Journal de Théorie des Nombres
de Bordeaux **11** (1999), 269–305

Lubin-Tate formal groups and module structure over Hopf orders

par Werner BLEY et Robert BOLTJE

Résumé. Ces dernières années les ordres de Hopf ont joué dans des situations diverses un rôle important dans l'étude de la structure des module galoisiens en géométrie arithmétique. Nous introduisons ici un cadre qui rend compte des situations précédentes, et nous étudions les propriétés des algèbres de Hopf dans ce contexte général. Nous insistons en particulier sur le rôle des résolvantes dans les calculs explicites. Nous illustrons cette étude en appliquant nos résultats à la détermination de la structure de module de Hopf de l'anneau des entiers d'une extension de Lubin-Tate relative.

Abstract. Over the last years Hopf orders have played an important role in the study of integral module structures arising in arithmetic geometry in various situations. We axiomatize these situations and discuss the properties of the (integral) Hopf algebra structures which are of interest in this general setting. In particular, we emphasize the role of resolvents for explicit computations. As an illustration we apply our results to determine the Hopf module structure of the ring of integers in relative Lubin-Tate extensions.

1. Introduction

In this article we axiomatize the situation considered in Taylor's article [T2].

1.1. 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 via group automorphisms.

Manuscrit reçu le 14 juillet 1997.

- Γ is a finite set on which G and Ω act from the left such that G acts simply transitive (thus $|G| = |\Gamma|$) with ${}^{\omega}({}^{g}\gamma) = {}^{({}^{\omega}g)}({}^{\omega}\gamma)$ 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 (like ${}^{\omega}g$ 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.

There is a variety of natural examples for the general situation described in 1.1.

1.2. **Examples.** 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.

(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 K as in 1.1, 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 $\mathcal{O}_M$, where F is a finite extension of a quadratic imaginary number field M. For any integral ideal $\mathfrak{a} \subseteq \mathcal{O}_M$ write $E[\mathfrak{a}]$ for the subgroup of points of $E(\bar{F})$ that are annihilated by all elements $a \in \mathfrak{a}$. For $x \in \mathcal{O}_M$ let $[x] \in \mathrm{End}(E)$ be the corresponding endomorphism of E. Let, for simplicity, $(a) = \mathfrak{a} \subseteq \mathcal{O}_M$ 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 [A], [ST] and [T2].

(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 $r, m \in \mathbb{N}$, set $K := F_r$, $G := G_m$, choose $\beta \in G_r \smallsetminus G_{r-1}$, 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],[By], [T1], [By], and [CL].

1.3. Following [T2] we define in the situation described in 1.1

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

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

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

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 5.2 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 5.3.

1.4. 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 $L=K$.

1.5. **Remark.** (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 $\Omega/\Omega_L \xrightarrow{\cong} G$, 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 $C \xrightarrow{\cong} L$ and $\mathcal{C} \xrightarrow{\cong} \mathcal{O}_L$ of L- (resp. $\mathcal{O}_L$-) algebras.

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

1.6. If one assumes suitable Kummer conditions in Examples 1.2 (a), (d) and (e), then $A = KG$. Moreover, in many interesting examples Ω acts transitively on Γ and, in the notation of Remark 1.5 (a), the fixed field L of the stabilizer $\mathrm{stab}_\Omega(\gamma_0)$ is an abelian Galois extension of K such that the bijection $\mathrm{Gal}(L/K) = \Omega/\Omega_L \xrightarrow{\cong} G$ is a group isomorphism (see e.g. Lemma 6.1). 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. Then, there are results due to Cassou-Noguès, Schertz, and Taylor, stating that $\mathcal{O}_L$ is free over its associated order in KG, see e.g. [CT, Ch. X, Ch. XI], [S]. In Section 6 we will study a slight generalization of Example 1.2 (e), namely relative Lubin-Tate extensions. We will show that also without any Kummer condition, the maximal order $\mathcal{C} \cong \mathcal{O}_L$ is a free rank one module over its associated order $\mathcal{A}^{\mathrm{ass}}$ (see Theorem 6.11). But note that in general the algebra A is not the group ring KG. Combining ideas of [T1] and [T2] we will give an explicit description of $\mathcal{A}^{\mathrm{ass}}$ as the Cartier dual of the $\mathcal{O}_K$-Hopf order which represents the $\mathcal{O}_K$-group scheme of π^m-torsion on $\mathcal{F}$ (see Proposition 6.5 and Corollary 6.9). In contrast to the methods used in [CT, Ch. X] the main tool for our proof of Theorem 6.11 will be the factorization of a suitable resolvent function which takes values in $\mathcal{O}_{\bar{F}}[[X]]$ (see Theorem 6.10). This will be of great importance for further applications of these local results to fields obtained by the division of points on elliptic curves as in Example 1.2 (d). These examples are dealt with by the first author in his habilitation thesis [B].

1.7. The article is arranged in the following way. Sections 1–5 are devoted to the general situation as stated in 1.1. In more details, the sections 2 and 3 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 4 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 $d_{\mathcal{B}_L}$ of $\mathcal{B}_L$ (resp. $d_{\mathcal{A}_L}$ of $\mathcal{A}_L$) over $\mathcal{O}_L$ are trivial, see Proposition 4.6 (resp. Proposition 4.8). 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 4.3. Section 5 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 5.3.

Finally, in Section 6, we apply the results from Sections 1–5, in particular the index formula of Section 5, to the Example 1.2 (e).

2. Forms of group algebras

We assume the situation defined in 1.1 and the notation introduced in Section 1.

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 H 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, then 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 $g \in G$.

2.1. **Lemma.** *Let $K \subseteq L \subseteq \bar{K}$ be an intermediate field, and let $g_1, \dots, g_r \in G$ be a set of representatives for the Ω_L-orbits of G. For each $i \in \{1, \dots, r\}$ let L_i be the fixed field of* $\mathrm{stab}_{\Omega_L}(g_i) \leqslant \Omega_L$*, and let $x_{i,1}, \dots, x_{i,r_i}$ 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 $i \in \{1, \dots, r\}$ 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 $\mathcal{A}_L^0$.*

(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*

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

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 $i\in\{1,\dots,r\}$. Moreover, for each $i\in\{1,\dots,r\}$ 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 assertion 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 block diagonal matrix with r blocks indexed by the Ω_L-orbits of G, where the i-th block is given by

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

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. □

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

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

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

3. Duality

We assume the situation described in 1.1 and the notation from Section 1.

It is well-known that the Hopf algebra 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

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

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

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

3.1. **Lemma.** *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*

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

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 $i \in \{1,\dots,r\}$, the elements $x_{i,1},\dots,x_{i,r_i}$ form an $\mathcal{O}_L$-basis of $\mathcal{O}_{L_i}$ then the elements $b_{i,j}$, $1 \leqslant i \leqslant r$, $1 \leqslant j \leqslant r_i$, 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*

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

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*

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

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

$$\begin{tikzcd}
M \otimes_L B_L \arrow[r, "\psi_L^M"] \arrow[d, "\omega\otimes\omega"'] & B_M \arrow[d, "\omega"] \\
\omega(M) \otimes_{\omega(L)} B_{\omega(L)} \arrow[r, "\psi_{\omega(L)}^{\omega(M)}"] & B_{\omega(M)}
\end{tikzcd}
\qquad
\begin{tikzcd}
N \otimes_M M \otimes_L B_L \arrow[r, "N\otimes\psi_L^M"] \arrow[d, "\mathrm{can}\otimes B_L"'] & N \otimes_M B_M \arrow[d, "\psi_M^N"] \\
N \otimes_L A_L \arrow[r, "\psi_L^N"] & B_N
\end{tikzcd}$$

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 $\mathbf{A} \otimes_{\bar{K}} \mathbf{B}$. Moreover, 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 $i \in \{1,\dots,r\}$, 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 $\lambda_i \in L_i$, $i = 1,\dots,r$, 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 well-defined and 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). □

4. Indices and Hopf structures

We assume the situation described in 1.1 and the notation from Section 1.

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 $\mathfrak{p}_1, \ldots, \mathfrak{p}_t$ of $\mathcal{O}_L$ if $R/\mathfrak{p}_1, \ldots, R/\mathfrak{p}_t$ 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

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

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

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

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

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

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 3.1. 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 $\mathcal{O}_L$.

4.1. **Lemma.** *With the notation of Lemma 2.1 and Lemma 3.1 one has*

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

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

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

Proof. The inclusion $\mathcal{A}_L^\circ \subseteq \mathcal{B}_L^*$ is clear from Lemma 4.1. From the definition of $\mathcal{A}_L^\circ$ and from Lemma 4.1 we have

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

□

We remark that, 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 $L_1, \dots, L_r$ and $\hat{L}_1, \dots, \hat{L}_s$ 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.

4.3. **Lemma.** *Let G be abelian. Then*

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

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 $(\mathcal{A}_L^\circ)_\mathfrak{p}$ 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

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

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, $[\mathcal{A}_L : \mathcal{A}_L^\circ]_{\mathcal{O}_L}\mathcal{O}_{L'}$ is the quotient of the squared order ideals

$$\left[\rho_{L'}(\mathcal{A}_{L'}) : (\rho_{L'} \circ \phi_L^{L'})(\mathcal{O}_{L'} \otimes_{\mathcal{O}_L} \mathcal{A}_L^\circ)\right]^2_{\mathcal{O}_{L'}} \tag{4}$$

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 squared 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 $y_{k,1}, \dots , y_{k,s_k}$ is an $\mathcal{O}_L$-basis of $\mathcal{O}_{\hat{L}_k}$ for each $k = 1, \dots , s$. 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

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

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 $x_{i,1}, \dots, x_{i,r_i}$ is an $\mathcal{O}_L$-basis of $\mathcal{O}_{L_i}$ for each $i \in \{1, \dots, r\}$. 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 $i = 1, \dots, r$, the i-th block given by

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

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. $\square$

4.4. 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 $a_1, \ldots, a_n$ 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 $i = 1, \ldots, n$ with $\alpha_{i,h} \in E$, and we consider the matrix

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

together with its inverse

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

Then we have the following criterion:

4.5. **Lemma.** *Keeping the notation of 4.4, the following assertions are equivalent:*

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

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

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 $i \in \{1, \ldots, n\}$, we have $\Delta(a_i) \in \mathcal{A} \otimes_R \mathcal{A}$ if and only if $\gamma_{j,j'}^{(i)} \in R$ for all $j, j' \in \{1, \ldots, n\}$. 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 $\gamma^{(i)}_{j,j'}$ are uniquely determined by the system of linear equations

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

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

$$\gamma^{(i)}_{j,j'} = \sum_{h \in H} \alpha_{i,h} \beta_{h,j} \beta_{h,j'},$$

and the result follows. □

In the following proposition we apply Lemma 4.5 to the $\mathcal{O}_L$-order $\mathcal{A}^\circ_L$ in A_L.

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

Proof. Clearly, $\mathcal{A}^\circ_L$ is stable under the antipode of A_L. The inclusion $\Delta(\mathcal{A}^\circ_L) \subseteq \mathcal{A}^\circ_L \otimes_{\mathcal{O}_L} \mathcal{A}^\circ_L$ 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 $\mathcal{A}^\circ_L$, and, in the notation of 4.4, the coefficient matrix S is a block diagonal matrix, the blocks indexed by $i = 1, \dots, r$, and the i-th block given by

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

If $x^*_{i,1}, \dots, x^*_{i,r_i} \in L_i$ is a dual basis of $x_{i,1}, \dots, x_{i,r_i}$ 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 i-th block

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

Now, taking into account the block diagonal structure of S and T, Lemma 4.5 states that $\Delta(\mathcal{A}^\circ_L) \subseteq \mathcal{A}^\circ_L \otimes_{\mathcal{O}_L} \mathcal{A}^\circ_L$ if and only if

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

for all $i \in \{1, \dots, r\}$ and all $j', j'' \in \{1, \dots, r_i\}$. But since $x^*_{i,j}$, $j = 1, \dots, r_i$, form an $\mathcal{O}_L$-basis of $\mathcal{D}^{-1}_{L_i/L}$, the condition in (9) holds for given $i \in \{1, \dots, r\}$ and all $j', j'' \in \{1, \dots, r_i\}$ 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. □

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

Proof. The equivalence of (i) and (ii) is the content of Proposition 4.6. The statements (ii) and (iii) are equivalent by Corollary 4.2 which asserts that $[\mathcal{B}_L^* : \mathcal{A}_L^\circ] = d_{B_L}$. 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 4.1 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 $\mathcal{A}_L^\circ$ is the smallest $\mathcal{O}_L$-Hopf order in A_L. □

4.8. **Proposition.** *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 4.6 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 of 4.4 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 $k = 1, \ldots, s$ and whose k-th block is given by

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

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

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 for 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 4.5 states that $\Delta(\mathcal{A}_L) \subseteq \mathcal{A}_L \otimes_{\mathcal{O}_L} \mathcal{A}_L$ if and only if

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

for all (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

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

since ${}^{\omega'}\chi_{k'}\,{}^{\omega''}\chi_{k''} = 1$ if and only if $\omega'' = \omega'\kappa$. The elements $\kappa(y_{k'',1}), \dots, \kappa(y_{k'',s_{k''}})$ 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 $k' \in \{1,\dots,s\}$. Thus, $d_{A_L} = \mathcal{O}_L$. □

5. Some A-modules and resolvents

We still assume the situation described in 1.1 and the notation from Section 1.

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 $\mathcal{A}_L^{\circ}$-module by restriction.

Similar to Lemma 3.1 for the algebra $\mathbf{B}$ we have the following lemma for $\mathbf{C}$.

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

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

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

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

of $\mathcal{O}_L$-algebras.

(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

$$\begin{array}{ccc} M \otimes_L C_L & \xrightarrow{\pi_L^M} & C_M \\ {\scriptstyle \omega\otimes\omega}\downarrow & & \downarrow{\scriptstyle \omega} \\ \omega(M) \otimes_{\omega(L)} C_{\omega(L)} & \xrightarrow{\pi_{\omega(L)}^{\omega(M)}} & C_{\omega(M)} \end{array} \qquad \begin{array}{ccc} N \otimes_M M \otimes_L C_L & \xrightarrow{N\otimes\pi_L^M} & N \otimes_M C_M \\ {\scriptstyle \mathrm{can}\otimes C_L}\downarrow & & \downarrow{\scriptstyle \pi_M^N} \\ N \otimes_L C_L & \xrightarrow{\pi_L^N} & C_N \end{array}$$

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

Proof. All assertions are proved in a similar way as the analogous assertions of Lemma 3.1. □

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].

5.2. **Proposition.** *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 5.1 (v) to reduce the assertion to the case $L = \bar{K}$. Moreover, by Lemma 2.1 (ii) and Lemma 5.1 (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 that, in the situation we consider in Section 6, $\mathcal{C}_L$ is free over $\mathcal{A}_L^{\mathrm{ass}}$. In the proof we make use of the *resolvent*

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

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 5.1 we have $d_{C_L} = \prod_{m=1}^{t} d_{\tilde{L}_m/L}$.

5.3. **Proposition.** *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, B_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*

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

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

$$\hat{a}_{k,l} = \sum_{\omega \in \Omega_L/\mathrm{stab}_{\Omega_L}(\chi_k)} \omega(y_{k,l})\, {}^{\omega}e_{\chi_k} \qquad (1 \leqslant k \leqslant s,\ 1 \leqslant l \leqslant s_k) \tag{12}$$

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

$$\big((f \cdot \hat{a}_{k,l})(\gamma)\big)_{\gamma \in \Gamma} \in \prod_{\gamma \in \Gamma} L' \tag{13}$$

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 entries 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 $M = M_1 M_2$, where M_1 is a block diagonal matrix, the blocks $M_{1,k}$ indexed by $k = 1, \dots, s$, with

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

and where

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

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,

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

by (7). Thus,

$$\det(M)^2\mathcal{O}_{L'} = d_{A_L}|G|^{-|G|}\prod_{\chi\in\hat{G}}(f,\chi)^2_{\gamma_0}\mathcal{O}_{L'}\,. \tag{14}$$

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 $y_{k,1},\dots,y_{k,s_k}$ is an $\mathcal{O}_L$-basis of $\mathcal{O}_{\hat{L}_k}$, for each $k = 1,\dots,s$, then the elements (12) form an $\mathcal{O}_L$-basis of $\mathcal{A}_L$, and the elements in (13) 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

(15)

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

Moreover, we already know from Proposition 4.3 that

$$[f\cdot\mathcal{A}_L : f\cdot\mathcal{A}_L^{\circ}]^2_{\mathcal{O}_L} = [\mathcal{A}_L : \mathcal{A}_L^{\circ}]^2_{\mathcal{O}_L} = d_{B_L}d_{A_L}^{-1}|G|^{|G|}\,. \tag{16}$$

Now, it suffices to show that

$$\big[\tau(\mathcal{C}_{L'}) : (\tau_{L'}\circ\pi_L^{L'})(\mathcal{O}_{L'}\otimes_{\mathcal{O}_L}\mathcal{C}_L)\big]^2_{\mathcal{O}_{L'}} = d_{C_L}\mathcal{O}_{L'}\,, \tag{17}$$

since then, dividing the product of (15) and (16) by (17) yields the result.

Let γ_m, $\tilde{L}_m$, $z_{m,n}$, and $c_{m,n}$ be given as in Lemma 5.1 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 $\tau_{L'}(\mathcal{C}_{L'}) = \prod_{\gamma \in \Gamma} \mathcal{O}_{L'}$ 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 (17), and the proof is complete. $\square$

As an immediate consequence of Proposition 5.3 we obtain:

5.4. **Corollary.** *In the situation of Proposition 5.3 with $f \in C_L$ 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 $\tilde{\mathcal{A}}_L \subset \mathcal{A}_L^{\mathrm{ass}}$ and 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, $\tilde{\mathcal{A}}_L = \mathcal{A}_L^{\mathrm{ass}}$.

6. 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 write ϕ for 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

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

For any power series g in one or more indeterminates over $\mathcal{O}_{F'}[[X]]$ 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

6.1. **Proposition.** ([dS, Ch.I, (1.5)]) *Let $f(X) = \pi_1 X + \dots$, $g(X) = \pi_2 X + \dots$ 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*

$$\text{(i)} \qquad [a]_{f,g} \equiv aX \mod X^2,$$

$$\text{(ii)} \qquad [a]_{f,g} \circ f = g \circ [a]_{f,g}.$$

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 $h(X) = \pi_3 X + \dots \in F_\xi$ 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 $[a]_{f,f}$. For $f(X) = \pi' X + \dots \in F_\xi$ and $i \geq 0$, we put $f^{(i)} = f^{\phi^{i-1}} \circ \dots \circ f^\phi \circ f$. Then $f^{(i)} \in \mathrm{Hom}(\mathcal{F}_f, \mathcal{F}_{f^{\phi^i}})$ and if $v_F(\xi) = d$, then $f^{(d)} = [\xi]_f \in \mathrm{End}(\mathcal{F}_f)$. Moreover, for $\alpha \in \mathcal{O}_{F'}$ we write $\alpha^{(i)} = \alpha^{\phi^{i-1}} \cdots \alpha^\phi \cdot \alpha$. It 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 $f(X) = \pi' X + \dots \in F_\xi$. 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 Sections 1–5. We fix integers $r, m \geqslant 1$ 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 in 1.1, 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 Sections 1–5 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.

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 $L = K(\gamma_0)$.

6.2. **Lemma.** *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 $u(X)\in\mathcal{O}_K[[X]]^\times$. 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 $g\in G$. □

Of course, the map τ of Lemma 6.2 is an isomorphism of K-algebras for arbitrary $m\geqslant 1$. The map in (c), however, is then no longer a homomorphism, but still a bijection. Via τ we can endow L with the structure of an A-module. But for $m>r$, this does not coincide with the usual Galois module structure, since A is no longer the group ring KG. At least in the context of this paper, this new module structure seems to be the more natural one. In the following we shall always identify C and L via τ; 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.

6.3. Proposition. ([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] 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

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

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

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

6.4. **Lemma.** *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. 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:

$$b \in D^{-1}(\mathcal{B}^{\mathrm{gs}}) \Longleftrightarrow \sum_{i=0}^{q^m-1} a_i \sum_{g \in G} g^{i+j} \in \mathcal{O}_K \text{ for } j = 0, \dots, q^m - 1. \tag{18}$$

From Propostion 6.3 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 (18) implies 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 6.3 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 $D^{-1}(\mathcal{B}^{\mathrm{gs}}) \subseteq \frac{1}{\pi'^{(m)}}\mathcal{B}^{\mathrm{gs}}$. □

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

$$\sigma_i := \frac{1}{\pi'^{(m)}} \sum_{g \in G} x_g^i (g - g_0)\,. \tag{19}$$

It is immediate that these elements are Ω-invariant.

6.5. **Proposition.** *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. For the proof of the first equality 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

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

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

$$\eta : \mathrm{Hom}_{\mathcal{O}_K}(\mathcal{B}^{\mathrm{gs}}, \mathcal{O}_K) \longrightarrow \mathcal{A}^{\mathrm{gs}}, \quad h \longmapsto \sum_{g \in G} a_g g,$$

if $h(b) = \sum_{g \in G} a_g b(g), \forall b \in \mathcal{B}^{\mathrm{gs}}$. 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 first equality in the proposition follows from Lemma 6.4. In order to prove the second one we first define $l \in \mathcal{B}^{\mathrm{gs}}$ by

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

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

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

It immediately follows that the set $\{\bar{1}, \bar{X}, \dots, \bar{X}^{q^m-2}, l\}$ also forms an $\mathcal{O}_K$-basis of $\mathcal{B}^{\mathrm{gs}}$. Now the second equality is an immediate consequence of the first one and Lemma 6.3. $\square$

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.

6.6. **Lemma.** ([CT, Ch. X, Lemma 3.5] *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

$$c_{\gamma_0^k} \cdot \sigma_i \in \mathcal{C} \tag{20}$$

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

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

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

$$\tau(c_{\gamma_0^k} \cdot \sigma_i) = \sum_{s=0}^{\infty} \alpha_0^s \cdot \frac{1}{\pi'(m)} \sum_{g \in G} g^i a_s(g).$$

Since the right-hand term is integral by Proposition 6.3, this establishes (20). $\square$

From Lemma 6.6 we deduce the following corollary which may be viewed as a generalization of the trace relations of Proposition 6.3.

6.7. **Corollary.** *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 6.6, 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 $\frac{1}{\pi'(m)} \sum\limits_{g \in G} g^i \chi(g)$ from Proposition 6.3. □

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 tameness 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 (19).

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

6.9. **Corollary.** *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 $\mathcal{A}^{\mathrm{ass}} = \mathcal{A}^{\mathrm{gs}}$. □

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 1.2(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

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

6.10. **Theorem.** *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

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

This completes the proof, since by Corollary 6.7 the terms in brackets are divisible by $\pi'^{(m)}$. □

Consider the map

$$c\colon \Gamma \to \bar{F}\,, \quad \gamma \mapsto \frac{f^{(m)}(\gamma)}{\gamma}\,. \tag{21}$$

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 5, we have the following relation:

$$\begin{aligned} (c,\chi)_{\gamma_0} &= \sum_{g\in G} c({}^g\gamma_0)\,\chi(g^{-1}) = \sum_{g\in G} \frac{f^{(m)}(g +_f \gamma_0)}{g +_f \gamma_0}\,\chi(g^{-1}) \\ &= \sum_{g\in G} \frac{f^{(m)}(\gamma_0)}{g +_f \gamma_0} = R_\chi(\gamma_0)\,. \end{aligned} \tag{22}$$

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

6.11. **Theorem.** (a) *The $\mathcal{A}^{\text{ass}}$-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 $\mathcal{A}^{\text{ass}}$-basis of $\mathcal{C}$. In particular,*

$$\mathcal{C} = c \cdot \mathcal{A}^{\text{ass}} \tag{23}$$

with $c = c_\theta$ from (21).

Proof. (a) Let L' be a splitting field for A, B and C. Then, by Corollary 5.4 it suffices to show that

$$[\mathcal{A}^{\text{ass}} : \mathcal{A}^\circ]^2_{\mathcal{O}_K} d_C \mathcal{O}_{L'} = d_B \prod_{\chi\in\hat{G}} (c,\chi)^2_{\gamma_0} \mathcal{O}_{L'}\,, \tag{24}$$

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

$$[\mathcal{A}^{\mathrm{ass}} : \mathcal{A}^\circ]^2 = d_B \pi^{mq^m} . \tag{25}$$

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

$$[\mathcal{O}_{L'} \otimes_{\mathcal{O}_K} \mathcal{A}^{\mathrm{ass}} : \mathcal{O}_{L'} G]^2_{\mathcal{O}_{L'}} = \pi^{mq^m} \mathcal{O}_{L'} \tag{26}$$

and

$$[\mathcal{O}_{L'} G : \mathcal{O}_{L'} \otimes_{\mathcal{O}_K} \mathcal{A}^\circ]^2_{\mathcal{O}_{L'}} = d_B . \tag{27}$$

Equation (27) follows immediately if we recall from Lemma 2.1 that the elements

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

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 $\mathcal{O}_{K_i}$, with K_i being the fixed field of $\mathrm{stab}_\Omega(g_i)$.

The proof of (26) 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 $\{1 \otimes_{\mathcal{O}_K} g_0\} \cup \{1 \otimes_{\mathcal{O}_K} \sigma_i \mid i = 0, \dots , q^m - 2\}$ 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 $j = 1, \dots, N$. 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 (26).

(b) It follows from Theorem 6.10 together with (22) 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 $x \in L^\times$ 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

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

Together with (23) 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. □

To conclude we have a closer look at the associated order when $F = \mathbb{Q}_p$.

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

Proof. From Lemma 4.3 we know that

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

whereas from (25) 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 $d_A = \mathcal{O}_K$. □

References

[A] A. Agboola, *Torsion points on elliptic curves and galois module structure.* Invent. Math. **123** (1996), 105–122.

[B] W. Bley, *Elliptic curves and module structure over Hopf orders* and *The conjecture of Chinburg-Stark for abelian extensions of a quadratic imaginary field.* Habilitation Thesis Universität Augsburg, Report des Instituts für Mathematik der Universität Augsburg No. **396**, 1998.

[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.

[By] N. Byott, *Associated orders of certain extensions arising fom Lubin-Tate formal groups.* J. Théor. Nombres Bordeaux **9** (1997),449–462.

[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.

[CL] Sh.-P. Chan, C.-H. Lim, *The associated orders of rings of integers in Lubin-Tate division fields over the p-adic number field*. Illinois J. Math. **39** (1995), 30–38.

[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.

[dS] E. deShalit, *Iwasawa Theory of Elliptic Curves with Complex Multiplication* . Perspectives in Math. **Vol. 3**, Academic Press, 1987.

[R] I. Reiner, *Maximal orders.*, Academic Press, 1975.

[S] R. Schertz, *Galoismodulstruktur und Elliptische Funktionen*. J. Number Theory **39** (1991), 285–326.

[ST] A. Srivastav, M.J. Taylor, *Elliptic curves with complex multiplication and Galois module structure*. Invent. Math. **99** (1990), 165–184.

[T1] M. J. Taylor, *Hopf Structure and the Kummer Theory of Formal Groups*. J. Reine Angew. 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.

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

Robert Boltje
Department of Mathematics
University of California
Santa Cruz, CA 95064
USA
E-mail : boltje@math.ucsc.edu