\mathfrak{l}$, if $\mathfrak{l} \mid \mathfrak{g}$.

We define $\mathcal{U}_N = \mathcal{U}_{N,M}$ to be the disjoint union of the sets $\mathcal{U}(\mathfrak{c})$ over all integral ideals $\mathfrak{c}$ of $\mathcal{O}_k$. Then $\mathcal{U}_N$ is closed under multiplication, inverses and the action of $\mathrm{Gal}(\bar{N}/k)$.

Recall the definition (16) of the function θ_0 which was based on a fixed elliptic curve E defined over $F = k(\mathfrak{b})$. The period lattice of E was denoted by L. Following [Ru2] we will now define a group of elliptic units. Let $\mathfrak{c}$ be an integral $\mathcal{O}_k$-ideal such that $\mathfrak{b} \mid \mathfrak{c}$. Let $\tau \in \mathbb{C}/L$ be a primitive $\mathfrak{c}$-torsion point of $\mathbb{C}/L$ and let $\mathfrak{a}$ be an integral $\mathcal{O}_k$-ideal with $(\mathfrak{a}, 6\mathfrak{c}) = 1$. For every $\mathfrak{l} \in \mathcal{L}$ we fix a primitive $\mathfrak{l}$-torsion point $\tau_\mathfrak{l}$ of $\mathbb{C}/L$. Then, for every $\mathfrak{g} \in \mathcal{S}(\mathfrak{a}\mathfrak{c})$, we set

$$\alpha_{\tau,\mathfrak{a}}(\mathfrak{g}) = N_{k(\mathfrak{c}\mathfrak{g})N/N[\mathfrak{g}]}(\theta_0(\tau + \sum_{\mathfrak{l}\mid\mathfrak{g}} \tau_\mathfrak{l}, \mathfrak{a})).$$

From Proposition 4.8 we conclude that $\alpha_{\tau,\mathfrak{a}} \in \mathcal{U}(\mathfrak{a}\mathfrak{c})$. As in [Ru2] we write C_N for the group of global units generated by

$$\{\alpha_{\tau,\mathfrak{a}}(1)^{\sigma-1} : \tau, \alpha \text{ as above }, \sigma \in \mathrm{Gal}(N/k)\}.$$

Then C_N is a $\mathbb{Z}\mathrm{Gal}(N/k)$-module and we define the group of elliptic units by

$$\mathcal{C}_N = \mu_N C_N. \tag{49}$$

Theorem 7.3 *[Ru2, Theorem 3.2] Suppose that $l \nmid [N : k]$ and $k(1)_l \subseteq N$. Let ψ be an irreducible $\mathbb{Q}_l$-character of G whose restriction to* $\mathrm{Gal}(N/N \cap k(\zeta_l))$ *is non-trivial. Then*

$$\ell_{\mathbb{Z}_l}(\mathrm{cl}_N^\psi) \mid \ell_{\mathbb{Z}_l}((E_N/\mathcal{C}_N)^\psi).$$

Remarks 7.4 (a) Unlike Rubin in [Ru2, §1] we do not assume that l does not divide the number $w_{k(1)}$ of roots of unity in $k(1)$. For that reason we have to replace the condition "$\psi \neq 1$" by "$\psi|_{\mathrm{Gal}(N/N\cap k(\zeta_l))} \neq 1$" (see [Ru3, Theorem 3.2] or [Ho, Theorem 5.9]).

(b) In our applications we can assume that ψ is a faithful character. Therefore the restriction of ψ to $\mathrm{Gal}(N/N \cap k(\zeta_l))$ is non-trivial unless $N \subseteq k(\zeta_l)$. But in this case $N/\mathbb{Q}$ is abelian, $l \neq 2$ and we deduce from [RW2, Theorem A] and the induction property for $\mathfrak{a}^{(l)}(\psi)$ that $\mathfrak{a}^{(l)}_{N/k}(\psi) = (1)$.

Recall the definition of the elements θ_N (Definition 5.1) and θ_i, $i = 0, \ldots, t$ (Definition 6.1). The next lemma shows that the unit groups $\mathrm{im}(\underline{\varphi})$ and $\mathcal{C}_{\mathrm{Ha}}$ are contained in $\mathcal{C}_N$.

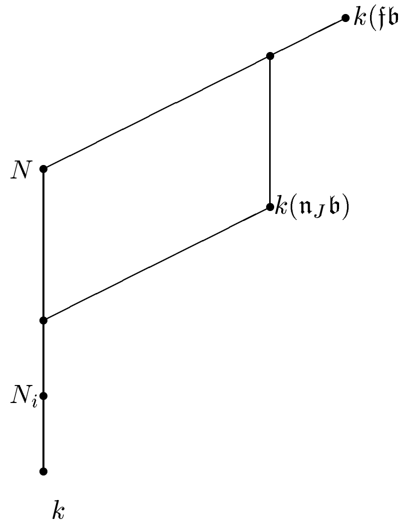
Lemma 7.5 *(a) $\theta_N^{h-1} \in \mathcal{C}_N$ for $h \in H \setminus \{1\}$.*

(b) $\theta_i^{\sigma-1} \in \mathcal{C}_N$ for $i \in \{0, \ldots, t\}$ and $\sigma \in G = \mathrm{Gal}(N/K)$.

Proof (a) For each subset $J \subseteq \{0, \ldots, t\}$ we define a map $\alpha_J = \alpha_{\tau_J, \mathfrak{a}} : \mathcal{S}(\mathfrak{n}_J \mathfrak{b}\mathfrak{a}) \to \bar{N}^*$ by

$$\alpha_J(\mathfrak{g}) = N_{k(\mathfrak{n}_J \mathfrak{b}\mathfrak{g})N/N[\mathfrak{g}]} \left(\theta_0(\tau_J + \sum_{\mathfrak{l}|\mathfrak{g}} \tau_{\mathfrak{l}}, \mathfrak{a}) \right).$$

Considering the diagram



we derive from Proposition 4.8(c)

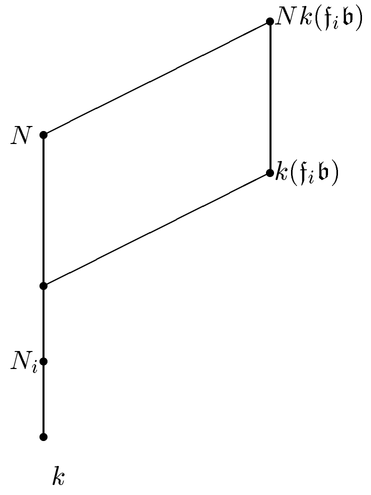
$$\begin{aligned} & N_{k(\mathfrak{f}\mathfrak{b})/N}(\theta_0(\tau_J, \mathfrak{a})) = N_{k(\mathfrak{n}_J \mathfrak{b})N/N} N_{k(\mathfrak{f}\mathfrak{b})/k(\mathfrak{n}_J \mathfrak{b})N}(\theta_0(\tau_J, \mathfrak{a})) \\ = \;& N_{k(\mathfrak{n}_J \mathfrak{b})N/N}(\theta_0(\tau_J, \mathfrak{a}))^{[k(\mathfrak{f}\mathfrak{b}):k(\mathfrak{n}_J \mathfrak{b})N]} = \alpha_J(1)^{[k(\mathfrak{f}\mathfrak{b}):k(\mathfrak{n}_J \mathfrak{b})N]}. \end{aligned}$$

Hence $\theta_N^{h-1} \in \mathcal{C}_N$ for all $h \in H \setminus \{1\}$.

(b) For each $i \in \{0, \ldots, t\}$ we define a map $\alpha_i = \alpha_{\nu_i, \mathfrak{a}} : \mathcal{S}(\mathfrak{f}_i \mathfrak{b} \mathfrak{a}) \to \bar{N}^*$ by

$$\alpha_i(\mathfrak{g}) = N_{k(\mathfrak{f}_i \mathfrak{b} \mathfrak{g})N/N[\mathfrak{g}]} \left(\theta_0(\nu_i + \sum_{\mathfrak{l} \mid \mathfrak{g}} \tau_{\mathfrak{l}}, \mathfrak{a}) \right)$$

Since $\theta_0(\nu_i, \mathfrak{a}) \in k(\mathfrak{f}_i \mathfrak{b})$ by Proposition 4.8 the diagram of fields



implies that $\theta_i = N_{k(\mathfrak{f}_i \mathfrak{b})/N_i}(\theta_0(\nu_i, \mathfrak{a})) = N_{k(\mathfrak{f}_i \mathfrak{b}) \cap N/N_i}(\alpha_i(1))$. Hence $\theta_i^{\sigma-1} \in \mathcal{C}_N$. □

Proof of Theorem 1.1 By the inflation property (Proposition 3.1(d)) we may assume that N/k is cyclic. By Proposition 3.3(c) it suffices to show that $\mathfrak{a}^{(l)}(\psi)^{-1}$ is integral whenever ψ is a non-trivial $\mathbb{Q}_l$-irreducible character of N/k. By the inflation property we may also assume that ψ is faithful. Write

$$\psi = \sum_{\alpha \in \mathrm{Gal}(\mathbb{Q}_l(\chi)/\mathbb{Q}_l)} \chi^\alpha,$$

where χ is a non-trivial linear character of $\mathrm{Gal}(N/k)$. Without loss of generality we may assume that hypothesis (46) is satisfied. In the exceptional case, $N = K_0 = k(\zeta_l)$, the absolut extension $N/\mathbb{Q}$ is abelian and $l \neq 2$. Thus $\mathfrak{a}^{(l)}(\psi) = (1)$ follows from [RW2, Theorem A] (see also Remark 7.4(b)).

From (47) and the l-adic analogue of Propositon 3.1(a) we obtain

$$\mathfrak{a}^{(l)}(\psi) = \frac{\ell_{\mathbb{Z}_l}(\mathrm{cl}^\psi)}{\ell_{\mathbb{Z}_l}((E_N/(\mu_N \times \mathcal{C}_{\mathrm{Ha}}))^\psi)}.$$

By Lemma 7.5 $(\mu_N \times \mathcal{C}_{\mathrm{Ha}})^{\psi} \subseteq \mathcal{C}_N{}^{\psi}$. Since $l \nmid h_k$ we have $k(1)_l = k$ and assumption (48) is trivially satisfied. Therefore we can apply Theorem 7.3. If the restriction of ψ to $\mathrm{Gal}(N/N \cap k(\zeta_l))$ is non-trivial, then $\mathfrak{a}^{(l)}(\psi)^{-1}$ is integral. Otherwise $N \subseteq k(\zeta_l)$, $l \neq 2$ and we obtain $\mathfrak{a}^{(l)}(\psi) = (1)$ from [RW2, Theorem A]. □

Certainly it is unsatisfactory that we have to exclude prime divisors l of $[N : k]$ in Theorem 1.1. To deal with these primes we have to consider a diagram of fields like in (19). In this situation we need a divisibility result of the form

$$\ell_{\mathbb{Z}_l}(\mathrm{cl}_N^{\psi}) \mid \ell_{\mathbb{Z}_l}((E_N/\mathcal{C}_N)^{\psi}) \tag{50}$$

for all $\mathbb{Q}_l$-irreducible characters ψ of $\mathrm{Gal}(N/K)$.

A statement like this is given in [Ho, Theorem 5.9]. Unfortunately there is an error in the proof. To point out this mistake we use the notation of [Ho]. On page 334 of [Ho] a tower of fields $F[\lambda]/F$ is exhibited satisfying the axioms EF(i)–(iv). But the fields constructed in the last but one paragraph do not satisfy EF(ii). On the contrary, each finite place above $\lambda \cap K_0$ (and not only λ) is totally ramified in $F[\lambda]/F$. Despite strong effort this mistake has not yet been fixed. Note however, that an analogous assertion for abelian extensions $N/\mathbb{Q}$ holds true. This can be derived from [RW2, §11 and Theorem A] together with a result analogous to Proposition 6.2. We also mention that the proof of [RW2, Theorem A] heavily relies on the results concerning the main conjecture of Iwasawa theory for totally real fields of A.Wiles [Wi].

Assuming (50) we can prove a stronger result.

Theorem 7.6 *Let k be an imaginary quadratic number field with class number $h_k = 1$. Let L be an abelian number field extension of k. Suppose that for each prime l and all subextensions N/k of L/k the divisibility assertion of (50) holds. Suppose further that $w_L = 3^a w_k^b$ with $a \geq 0, b \geq 1$. Then $\mathfrak{a}(\chi) = (1)$ for all characters χ of $\mathrm{Gal}(L/k)$.*

Proof We fix a prime l and show $(l, \mathfrak{a}(\chi)) = 1$. By Proposition 3.1(d) it suffices to show that $\mathfrak{a}^{(l)}(\psi)^{-1}$ is integral for all cyclic subextensions N/k of L/k and all $\mathbb{Q}_l$-irreducible faithful characters ψ of $\mathrm{Gal}(N/K)$ with K as in diagram (19).

Suppose first $l \neq 3$. Then $w_L = 3^a w_k^b$ implies that either (46) is satisfied or that $k = K_0$. If $k = K_0$ we are done since then $N = K$. If (46) holds then

$$\mathfrak{a}^{(l)}(\psi) = \frac{\ell_{\mathbb{Z}_l}(\mathrm{cl}_N^{\psi})}{\ell_{\mathbb{Z}_l}((E_N/(\mu_N \times \mathcal{C}_{\mathrm{Ha}}))^{\psi})}.$$

By Lemma 7.5 we have $(\mu_N \times \mathcal{C}_{\mathrm{Ha}})^{\psi} \subseteq \mathcal{C}_N{}^{\psi}$. Hence (50) implies that $\mathfrak{a}^{(l)}(\psi)$ is integral.

If $l = 3$ then either (46) is satisfied, in which case we procedd as before, or $K_0 = k(\zeta_3)$. But then N/K is of degree 2 and we obtain $\mathfrak{a}^{(l)}(\psi) = (1)$ from $\mathfrak{a}^{(l)}(\mathrm{ind}_1^{\mathrm{Gal}(N/K)} 1) = (1) = \mathfrak{a}^{(l)}(1)$. □

Remarks

(a) Theorem 7.6 should be compared to [BH, Theorem 1].

(b) The assumption $h_k = 1$ is needed to define the subgroup $\mathcal{C}_N$ for all primes l. Without the hypothesis $h_k = 1$ we can derive a result of the form

$$(\mathfrak{a}(\chi), l) = 1 \text{ for all primes } l \text{ with } l \nmid h_k$$

and all characters χ of $\mathrm{Gal}(L/k)$.

In order to prove Theorem 1.3 we need some more notation. For the convenience of the reader we adopt most of the notation of [Ru2]. We write

$$\Gamma = \mathrm{Gal}(K_\infty/K_0), \quad \Delta = \mathrm{Gal}(K_0/k), \quad \mathcal{G} = \Delta \times \Gamma = \mathrm{Gal}(K_\infty/k).$$

As always we assume $l \nmid |\Delta|$. For every extension F of k in K_∞ write A_F for the l-part of the ideal class group cl_F, E_F for the group of global units of F and $\mathcal{C}_F$ for the group of elliptic units as defined in (49). Fix an $\mathcal{O}_k$-prime ideal $\mathfrak{p}$ and write U_F for the group of local units of $F \otimes_{\mathbb{Z}} k_{\mathfrak{p}}$ which are congruent to 1 modulo all primes above $\mathfrak{p}$. Let $\bar{\mathcal{E}}_F$ and $\bar{\mathcal{C}}_F$ be the closures of $E_F \cap U_F$ and $\mathcal{C}_F \cap U_F$, respectively, in U_F.

Finally we define

$$A_\infty = \varprojlim A_F, \quad \bar{\mathcal{E}}_\infty = \varprojlim \bar{\mathcal{E}}_F, \quad \bar{\mathcal{C}}_\infty = \varprojlim \bar{\mathcal{C}}_F,$$

where the inverse limits are taken over all finite extensions F of k in K_∞ with respect to the norm maps.

We define the Iwasawa algebra

$$\Lambda = \mathbb{Z}_l[[\mathcal{G}]] = \varprojlim \mathbb{Z}_l[\mathrm{Gal}(F/k)]$$

with the inverse limit taken over all finite extensions F of k in K_∞. For a closed subgroup $\mathcal{H}$ of $\mathcal{G}$ we define $\mathcal{J}(\mathcal{H})$ to be the Λ-ideal generated by $\{\gamma - 1 : \gamma \in \mathcal{H}\}$. We write $\mathcal{D}_{\mathfrak{p}}$ for the decomposition group of an $\mathcal{O}_k$-ideal $\mathfrak{p}$ in K_∞/k. Finally let $T \subseteq \{\mathfrak{p} : \mathfrak{p} \mid l\}$ be the set of primes of k which ramify in K_∞/K_0 and define $\mathcal{J}_T = \prod_{\mathfrak{p} \in T} \mathcal{J}(\mathcal{D}_{\mathfrak{p}})$.

For every irreducible $\mathbb{Q}_l$-character ψ of Δ we have

$$\Lambda^\psi = e_\psi \mathbb{Z}_l[[\Delta \times \Gamma]] \simeq R_\psi[[\Gamma]],$$

where R_ψ is the valuation ring in the unramified extension of $\mathbb{Q}_l$ of degree $\dim(\psi)$. Furthermore each Λ^ψ is (non-canonically) isomorphic to a power series ring over R_ψ,

$$\Lambda^\psi \simeq R_\psi[[T]].$$

A Λ-module Y is called a torsion Λ-module if and only if Y^ψ is a torsion Λ^ψ-module for every ψ. By the well-known classification theorem for Λ^ψ-modules we know that for every finitely generated torsion Λ^ψ-module Y^ψ we can find power series $f_{i,\psi} \in \Lambda^\psi$ and a pseudo-isomorphism

$$Y^\psi \longrightarrow \oplus \Lambda^\psi / f_{i,\psi} \Lambda^\psi.$$

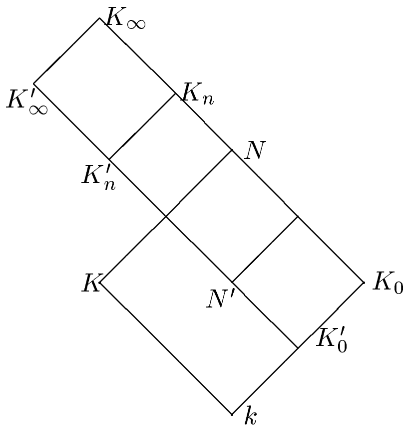
Then $\mathrm{char}(Y^\psi) = (\prod f_{i,\psi}) \Lambda^\psi$ is a well-defined invariant of the Λ^ψ-module Y^ψ and is usually called the characteristic ideal.

In [Ru2, §5] it is proved that A_∞ and $\bar{\mathcal{E}}_\infty/\bar{\mathcal{C}}_\infty$ are finitely generated torsion Λ-modules. Moreover it is shown in the proof of [Ru2, Theorem 4.1] that

$$\mathrm{char}(A_\infty^\psi) \mid \mathrm{char}((\bar{\mathcal{E}}_\infty/\bar{\mathcal{C}}_\infty)^\psi) \tag{51}$$

for all $\mathbb{Q}_l$-irreducible characters ψ of Δ (see in particular the table at the end of [Ru2, §10]).

Proof of Theorem 1.3 Note first that every subfield N' of N is again contained in some $\mathbb{Z}_l$- extension K'_∞/K'_0:



By the inflation property of Proposition 3.1(d) we we may therefore assume that N/k is cyclic. By Proposition 3.3(c) it is enough to show that $\mathfrak{a}^{(l)}(\psi)^{-1}$ is integral for all non-trivial $\mathbb{Q}_l$- irreducible characters of $\mathrm{Gal}(N/K)$. By the inflation property we may also assume that ψ is faithful. By assumption the hypothesis (46) is satisfied. This implies

$$\mathfrak{a}^{(l)}(\psi) = \frac{\ell_{\mathbb{Z}_l}(\mathrm{cl}^\psi)}{\ell_{\mathbb{Z}_l}((E_N/(\mu_N \times \mathcal{C}_{\mathrm{Ha}})^\psi)}$$

By Lemma 7.5 we have $(\mu_N \times \mathcal{C}_{\mathrm{Ha}})^\psi \subseteq \mathcal{C}_N{}^\psi$ and therefore it suffices to prove

$$\ell_{\mathbb{Z}_l}(\mathrm{cl}_N^\psi) \mid \ell_{\mathbb{Z}_l}((E_N/\mathcal{C}_N)^\psi). \tag{52}$$

This will be a consequence of (51). Consider the canonical embedding $\alpha : E_N \to \prod_{\mathfrak{P}|\mathfrak{p}} \mathcal{O}_{\mathfrak{P}}^*$, where $\mathfrak{p}$ is the fixed prime of k above l. Since the index of U_N in $\prod_{\mathfrak{P}|\mathfrak{p}} \mathcal{O}_{\mathfrak{P}}^*$ is prime to l the map α induces a map

$$\begin{array}{rcl} \tilde{\alpha} : \mathbb{Z}_l \otimes_{\mathbb{Z}} E_N = \mathbb{Z}_l \otimes_{\mathbb{Z}} \alpha^{-1}(U_N) & \longrightarrow & U_N, \\ s \otimes \beta & \longmapsto & \beta^s. \end{array}$$

It follows from [Br, Theorem 2'] that $\tilde{\alpha}$ is injective. (A proof of this is achieved along the lines of proof of Leopoldt's conjecture for abelian extensions $K/\mathbb{Q}$ [Wa, Theorem 5.31]).

Note that

$$\tilde{\alpha}(\mathbb{Z}_l \otimes_{\mathbb{Z}} E_N) = \bar{\mathcal{E}}_N, \quad \tilde{\alpha}(\mathbb{Z}_l \otimes_{\mathbb{Z}} \mathcal{C}_N) = \bar{\mathcal{C}}_N. \tag{53}$$

By hypothesis $\mathfrak{p} \in T$ does not split in K_0/k. Therefore we have $\Delta \subseteq \mathcal{D}_{\mathfrak{p}}$ for all $\mathfrak{p} \in T$. This implies $\mathcal{J}_T^{\psi} = \Lambda^{\psi}$ for all non-trivial $\mathbb{Q}_l$-irreducible characters ψ of Δ. Hence we derive from [Ru2, Corollary 7.9(ii)] and (51)

$$\ell_{\mathbb{Z}_l}(\mathrm{cl}_N^{\psi}) \mid \ell_{\mathbb{Z}_l}((\bar{\mathcal{E}}_N/\bar{\mathcal{C}}_N)^{\psi}).$$

Together with (53) this implies (52).

8 Galois module structure

In this Section we discuss the implications of Theorem 1.1 for the Galois module structure of global units.

Let N/K be a Galois extension of number fields with group G and let S be a large set of places of N. One of the most important invariants attached to the group E_S of S-units of N is the so-called Chinburg class Ω_m. We briefly recall its definition.

For S large we have a Tate sequence

$$0 \longrightarrow E_S \longrightarrow A \longrightarrow B \longrightarrow \Delta S \longrightarrow 0 \tag{54}$$

with A and B cohomologically trivial and whose extension class in $\mathrm{Ext}_{\mathbb{Z}G}(\Delta S, E_S)$ is the canonical class α_3 defined in [Ta1].

Let $\mathrm{cl}(\mathbb{Z}G)$ denote the locally free class group. Every cohomologically trivial $\mathbb{Z}G$-module has a resolution of length at most two by locally free $\mathbb{Z}G$-modules. Therefore, by Schanuel's Lemma, every cohomologically trivial $\mathbb{Z}G$-module C defines a class (C) in $\mathrm{cl}(\mathbb{Z}G)$.

The Chinburg class is then defined by

$$\Omega_m = (A) - (B) \quad \in \mathrm{cl}(\mathbb{Z}G).$$

By [Ch1, Theorem 3.1] the class Ω_m is independent of S and the chosen Tate sequence as long as S is large and the extension class of (54) is the canonical class. The analogy with the tame additive theory of Fröhlich-Taylor [Ch1] suggest the

Conjecture of Chinburg Ω_m equals the root number class W in $\mathrm{cl}(\mathbb{Z}G)$.

For the definition of the root number class W see for example [Fr1]. We only recall the $W = 0$ if the extension N/K is trivial.

Let $\mathcal{M} \subseteq \mathbb{Q}G$ be a maximal $\mathbb{Z}$-order. Tensoring with $\mathcal{M}$ over $\mathbb{Z}G$ from the left induces an epimorphism $\mathrm{cl}(\mathbb{Z}G) \to \mathrm{cl}(\mathcal{M})$ whose kernel is independent of the choice of $\mathcal{M}$. As usual we denote the kernel group by $D(\mathbb{Z}G)$.

We briefly recall the Hom-description of $\mathrm{cl}(\mathbb{Z}G)/D(\mathbb{Z}G) \simeq \mathrm{cl}(\mathcal{M})$ in its ideal theoretic form. Let $F/\mathbb{Q}$ be a finite Galois extension with group Γ such that every representation of G is realizable over F. Let $R(G)$ be the character ring of G. Write I_F for the group of fractional $\mathcal{O}_F$-ideals. Let $I_{\mathbb{Z}}(G)$ be the group of $f \in \mathrm{Hom}_\Gamma(R(G), I_F)$ such that for all irreducible characters χ the ideal $f(\chi)$ is an ideal of $\mathbb{Q}(\chi)$. Define $P_{\mathbb{Z}}(G)$ to be the subgroup of $I_{\mathbb{Z}}(G)$ whose elements are homomorphisms of the form $\chi \mapsto b(\chi)\mathcal{O}_F$ for some Γ-homomorphism $b : R(G) \to F^*$ which satisfies: $b(\chi)$ is totally positive, if χ is a simplectic irreducible character. Then Fröhlich's Hom-description of $\mathrm{cl}(\mathbb{Z}G)$ induces an isomorphism

$$\mathrm{cl}(\mathbb{Z}G)/D(\mathbb{Z}G) \simeq I_{\mathbb{Z}}(G)/P_{\mathbb{Z}}(G).$$

Let $\varphi : \Delta S \to E_S$ be a G-embedding. On the one hand, by [Ch1, Proposition 3.1] the homomorphism $\chi \mapsto q_\varphi(\chi)$ is an element of $I_{\mathbb{Z}}(G)$ and represents $-\Omega_m$ in $\mathrm{cl}(\mathbb{Z}G)/D(\mathbb{Z}G)$. On the other hand, if Stark's conjecture is true for N/K, then $\chi \mapsto A_\varphi(\chi)\mathcal{O}_F$ represents the root number class W in $\mathrm{cl}(\mathbb{Z}G)/D(\mathbb{Z}G)$. Thus the conjecture of Chinburg-Stark would impliy

$$W = \Omega_m \text{ in } \mathrm{cl}(\mathbb{Z}G)/D(\mathbb{Z}G).$$

Let now k be an imaginary quadratic field and let N/k be a finite abelian extension. Let N/K be a subextension of N/k and as before write $G = \mathrm{Gal}(N/K)$. Then Chinburg's conjecture simply reads as $\Omega_m = 0$.

Let $\mathcal{M} \subseteq \mathbb{Q}G$ be the unique maximal $\mathbb{Z}$-order. Let $D_1, \ldots, D_n$ be the divisions of $\widehat{G}$. For $i = 1, \ldots, n$ we choose a character $\chi_i \in D_i$ and thus fix an isomorphism

$$\mathcal{M} \longrightarrow \bigoplus_{i=1}^n \mathcal{O}_{\mathbb{Q}(\chi_i)}, \quad \chi \longmapsto (\chi_i(\lambda))_i \,.$$

This isomorphism induces an isomorphism

$$\mathrm{cl}(\mathcal{M}) \simeq \mathrm{cl}(\mathbb{Z}G)/D(\mathbb{Z}G) \xrightarrow{\psi} \bigoplus_{i=1}^n \mathrm{cl}(\mathcal{O}_{\mathbb{Q}(\chi_i)}).$$

For a number field L and a natural number N we set

$$\mathrm{cl}(\mathcal{O}_L, \frac{1}{N}) := \mathrm{cl}(\mathcal{O}_L)/ < (\mathfrak{p}) : \mathfrak{p} \mid N > .$$

Finally we define $\mathrm{cl}(\mathcal{M}, 1/N)$ such that ψ induces an isomorphism

$$\mathrm{cl}(\mathcal{M}, \frac{1}{N}) \simeq \bigoplus_{i=1}^n \mathrm{cl}(\mathcal{O}_{\mathbb{Q}(\chi_i)}, \frac{1}{N}).$$

Theorem 8.1 *Let N/K be a subextension of an abelian extension N/k. Then*

$$\Omega_m(N/K) = 0 \text{ in } \mathrm{cl}\left(\mathcal{M}, \frac{1}{[N:k]h_k}\right).$$

Proof The proof is immediate from Theorem 1.1 and the above discussion. □

If N/k is a p-extension, then each of the fields $\mathbb{Q}(\chi_i)$ is of the from $\mathbb{Q}(\zeta_{p^r})$ with $r \geq 0$. It follows that $\mathrm{cl}(\mathcal{M}, 1/[N:k]h_k) = \mathrm{cl}(\mathcal{M}, 1/h_k)$, since every prime divisor $\mathfrak{p}$ of p is principal in $\mathbb{Q}(\zeta_{p^r})$. Therefore Corollary 1.2 does not give any additional information.

From Theorem 1.3 we obtain

Theorem 8.2 *Assume the situation of Theorem 1.3. Let N/K be a subextension of N/k. Then*

$$\Omega_m(N/K) = 0 \text{ in } \mathrm{cl}\left(\mathcal{M}, \frac{1}{w_N[K_0:k]}\right)$$

.

This Theorem should be compared to [BH, Theorem 1]. Note however, hat there might be a gap in their proof because it is based on the Euler system method as presented in [Ho] (see the discussion preceeding Theorem 7.6).

References

[Ag] A. Agboola, *Torsion points on elliptic curves and galois module structure*, Invent.Math **123** (1996), 105-122.

[BBC] A. Bayad, W. Bley, Ph. Cassou-Noguès, *Sommes arithmétiques et éléments de Stickelberger*, J.Algebra**179** (1996), 145-190.

[BB] W. Bley, R, Boltje, *Relative Lubin-Tate formal groups and module structure over Hopf orders*, preprint (1997).

[BK] W. Bley, M. Klebel, *An infinite family of elliptic curves and Galois module structure*, preprint (1996).

[Br] A.Brumer, *On the units of algebraic number fields*, Mathematika **14** (1967), 121–124.

[BH] D.Burns, D.Holland, *Chinburg's third invariant for abelian extensions of imaginary quadratic fields*,Proc. London Math.Soc. **74** (1997), 29-51.

[BT] N. Byott, M. J. Taylor, *Hopf orders and Galois module structure.* In: Group rings and class groups, R. W. Roggenkamp, M. J. Taylor (eds.) Birkhäuser, Basel Boston 1992.

[CT] Ph. Cassou-Noguès, M. J. Taylor, *Elliptic functions and rings of integers*, Prog. in Math. 66, Basel-Stuttgart-Boston 1987.

[Ch] Sh.-P. Chan, *Relative Lubin-Tate formal groups and Galois module structure*, Manuscripta Math. **39** (1992), 109–113.

[CS] S. U. Chase, M. E. Sweedler, *Hopf algebras and Galois theory*, Springer Lecture Notes in Mathematics 97, Springer-Verlag 1969.

[CH] L.N.Childs, S.Hurley, *Tameness and local normal bases for objects of finite Hopf algebras*, Trans. Amer. Math. Soc. **298** (1986), 763–778.

[Ch1] T. Chinburg, *On the Galois structure of algebraic integers and S-units*, Invent.Math. **74** (1983), 321–349.

[Co1] J. Coates, *Elliptic curves with complex multiplication and Iwasawa theory*, Bull.London Math.Soc **23** (1991), 321–350.

[Co] J. Cougnard, *Modèle de Legendre d'une courbe elliptique à multiplication complexe et monogénéité d'anneaux d'entiers*, Acta Arith. **54** (1990), 191–212.

[CR] C. Curtis, I. Reiner, *Methods of Representation Theory I*, J. Wiley and Sons, New York.

[Fl] Fleckinger, *Monogénéité de l'anneau des entiers de certains corps de classes de rayons*, Ann. Inst. Fourier (Grenoble) **38** (1988) 17–57.

[Fr1] A. Fröhlich, *Some problems of Galois module structure for wild extensions*, Proc.LMS. **27** (1978), 193–212.

[Fr2] A. Fröhlich, *Galois module structure of Algebraic Integers*, Springer Verlag, Ergebnisse 3 Folge, Band I, 1983.

[GS] C. Goldstein, N. Schappacher, *Séries d'Eisenstein et fonctions L des courbes elliptiques à multiplication complexe*, J. Reine Angew. Math. **327** (1981), 184–218.

[GW] K.W. Gruenberg, A. Weiss, *Galois invariants for units*, Proc.LMS. **70** (1995), 264–284.

[Ha1] H. Hasse, *Über die Klassenzahl abelscher Zahlkörper*, Akademie-Verlag, Berlin 1952.

[Ha2] H. Hasse, *Vorlesungen über Klassenkörpertheorie*, Würzburg 1967.

[Ho] D. Holland, *Chinburg's third invariant in the factorisability defect group*, Can.J.Math. **46** (1994), 324–342.

[Ko] V.A. Kolyvagin, *Euler systems* (1988). In: The Grothendieck Festschrift (Vol.2), Prog. in Math. **86**, Boston, Birkhäuser 1990.

[KL] D. S. Kubert, S. Lang, *Modular units*, Berlin-Heidelberg-New York 1981.

[La1] S. Lang, *Elliptic functions*, Springer Verlag, New York-Berlin-Heidelberg 1987.

[La2] S. Lang, *Algebraic Number Theory*, Springer Verlag, New York-Berlin-Heidelberg 1994.

[Leo] H.W. Leopoldt, *Über die Hauptordnung der ganzen Elemente eines Zahlkörpers*, J. Reine Angew. Math. **286/287** (1962), 54–71.

[Neu] J. Neukirch, *Algebraische Zahlentheorie*, Springer-Verlag, Berlin-Heidelberg- New York 1992.

[Pa] G. Pappas, *On torsion line bundles and torsion points on abelian varieties*, preprint (1996).

[Ra] K. Ramachandra, *Some applications of Kroneckers limit formulas*, Ann. Math. **80** (1964), 104–148.

[R] I. Reiner, *Maximal orders*, Academic Press 1975.

[RW1] J. Ritter, A. Weiss, *A Tate-Sequence for global units*, Compositio Math. **102** (1996), 147-178 .

[RW2] J. Ritter, A. Weiss, *Cohomology of units and L-values at zero*, J. Amer. Math. Soc. **10** (1997), 513–552.

[Ro] G. Robert, *Unités elliptiques*, Bull.Soc.Math.France, Mémoire **36** (1973).

[Ru1] K. Rubin, *Tate-Shafarevich groups and L-functions of elliptic curves with complex multiplication*, Invent.Math. **89** (1987), 527–560.

[Ru2] K. Rubin, *The "main conjectures" of Iwasawa theory for imaginary quadratic fields*, Invent.Math. **103** (1991), 25–68.

[Ru3] K. Rubin, *Stark Units and Kolyvagin's Euler systems*, J. Reine Angew. Math. **425** (1992), 141–154.

[Sch1] R. Schertz, *Konstruktion von Potenzganzheitsbasen in Strahlklassenkörpern über imaginär-quadratischen Zahlkörpern*, J. Reine Angew. Math. **398** (1989), 105–129.

[Sch2] R. Schertz, *Galoismodulstruktur und Elliptische Funktionen*, J. Number Theory **39** (1991), 285–326.

[dS] E. deShalit, *Iwasawa Theory of Elliptic Curves with Complex Multiplication* , Perspectives in Math. Vol. 3, Academic Press 1987.

[Sh] G. Shimura, *Introduction to the arithmetic theory of automorphic functions*, Iwanami Shoten and Princeton University Press 1971.

[Sil1] J. Silverman, *The arithmetic of elliptic curves*, Springer Verlag GTM 106 (1986).

[Sil2] J. Silverman, *Advanced topics in the Arithmetic of Elliptic Curves*, Springer-Verlag, Berlin-Heidelberg-New York 1994.

[ST] A. Srivastav, M. J. Taylor, *Elliptic curves with complex multiplication and Galois module structure*, Invent. Math. **99** (1990), 165-184.

[St] H. M. Stark, *L-functions at* $s = 1$, Adv. in Math. **35** (1980), 197–235.

[Ta1] J.Tate, *The cohomology groups of tori in finite Galois extensions of number fields*, Nagoya Math.J. **27** (1966), 709–719.

[Ta2] J.Tate, *Les Conjectures de Stark sur les Fonctions L d'Artin en* $s = 0$, Progress in Math. 47, Birkhäuser 1984.

[T1] M. J. Taylor, *Hopf Structure and the Kummer Theory of Formal Groups*, J.ReineAngew.Math. **375/376** (1987), 1–11.

[T2] M. J. Taylor, *Mordell-Weil Groups and the Galois Module Structure of Rings of Integers*, Illinois J. Math. **32** (1988), 428–452.

[Wa] L. Washington, *Introduction to cyclotomic fields*, Graduate Texts in Mathematics 83, Springer Verlag, 1982.

[We] A. Weiss, *Multiplicative Galois module structure*, Fields Institute Monographs, AMS, Providence, Rhode Island 1996.

[Wi] A. Wiles, *The Iwasawa conjecture for totally real fields*, Annals of Math. **131** (1990), 555–565.