Lubin-Tate formal groups and module structure over Hopf orders

Journal de Théorie des Nombres de Bordeaux, tome 11, n° 2 (1999), p. 269-305

<http://www.numdam.org/item?id=JTNB_1999__11_2_269_0>
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 \( \Omega := \text{Gal}(\bar{K}/K) \) the absolute Galois group of \( K \).
- \( G \) is a finite group on which \( \Omega \) acts from the left via group automorphisms.
\( \Gamma \) is a finite set on which \( G \) and \( \Omega \) act from the left such that \( G \) acts simply transitive (thus \( |G| = |\Gamma| \)) with \( \omega'(g) = (\omega g)(\omega') \) for all \( \omega \in \Omega \), \( g \in G \), and \( \gamma \in \Gamma \) (the last condition just means that the semidirect product \( G \times \Omega \) acts on \( \Gamma \)).

We always write the action of \( \omega \in \Omega \) on \( G \) and \( \Gamma \) exponentially from the left (like \( \omega g \) and \( \omega \gamma \) for \( g \in G \) and \( \gamma \in \Gamma \)) and its action on \( \overline{K} \) as \( \omega(x) \) for \( x \in \overline{K} \).

For any intermediate field \( K \subseteq L \subseteq \overline{K} \), we set \( \Omega_L := \text{Gal}(\overline{K}/L) \subseteq \Omega \), and denote by \( O_L \) the integral closure of \( O \) 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 \( \mu_n, n \in \mathbb{N} \), 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 \( \Gamma := \{ x \in \overline{K} \mid x^m = \beta \} \). Then \( \Gamma \subseteq \mu_{r+m} \) and \( G \) acts on \( \Gamma \) 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 \( \Gamma := \{ x \in \overline{K} \mid x^m = \beta \} \). Then \( G \) acts on \( \Gamma \) by multiplication.

(c) For \( K \) as in 1.1, let \( L/K \) be a finite Galois extension with Galois group \( G \), and let \( \Omega \) act on \( G \) by conjugation. Moreover, let \( \gamma_0 \in L \) be a primitive element \( (L = K(\gamma_0)) \), and let \( \Gamma \) be the set of Galois conjugates of \( \gamma_0 \).

(d) Let \( E/F \) be an elliptic curve with complex multiplication by \( O_M \), where \( F \) is a finite extension of a quadratic imaginary number field \( M \). For any integral ideal \( a \subseteq O_M \) write \( E[a] \) for the subgroup of points of \( E(\overline{F}) \) that are annihilated by all elements \( a \in a \). For \( x \in O_M \) let \( [x] \in \text{End}(E) \) be the corresponding endomorphism of \( E \). Let, for simplicity, \( (a) = a \subseteq O_M \) be a principal ideal and set \( G := E[a] \). For \( P \in E(\overline{F}) \) define \( K := F(P) \) and \( \Gamma := \{ Q \in E(\overline{F}) \mid [a](Q) = P \} \). Then \( G \) acts on \( \Gamma \) 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 \( p_F = (\pi) \) be the maximal ideal of the ring \( O_F \) of integers in \( F \).

Let \( F \) be a Lubin-Tate formal group attached to a Lubin-Tate power series \( f(X) \in O_F[[X]] \). Let \([-\cdot] : O_F \to \text{End}(F) \) be the usual ring isomorphism with \([\pi](X) = f(X) \). For \( n \in \mathbb{N} \) set \( G_n := \{ x \in p_F \mid [\pi^n](x) = 0 \} \), the subgroup of \( \pi^n \)-torsion points in the \( O_F \)-module \( p_F \) endowed with the \( F \)-group law and the \( O_F \)-action \( ax := [a](x) \) for \( a \in O_F \) and \( x \in p_F \), 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 \( \beta \in G_r \setminus G_{r-1} \), and set \( \Gamma := \{ x \in p_F \mid [\pi^m](x) = \beta \} \subseteq G_{m+r} \). Then \( G \) acts on \( \Gamma \) 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
\[ A := \bar{K}G, \quad B := \text{Map}(G, \bar{K}), \quad C := \text{Map}(\Gamma, \bar{K}), \]
the group algebra of \( G \) over \( \bar{K} \), the set of maps from \( G \) and from \( \Gamma \) to \( \bar{K} \), respectively. Then \( A \) is a \( \bar{K} \)-Hopf algebra, \( B \) is its \( \bar{K} \)-dual Hopf algebra, \( C \) is a \( \bar{K} \)-algebra and a right \( A \)-module by the \( \bar{K} \)-linear extension of the action \( (f \cdot g)(\gamma) := f(\gamma g) \) of \( G \) on \( C \), where \( g \in G, f \in C, \) and \( \gamma \in \Gamma \).

Note that \( \Omega \) acts on \( A, B, \) and \( C \) by

\[
\omega\left(\sum_{g \in G} \lambda_g g\right) := \sum_{g \in G} \omega(\lambda_g) g, \quad (\omega b)(g) := \omega(b(\omega^{-1} g)), \quad (\omega f)(\gamma) := \omega(f(\omega^{-1} \gamma)),
\]
for \( \omega \in \Omega, \lambda_g \in \bar{K}, \ b \in B, \ g \in G, \ f \in C, \) and \( \gamma \in \Gamma \). This is an action via \( \bar{K} \)-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 \( \Omega_L = \text{Gal}(\bar{K}/L) \) for any intermediate field \( K \subseteq L \subseteq \bar{K} \):

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

We omit the index \( L \) for \( L = K \). Then \( A_L \) and \( B_L \) are \( L \)-Hopf subalgebras of \( A \) and \( B \), and they are \( L \)-dual to each other. Moreover, \( C_L \) is an \( L \)-algebra and an \( A_L \)-module by restriction of the \( A \)-action on \( C \). 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 \((f, \chi) \in \hat{K}, \) for \( f \in C \) and \( \chi \in \hat{G} := \text{Hom}(G, \bar{K}^\times) \), 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

\[ A_L, \quad B_L = \text{Map}(G, \mathcal{O}_L)^{\Omega_L}, \quad C_L := \text{Map}(\Gamma, \mathcal{O}_L)^{\Omega_L}, \]
of \( A_L, B_L, \) and \( C_L, \) respectively. Moreover, for arbitrary \( G, \) set

\[ A_L^\circ := (\mathcal{O}_L G)^{\Omega_L}, \]

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

\[ A_L^{\text{ass}} := \{ a \in A_L \mid C_L \cdot a \subseteq C_L \} \]
of \( C_L \) in \( A_L \), which contains \( A_L^\circ \). If \( G \) is abelian, then we have inclusions

\[ A_L^\circ \subseteq A_L^{\text{ass}} \subseteq A_L. \]

Again, we omit the index \( L \) in \( A_L, B_L, C_L, A_L^\circ, A_L^{\text{ass}}, \) if \( L = K \).
1.5. Remark. (a) Suppose that the action of $\Omega$ on $\Gamma$ is transitive. Fix an element $\gamma_0$ and denote its stabilizer by $\Omega_L$ 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 $\omega \gamma_0 = \gamma_0$. Moreover, associating to $f \in C$ the value $f(\gamma_0) \in \bar{K}$, defines isomorphisms $C \xrightarrow{\cong} L$ and $C \xrightarrow{\cong} \mathcal{O}_L$ of $L$- (resp. $\mathcal{O}_L$-) algebras.

(b) The absolute Galois group $\Omega$ 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 $\Omega$ acts transitively on $\Gamma$ and, in the notation of Remark 1.5 (a), the fixed field $L$ of the stabilizer $\text{stab}_{\Omega}(\gamma_0)$ is an abelian Galois extension of $K$ such that the bijection $\text{Gal}(L/K) \xrightarrow{\cong} G$ 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 $C \cong \mathcal{O}_L$ is a free rank one module over its associated order $A^{\text{ass}}$ (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 $A^{\text{ass}}$ as the Cartier dual of the $\mathcal{O}_K$-Hopf order which represents the $\mathcal{O}_K$-group scheme of $\pi^m$-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 $\mathcal{O}_P[[X]]$ (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 $A_L^0$ (resp. $A_L$ if $G$ is abelian) is an $\mathcal{O}_L$-Hopf order in $A_L$ if and only if the discriminant ideals $d_B_L$ of $B_L$ (resp. $d_{A_L}$ of $A_L$) 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 \([A_L : A^0_L]_{O_L}\) 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 \([C_L : f \cdot A^0_L]_{O_L}\) in terms of \(d_{B_L}\), \(d_{C_L}\), and the resolvents \((f, \chi), \chi \in \hat{G}\), 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 \(A\) and its subalgebras \(A_L = A^\Omega_L\), 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 \(A\) 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 \(g_1, \ldots, g_r \in G\) be a set of representatives for the \(\Omega_L\)-orbits of \(G\). For each \(i \in \{1, \ldots, r\}\) let \(L_i\) be the fixed field of \(\text{stab}_{\Omega_L}(g_i) \leq \Omega_L\), and let \(x_{i,1}, \ldots, x_{i,r_i}\) be an \(L\)-basis of \(L_i\). Finally, for \(1 \leq i \leq r\) and \(1 \leq j \leq r_i\), set

\[
    a_{i,j} := \sum_{\omega \in \Omega_L/\text{stab}_{\Omega_L}(g_i)} \omega(x_{i,j}) \omega g_i \in A,
\]

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

(i) The elements \(a_{i,j}, 1 \leq i \leq r, 1 \leq j \leq r_i\), form an \(L\)-basis of \(A_L\). If, for each \(i \in \{1, \ldots, r\}\), the elements \(x_{i,1}, \ldots, x_{i,r_i}\) form an \(\Omega_{L_i}\)-basis of \(\Omega_{L_i}\) then the elements \(a_{i,j}, 1 \leq i \leq r, 1 \leq j \leq r_i\), form an \(\Omega_L\)-basis of \(\Omega_L\).

(ii) One has \(\text{dim}_L(A_L) = |G|\).

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

(iv) The map

\[
i^M_L : A_L \otimes_L A_L \to A_M \otimes_M A_M, \quad a \otimes_L a' \mapsto a \otimes_M a',
\]

is an injective \(L\)-algebra map such that \(i^M_M \circ i^M_L = i^L_L\). In particular, \(A_L \otimes_L A_L\) can be regarded as an \(L\)-subalgebra of \(A \otimes_{\bar{K}} A\).

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

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

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

$$\begin{array}{cccc}
M \otimes_L A_L & \xrightarrow{\phi_L^M} & A_M & \\
\omega \otimes \omega & \downarrow & \omega & \\
\omega(M) \otimes_{\omega(L)} A_{\omega(L)} & \xrightarrow{\phi_L(M)} & A_{\omega(M)} & \\
N \otimes_M M \otimes_L A_L & \xrightarrow{\text{can} \otimes_M \phi_L^M} & N \otimes_M A_M & \\
\end{array}$$

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

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

(ii) Indeed, by (i) we have

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

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

$$\left( \omega(x_{i,j}) \right)_{j \in \{1, \ldots, r_i\}}^{i \in \{1, \ldots, r\}}_{\omega \in \Omega_L / \text{stab}_{\Omega_L}(g_i)}$$

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

(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 $\Omega$-action on $A$. Let $a \in A_L$. Then, by (iii), we may write

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

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 $\Delta$ respects the $\Omega$-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 $\Delta(a) \in \bar{K}^L (A_L \otimes_L A_L)$.

(vi) It is easy to see that $\phi_L^M$ is a homomorphism of $M$-Hopf algebras and that the two diagrams commute. Moreover, by (iii), $\phi_L^M$ 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 $A$. Let $\hat{G} := \text{Hom}(G, \bar{K}^\times)$ denote the abelian group of $\bar{K}$-characters of $G$. Then $\Omega$ acts on $\hat{G}$ by

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

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

$$\rho: A = \bar{K} G \rightarrow \prod_{\chi \in \hat{G}} \bar{K}, \quad \sum_{g \in G} \lambda_g g \mapsto \left( \sum_{g \in G} \lambda_g \chi(g) \right)_{\chi \in \hat{G}}$$

is an isomorphism of $\bar{K}$-algebras. For $\chi \in \hat{G}$, we denote by $e_\chi \in A$ the element corresponding to the primitive idempotent $\varepsilon_\chi$ of $\prod_{\chi \in \hat{G}} \bar{K}$ which has entry 1 in the component $\chi$ 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 $\Omega$-action on $A$ is transported via $\rho$ to the action

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

for $(\lambda_\chi)_{\chi \in \hat{G}} \in \prod_{\chi \in \hat{G}} \bar{K}$ and $\omega \in \Omega$. Thus, the application of $\omega$ moves the $\chi$-component $\lambda_\chi$ to the $\omega\chi$-component while simultaneously applying $\omega$ to $\lambda_\chi$. This implies that $\rho$ restricts to an isomorphism.
2.2. Lemma. Assume that $G$ is abelian and let $K \subseteq L \subseteq \bar{K}$ be an intermediate field. Let $\chi_1, \ldots, \chi_s \in \hat{G}$ be a set of representatives for the $\Omega_L$-orbits of $\hat{G}$. For each $k \in \{1, \ldots, s\}$, let $\hat{L}_k$ denote the fixed field of $\text{stab}_{\Omega_L}(\chi_k) \subseteq \Omega_L$, and let $y_{k,1}, \ldots, y_{k,s_k}$ be an $L$-basis of $\hat{L}_k$. For $1 \leq k \leq s$ and $1 \leq l \leq s_k$, set

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

Then the following assertions hold:

(i) The composition

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

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

$$\bar{\rho}_L: A_L \rightarrow \prod_{k=1}^{s} \hat{L}_k.$$ 

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

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

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

(ii) The elements $\hat{a}_{k,l}$ are contained in $A_L$ and the elements $\bar{\rho}_L(\hat{a}_{k,l})$, $1 \leq k \leq s$, $1 \leq l \leq s_k$ 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.

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 $A$ is the $\bar{K}$-Hopf algebra $B := \text{Map}(G, \bar{K})$ consisting of all set maps from $G$ to $\bar{K}$. The duality is given by the non-degenerate bilinear form

$$(-, -): A \otimes_K B \rightarrow \bar{K}, \quad (\sum_{g \in G} \lambda_g g, f) \mapsto \sum_{g \in G} \lambda_g f(g).$$
The \( \bar{K} \)-linear structure of \( B \) is obvious. Multiplication is given by \( (f_1 f_2)(g) = f_1(g)f_2(g) \), for \( f_1, f_2 \in B \) and \( g \in G \), with the constant map with value 1 as unity. The diagonal \( \Delta \), augmentation \( \epsilon \), and antipode \( S \) are given by

\[
\Delta(f)(g_1, g_2) = f(g_1 g_2), \\
\epsilon(f) = f(1), \\
S(f)(g) = f(g^{-1}),
\]
respectively, for \( f \in B \), \( g, g_1, g_2 \in G \), where in the definition of \( \Delta \) we identify \( B \otimes_K B \) with \( \text{Map}(G \times G, \bar{K}) \) 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

\[
\Delta(l_g) = \sum_{g_1, g_2 \in G} l_{g_1} \otimes_{\bar{K}} l_{g_2}.
\]

Note that \( \Omega \) acts on \( B \) by

\[
(\omega f)(g) := \omega(f(\omega^{-1} g))
\]
for \( \omega \in \Omega \), \( f \in B \), and \( g \in G \). This action respects the \( \bar{K} \)-Hopf algebra structure, as is easily verified. For \( a \in A \), \( f \in B \), and \( \omega \in \Omega \) one has

\[
(\omega a, \omega f) = \omega((a, f)).
\]

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

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

Then \( B_L \) is an \( L \)-subalgebra of \( B \).

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

\[
B_L = \text{Map}(G, O_{\bar{K}})^{\Omega_L}.
\]

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 \( x_{i,1}, \ldots, x_{i,r_i} \in L_i \) \((1 \leq i \leq r)\) be given as in Lemma 2.1. Moreover, for \( 1 \leq i \leq r \) and \( 1 \leq j \leq r_i \), let \( b_{i,j} \in B \) 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
\[ \sigma_L : B_L \rightarrow \prod_{i=1}^{r} L_i, \quad b \mapsto (b(g_i))_{i=1,...,r}, \]
is an \(L\)-algebra isomorphism. In particular, \(\sigma_L\) restricts to an isomorphism
\[ \sigma_L : B_L \rightarrow \prod_{i=1}^{r} \mathcal{O}_{L_i}. \]

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

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

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

(v) The map
\[ j^M_L : B_L \otimes_L B_L \rightarrow B_M \otimes_M B_M, \quad b \otimes b' \mapsto b \otimes_M b', \]
is an injective \(L\)-algebra homomorphism such that \(j^N_M \circ j^M_L = j^N_L\). In particular, \(B_L \otimes_L B_L\) can be regarded as \(L\)-subalgebra of \(B \otimes_K B\).

(vi) Under the identification \(B_L \otimes_L B_L \subseteq B \otimes_K B\) of (v), \(B_L\) is an \(L\)-Hopf subalgebra of \(B\).

(vii) The map
\[ \psi^M_L : M \otimes_L B_L \rightarrow B_M, \quad \lambda \otimes_L b \mapsto \lambda b, \]
is an isomorphism of \(M\)-Hopf algebras such that the diagrams

\[ \begin{array}{ccc}
M \otimes_L B_L & \xrightarrow{\psi^M_L} & B_M \\
\omega \otimes \omega \downarrow & & \downarrow \omega \\
\omega(M) \otimes_{\omega(L)} B_{\omega(L)} & \xrightarrow{\psi^{\omega(M)}_{\omega(L)}} & B_{\omega(M)} \\
\end{array} \]

\[ \begin{array}{ccc}
N \otimes_M M \otimes_L B_L & \xrightarrow{N \otimes_M \psi^M_L} & N \otimes_M B_M \\
\text{can} \otimes B_L \downarrow & & \downarrow \psi^N_M \\
N \otimes L A_L & \xrightarrow{\psi^N_L} & B_N \\
\end{array} \]

commute for all \(\omega \in \Omega\).

(viii) The map \(A_L \otimes_L B_L \rightarrow A_M \otimes_M B_M, a \otimes_L b \mapsto a \otimes_M b\), is injective; in particular, \(A_L \otimes_L B_L\) can be regarded as an \(L\)-subspace of \(A \otimes_K B\). 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 \((-,-)\): \(A_L \otimes_L B_L \rightarrow L\).

Proof. (i) For \(b \in B_L\) and \(i \in \{1, \ldots, r\}\), the elements \(b(\omega g_i) = \omega(b(g_i))\), \(\omega \in \Omega_L\), are determined by \(b(g_i)\). Hence, \(\sigma_L\) is injective. On the other hand, for given elements \(\lambda_i \in L_i, i = 1, \ldots, r\), the map \(b : G \rightarrow K\), 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 \( \sum_{i=1}^{r} [\Omega_L : \text{stab}_{\Omega_L}(g_i)] = |G| \).

(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 \( B \) which leads to the same transition matrix as in the proof of Lemma 2.1 (iii).

(v) This follows from (iv).

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

(vii) By (iv), \( \psi_{\Omega}^M \) is an isomorphism of \( M \)-spaces. The remaining assertions are easily verified.

(viii) The injectivity of the map \( A_L \otimes_{\Omega} B_L \rightarrow A_M \otimes_{M} B_M \) 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 \( B_L \), \( 1 \leq i \leq r, 1 \leq j \leq r_i, \) with their property from Lemma 2.1 (iii) and from (iv), we see that \( (A_L, B_L) = L \) and that the restricted pairing \( A_L \otimes L B_L \rightarrow L \) 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

\[
A_L \otimes_{\mathcal{O}} B_L \rightarrow L, \quad \left( \sum_{g \in G} \lambda g, f \right) \mapsto \sum_{g \in G} \lambda g f(g).
\]

More precisely, if \( \mathcal{R} \subseteq A_L \) and \( S \subseteq B_L \) 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

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

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 \( S \). 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 \( S \).

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 \( p_1 \cdots p_t \) of non-zero prime ideals \( p_1, \ldots, p_t \) of \( \mathcal{O}_L \) if \( R/p_1, \ldots, R/p_t \) 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 $[Y : X \cap Y]_{\mathcal{O}_L} [X : X \cap Y]^{-1}_{\mathcal{O}_L}$. 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 $$[\mathcal{O}_{L'} \otimes \mathcal{O}_L Y : \mathcal{O}_{L'} \otimes \mathcal{O}_L X]_{\mathcal{O}_{L'}} = [Y : X]_{\mathcal{O}_L} \mathcal{O}_{L'}.$$ If $p$ is a non-zero prime ideal of $\mathcal{O}_L$ then the following localization property holds: $$[Y_p : X_p]_{(\mathcal{O}_L)_p} = ([Y : X]_{\mathcal{O}_L})_p.$$
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 $$[Y' : X']_{\mathcal{O}_L} = N_{L'/L} ([Y' : X']_{\mathcal{O}_{L'}}).$$

If $G$ is abelian we denote by $d_{A_L}$ the discriminant ideal of the maximal order $A_L$ over $\mathcal{O}_L$, i.e. $d_{A_L} = \prod_{k=1}^s d_{L_k/L}$ in the notation of Lemma 2.2. Similarly, for arbitrary $G$, we denote by $d_{B_L}$ the discriminant ideal of the maximal order $B_L$ 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 $D_{L'/L}$ 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 $$B_L^* = \left\{ \sum_{i=1}^r \sum_{\omega \in \Omega_L/\text{stab}_{\Omega_L}(g_i)} \omega(\lambda_i) \omega g_i \mid \lambda_i \in D_{L_i/L}^{-1} \text{ for } i = 1, \ldots, r \right\}.$$ Moreover, $B_L^*$ 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 $$a = \sum_{i=1}^r \sum_{\omega \in \Omega_L/\text{stab}_{\Omega_L}(g_i)} \omega(\lambda_i) \omega g_i$$ with uniquely determined $\lambda_i \in L_i$, $i = 1, \ldots, r$, by Lemma 2.1 (i). Then $a \in B_L^*$ if and only if $(a, f) \in \mathcal{O}_L$ for all $f \in B_L$. By Lemma 3.1 (i), each $f \in B_L$ is a sum of elements of the form $\sum_{i} \omega(x_i) \omega g_i$, $x_i \in \mathcal{O}_{L_i}$, $i = 1, \ldots, r$, where the sum runs over coset representatives of $\Omega_L/\text{stab}_{\Omega_L}(g_i)$. Hence, $a \in B_L^*$ if and only if $$\sum_{\omega \in \Omega_L/\text{stab}_{\Omega_L}(g_i)} \omega(\lambda_i) \omega(x_i) = \text{Tr}_{L_i/L}(\lambda_i x_i) \in \mathcal{O}_L$$
for all \(i \in \{1, \ldots, r\}\) and all \(x_i \in \mathcal{O}_{L_i}\), which is equivalent to \(\lambda_i \in \mathcal{D}_{L_i/L}^{-1}\) for all \(i \in \{1, \ldots, r\}\).

If \(d_{BL} = \mathcal{O}_L\) then \(\mathcal{D}_{L_i/L} = \mathcal{O}_{L_i}\) for all \(i = 1, \ldots, r\), and therefore \(B_L^* = A_L^2\) is an \(\mathcal{O}_L\)-order. Suppose, conversely, that \(B_L^*\) is an \(\mathcal{O}_L\)-order and let \(i \in \{1, \ldots, r\}\) be arbitrary. Let \(i' \in \{1, \ldots, r\}\) and \(\nu \in \Omega_L\) be such that \(g_i^{-1} = \nu g_{i'}\). Note that \(\text{stab}_{\Omega_L}(g_i) = \text{stab}_{\Omega_L}(g_i^{-1})\) 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

\[
\sum_{\omega \in \Omega_L/\text{stab}_{\Omega_L}(g_i)} \omega(\lambda_i) \omega_{g_i} + \sum_{\omega' \in \Omega_L/\text{stab}_{\Omega_L}(g_{i'})} \omega'(\lambda_{i'}) \omega'_{g_{i'}}
\]

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

\[
(3) \quad \sum_{\omega \in \Omega_L/\text{stab}_{\Omega_L}(g_i)} \omega(\lambda_i) \omega(\nu(\lambda_{i'})) = \text{Tr}_{L_i/L}(\lambda_i \nu(\lambda_{i'})) \in \mathcal{O}_L.
\]

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 \(\text{Tr}_{L_i/L}(\mathcal{D}_{L_i/L}^{-2}) \subseteq \mathcal{O}_L\). But this is only possible if \(d_{L_i/L} = \mathcal{O}_L\). Since this holds for all \(i \in \{1, \ldots, r\}\) we obtain \(d_{BL} = \mathcal{O}_L\).

4.2. Corollary. One has \(A_L^2 \subseteq B_L^*\) and \([B_L^* : A_L^2]_{\mathcal{O}_L} = d_{BL}\).

Proof. The inclusion \(A_L^2 \subseteq B_L^*\) is clear from Lemma 4.1. From the definition of \(A_L^2\) and from Lemma 4.1 we have

\[
[B_L^* : A_L^2]_{\mathcal{O}_L} = \prod_{i=1}^r \mathcal{D}_{L_i/L}^{-1} : \prod_{i=1}^r \mathcal{O}_{L_i}]_{\mathcal{O}_L} = \prod_{i=1}^r [\mathcal{O}_{L_i} : \mathcal{D}_{L_i/L}]_{\mathcal{O}_L} = \prod_{i=1}^r d_{L_i/L} = d_{BL}.
\]

We remark that, for \(G\) abelian, \(B_L^*\) is not necessarily contained in \(A_L\).

For the following lemma we assume that \(G\) is abelian. Let \(L \subseteq L' \subseteq \overline{K}\) be a finite extension field of \(L\) containing \(L_1, \ldots, L_r\) and \(\hat{L}_1, \ldots, \hat{L}_s\), in the notation of Lemma 2.1 and Lemma 2.2. Then \(A_{L'} = L'G, B_{L'} = \text{Map}(G, L')\) 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

$$[A_L : A_L^O]_{O_L}^2 = |G|^G d_{B_L} d_{A_L}^{-1}$$

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

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

$$[A_L : A_L^O]_{O_L}^2 = [O_{L'} \otimes_{O_L} A_L : O_{L'} \otimes_{O_L} A_L^O]_{O_{L'}}^2$$

using the isomorphism $\phi_{L'} : L' \otimes O_L A_L \to A_{L'}$, the maximal $O_{L'}$-order $A_{L'}$ of $A_L$, and the isomorphism $\rho_{L'} : A_{L'} \to \prod_{\chi \in \hat{G}} L'$. More precisely, $[A_L : A_L^O]_{O_L} O_{L'}$ is the quotient of the squared order ideals

$$[\rho_{L'}(A_{L'}) : (\rho_{L'} \circ \phi_{L'}^\Lambda)(O_{L'} \otimes_{O_L} A_L^O)]_{O_{L'}}^2$$

and

$$[\rho_{L'}(A_{L'}) : (\rho_{L'} \circ \phi_{L'}^\Lambda)(O_{L'} \otimes_{O_L} A_L)]_{O_{L'}}^2.$$

For the computation of the squared order ideal (5) let $\chi_k, \hat{L}_k, y_k, l, \hat{a}_{k,l}$, $1 \leq k \leq s, 1 \leq l \leq s_k$, be given as in Lemma 2.2 such that $y_{k,1}, \ldots, y_{k,s_k}$ is an $O_L$-basis of $O_{L_k}$ for each $k = 1, \ldots, s$. Then the elements

$$\hat{a}_{k,l} = \sum_{\omega \in O_L/\text{stab}_{O_L}(\chi_k)} \omega(y_{k,l}) e^{\omega \chi_k} \quad (1 \leq k \leq s, 1 \leq l \leq s_k)$$

form an $O_L$-basis of $A_L$ and $(\rho_{L'} \circ \phi_{L'}^\Lambda)(O_{L'} \otimes_{O_L} A_L)$ has as $O_{L'}$-basis the elements

$$(\chi(\hat{a}_{k,l}))_{\chi \in \hat{G}} \quad (1 \leq k \leq s, 1 \leq l \leq s_k).$$

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

$$\left(\omega(y_{k,l})\right)_{\substack{i \in \{1, \ldots, s_k\} \ \omega \in O_L/\text{stab}_{O_L}(\chi_k)}}.$$

The square of the determinant of this block generates the $O_L$-ideal $d_{L_k/L}$. Thus, the squared order ideal in (5) is given by

$$\prod_{k=1}^s d_{L_k/L} O_{L'} = d_{A_L/L} O_{L'}.$$
For the computation of the squared order ideal (4) let $g_i, L_i, x_{i,j}$, and $a_{i,j}$, $1 \leq i \leq r$, $1 \leq j \leq r_i$, be given as in Lemma 2.1 such that $x_{i,1}, \ldots, x_{i,r_i}$ is an $O_L$-basis of $O_{L_i}$ for each $i \in \{1, \ldots, r\}$. Then, the elements

$$a_{i,j} = \sum_{\omega \in \Omega_L/\text{stab}_{\Omega_L}(g_i)} \omega(x_{i,j}) \omega g_i \quad (1 \leq i \leq r, 1 \leq j \leq r_i)$$

form an $O_L$-basis of $A^o_L$. Thus, the elements

$$\left( \sum_{\omega \in \Omega_L/\text{stab}_{\Omega_L}(g_i)} \omega(x_{i,j}) \chi(\omega g_i) \right)_{\chi \in \hat{G}} \quad (1 \leq i \leq r, 1 \leq j \leq r_i)$$

form an $O_{L'}$-basis of $(\rho_{L'} \circ \phi_{L'}^0)(O_{L'} \otimes_{O_L} A^o_L)$. Expressing this basis by the basis $\epsilon_\chi$, $\chi \in \hat{G}$, of $\rho_{L'}(A_{L'}) = \prod_{\chi \in \hat{G}} O_{L'}$, we obtain the transition matrix

$$M = \left( \sum_{\omega \in \Omega_L/\text{stab}_{\Omega_L}(g_i)} \omega(x_{i,j}) \chi(\omega g_i) \right)_{(i,j), \chi \in \hat{G}}$$

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

$$M_{1,i} = \left( \omega(x_{i,j}) \right)_{j \in \{1, \ldots, r_i\}, \omega \in \Omega_L/\text{stab}_{\Omega_L}(g_i)}$$

and the matrix

$$M_2 = \left( \chi(g) \right)_{g \in G, \chi \in \hat{G}}.$$

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

$$\chi_1 \chi_2 \in \hat{G},$$

(7) $\quad \det(M_2)^2 = \det(M_{2}^T M_2) = \pm |G| |G|$.

Altogether this yields

(8) $\quad \det(M)^2 O_{L'} = |G|^{|G|} d_{B_L} O_{L'}$

which expresses the squared order ideal in (4). Now, dividing the ideal in (8) by the ideal in (6), the result follows, since extending $O_L$-ideals to $O_{L'}$-ideals is injective. \qed
4.4. Next we investigate under which circumstances $A_L^0$ and (in the abelian case) $A_L$ 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 $\mathcal{A} \subseteq E\mathcal{H}$ is an $R$-subalgebra of $E\mathcal{H}$ with $R$-basis $a_1, \ldots, a_n$ which is also an $E$-basis of $E\mathcal{H}$. Then the multiplication map $E \otimes_R A \to E\mathcal{H}, \lambda \otimes_R a \mapsto \lambda a$, is an $E$-algebra isomorphism and the map $A \otimes_R A \to E\mathcal{H} \otimes_E E\mathcal{H}, a \otimes_R a' \mapsto a \otimes_E a'$, is injective, so that $A \otimes_R A$ can be regarded as an $R$-subalgebra in $E\mathcal{H} \otimes_E E\mathcal{H}$. We would like to decide whether $\Delta(A) \subseteq A \otimes_R A$ 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

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

together with its inverse

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

Then we have the following criterion:

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

(i) One has $\Delta(A) \subseteq A \otimes_R A$.

(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

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

with uniquely determined coefficients $\gamma_{j,j'}^{(i)} \in E$. Then, for $i \in \{1, \ldots, n\}$, we have $\Delta(a_i) \in A \otimes_R A$ 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 $\gamma_{j,j'}^{(i)}$ are uniquely determined by the system of linear equations
\[
\sum_{j,j'} \gamma_{j,j'}^{(i)} \alpha_{j,h_1} \alpha_{j',h_2} = \begin{cases} 
\alpha_{i,h}, & \text{if } h_1 = h_2 =: h, \\
0, & \text{if } h_1 \neq h_2,
\end{cases}
\]
one equation for each $i \in \{1, \ldots, n\}$ and each pair $(h_1, h_2) \in H \times H$. Now it is easy to verify that these equations are satisfied for
\[
\gamma_{j,j'}^{(i)} = \sum_{h \in H} \alpha_{i,h} \beta_{h,j} \beta_{h,j'},
\]
and the result follows.

In the following proposition we apply Lemma 4.5 to the $O_L$-order $A_L^0$ in $A_L$.

4.6. Proposition. The $O_L$-order $A_L^0$ is a Hopf order in $A_L$ if and only if $d_{B_L} = O_L$.

Proof. Clearly, $A_L^0$ is stable under the antipode of $A_L$. The inclusion $\Delta(A_L^0) \subseteq A_L^0 \otimes_{O_L} A_L^0$ can be tested by localization. Thus we may assume that $O_L$ 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 $i \in \{1, \ldots, r\}$, the elements $x_{i,1}, \ldots, x_{i,r_i}$, form an $O_L$-basis of $O_{L_i}$. Then the elements $a_{i,j}, 1 \leq i \leq r, 1 \leq j \leq r_i$, form an $O_L$-basis of $A_L^0$, and, in the notation of 4.4, the coefficient matrix $S$ is a block diagonal matrix, the blocks indexed by $i = 1, \ldots, r$, and the $i$-th block given by
\[
(\omega(x_{i,j}))_{j \in \{1, \ldots, r_i\}}^\omega_{U_{i}/\text{stab}_{U_{i}}(g_i)}.
\]
If $x_{i,1}, \ldots, x_{i,r_i}^* \in L_i$ is a dual basis of $x_{i,1}, \ldots, x_{i,r_i}$ with respect to the trace form $\text{Tr}_{L_i/L}$, then the inverse $T$ of $S$ is given by the block diagonal matrix with $i$-th block
\[
(\omega(x_{i,j}^*))_{j \in \{1, \ldots, r_i\}}^\omega_{U_{i}/\text{stab}_{U_{i}}(g_i)}.
\]

Now, taking into account the block diagonal structure of $S$ and $T$, Lemma 4.5 states that $\Delta(A_L^0) \subseteq A_L^0 \otimes_{O_L} A_L^0$ if and only if
\[
(9) \quad \sum_{\omega \in \Omega_{L_i}/\text{stab}_{\Omega_{L_i}}(g_i)} \omega(x_{i,j}) \omega(x_{i,j'}^*) \omega(x_{i,j''}^*) = \text{Tr}_{L_i/L}(x_{i,j} x_{i,j'}^* x_{i,j''}^*) \in O_L
\]
for all $i \in \{1, \ldots, r\}$ and all $j', j'' \in \{1, \ldots, r_i\}$. But since $x_{i,j}, j = 1, \ldots, r_i$, form an $O_L$-basis of $D_{L_i/L}^{-1}$, the condition in (9) holds for given $i \in \{1, \ldots, r\}$ and all $j', j'' \in \{1, \ldots, r_i\}$ if and only if $\text{Tr}_{L_i/L}(D_{L_i/L}^{-2}) \subseteq O_L$. 


4.7. Corollary. The following statements are equivalent:

(i) The order $A_L^o$ is a Hopf order in $A_L$.
(ii) The discriminant ideal $d_{B_L}$ is trivial.
(iii) One has $A_L^o = B_L^*$.
(iv) One has $(A_L^o)^* = B_L$.
(v) The maximal order $B_L$ of $B_L$ is an $O_L$-Hopf order.

If (i)-(v) hold then $A_L^o$ is the smallest $O_L$-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 $[B_L^*: A_L^o] = d_{B_L}$. Obviously, (iii) and (iv) are equivalent, since $O_L$ is a Dedekind domain. Moreover, (i) and (iv) imply (v). Finally, (v) implies that $B_L^*$ is an order in $A_L$, and then Lemma 4.1 implies (ii).

If (i)-(v) hold then $B_L$ is certainly the largest $O_L$-Hopf order in $B_L$. Therefore its dual $A_L^o$ is the smallest $O_L$-Hopf order in $A_L$.

4.8. Proposition. Let $G$ be abelian. Then the maximal $O_L$-order $A_L$ of $A_L$ is a Hopf order if and only if $d_{A_L} = O_L$.

Proof. Since the antipode $S$ is an $L$-algebra automorphism of $A_L$, the maximal $O_L$-order of $A_L$ is stable under $S$. As in the proof of Proposition 4.6 we may assume that $O_L$ is local. Now let $\chi_k, \hat{L}_k, y_{k,l}$, 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 $O_L$-basis of $O_{\hat{L}_k}$. Then the elements $\hat{a}_{k,l}, 1 \leq k \leq s, 1 \leq l \leq s_k$, form an $O_L$-basis of $A_L$. The matrix $S$ in the notation of 4.4 is given by

$$
1 \left| 
\sum_{\omega \in O_L/\text{stab}_{O_L}(\chi_k)} \omega(y_{k,l}) (\omega\chi_k)(g^{-1}) \right|_{g \in G}^{(k,l)}.
$$

We can write $S = S_1S_2$, where $S_1$ is the block diagonal matrix with blocks indexed by $k = 1, \ldots, s$ and whose $k$-th block is given by

$$
S_{1,k} = \left( \omega(y_{k,l}) \right)_{l \in \{1, \ldots, s_k\} \omega \in O_L/\text{stab}_{O_L}(\chi_k)}.
$$

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

But this is equivalent to $D_{L_i/L} = O_{L_i}$ and to $d_{L_i/L} = O_L$. Now the result follows.
If, for each \( k \in \{1, \ldots, s\} \), we denote by \( y_{k,1}^*, \ldots, y_{k,s_k}^* \in \hat{L}_k \) the dual basis of \( y_{k,1}, \ldots, y_{k,s_k} \) with respect to \( \text{Tr}_{\hat{L}_k/L} \), then

\[
T_{1,k} = \left( \omega(y_{k,l}^*) \right)_{\omega \in \Omega_L/\text{stab}_{\Omega_L}(x_k)}
\]

is the inverse of \( S_{1,k} \). Moreover, by the orthogonality relations for irreducible characters, the inverse of \( S_2 \) is given by

\[
T_2 = \left( \omega(x_k)(g) \right)_{g \in G}. \tag{1}
\]

Thus, the inverse of \( S \) is given by

\[
T = \sum_{\omega \in \Omega_L/\text{stab}_{\Omega_L}(x_k)} \omega(y_{k,l}^*) \left( \omega(x_k)(g) \right)_{g \in G}. \tag{2}
\]

Now, Lemma 4.5 states that \( \Delta(A_L) \subseteq A_L \otimes_{\Omega_L} A_L \) if and only if

\[
\sum_{g \in G, \omega, \omega', \omega''} \omega(y_{k,l})(\omega(x_k)(g) \omega'(y_{k',l'})(\omega''(x_{k''}(g) \omega''(y_{k'',l''}) (\omega''(x_{k''}(g) \omega''(y_{k'',l''})) (g) =
\]

\[
\sum_{g \in G, \omega, \omega', \omega''} \omega(y_{k,l})(\omega(x_k)(g) \omega'(y_{k',l'})(\omega''(x_{k''}(g) \omega''(y_{k'',l''})) (g) =
\]

for all \((k, l), (k', l'), (k'', l'')\), where the triple sum runs independently over all \( \omega \in \Omega_L/\text{stab}_{\Omega_L}(x_k) \), \( \omega' \in \Omega_L/\text{stab}_{\Omega_L}(x_{k'}) \), and \( \omega'' \in \Omega_L/\text{stab}_{\Omega_L}(x_{k''}) \). By the orthogonality relations of irreducible characters the last sum over \( g \in G \) reduces to \( |G| \) if \( \omega(x_k)(\omega'(x_{k'}(g) \omega''(x_{k''}(g) = 1 \) and vanishes otherwise. If \( d_{A_L} \neq 0 \), then \( y_{k,l}^* \in \hat{L}_k \) for all pairs \((k, l)\), and the above condition is certainly satisfied. Conversely, if the above condition is satisfied, then we choose \( k' \in \{1, \ldots, s\} \) arbitrarily and remark that \( \text{stab}_{\Omega_L}(x_{k'}) = \text{stab}_{\Omega_L}(x_{k'}^{-1}) \). Let \( k'' \in \{1, \ldots, s\} \) and \( \kappa \in \Omega_L \) be such that \( x_{k''}^{-1} = \chi_{k''}^{\kappa} \). Moreover let \( k \in \{1, \ldots, s\} \) be such that \( \chi_k = 1 \). Then \( \hat{L}_k = L \) and the above sum reduces further to

\[
\sum_{\omega', \omega''} \omega'(y_{k',l'}^*) \omega''(y_{k'',l''}^*) \delta_{\omega', \omega''(\chi_{k''}^{-1})} =
\]

\[
= \sum_{\omega'} \omega'(y_{k',l'}^*) \omega' \kappa(y_{k'',l''}^*) = \text{Tr}_{\hat{L}_k/L}(y_{k',l'}^* \kappa(y_{k'',l''}^*)),
\]

since \( \omega'(x_{k'}) \omega''(x_{k''}) = 1 \) if and only if \( \omega'' = \omega' \kappa \). The elements \( \kappa(y_{k'',1}), \ldots, \kappa(y_{k'',s_k''}) \) form an \( \Omega_L \)-basis of \( \text{Tr}_{\hat{L}_k/L}(D_{L_{k''}/L}^{-1}) = D_{L_{k''}/L}^{-1} \). Since the last term in the above equation lies in \( \Omega_L \) for all \( l' \) and \( l'' \), we have \( \text{Tr}_{L_{k'/L}}(D_{L_{k''}/L}^{-1}) \subseteq \Omega_L \). But this implies \( d_{\hat{L}_k/L} = \Omega_L \). This holds for all \( k' \in \{1, \ldots, s\} \). Thus, \( d_{A_L} = \Omega_L \). \( \square \)
5. SOME $A$-MODULES AND RESOLVENTS

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

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

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

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

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

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

$$C_L = \text{Map}(\Gamma, \mathcal{O}_L)^{\Omega_L}.$$

Note that $C$ is a right $A$-module via the $G$-action on $\Gamma$:

$$(f \cdot (\sum_{g \in G} \lambda_g g))(\gamma) := \sum_{g \in G} \lambda_g f(2^g)$$

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

$$\omega(f \cdot a) = (\omega f) \cdot (\omega a)$$

for all $a \in A$, $f \in C$, $\omega \in \Omega$. Thus, the $A$-module structure on $C$ 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), $C_L$ is an $A_L^\omega$-module by restriction.

Similar to Lemma 3.1 for the algebra $B$ we have the following lemma for $C$.

5.1. Lemma. Let $K \subseteq L \subseteq \bar{K}$ be an intermediate field, and let $\gamma_1, \ldots, \gamma_t \in \Gamma$ be a set of representatives for the $\Omega_L$-orbits of $\Gamma$. For each $m \in \{1, \ldots, t\}$ let $\bar{L}_m$ denote the fixed field of $\text{stab}_{\Omega_L}(\gamma_m) \subseteq \Omega_L$, and let $z_{m,1}, \ldots, z_{m,t_m}$ be an $L$-basis of $\bar{L}_m$. For $1 \leq m \leq t$ and $1 \leq n \leq t_m$, let $c_{m,n} \in C$ 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

$$\tau : C_L \xrightarrow{\cong} \prod_{m=1}^t \bar{L}_m, \quad f \mapsto (f(\gamma_m)),$$
is an $L$-algebra isomorphism. In particular, $\tau$ restrict to an isomorphism

$$\tau_L : C_L \xrightarrow{\cong} \prod_{m=1}^{t} O_{L_m}.$$  

of $O_L$-algebras.

(ii) The elements $c_{m,n}$, $1 \leq m \leq t$, $1 \leq n \leq t_m$, form an $L$-basis of $C_L$. If, for each $m \in \{1, \ldots, t\}$, the elements $z_{m,1}, \ldots, z_{m,t_m}$ form an $O_{L_m}$-basis of $O_{L_m}$, then the elements $c_{m,n}$, $1 \leq m \leq t$, $1 \leq n \leq t_m$, form an $O_L$-basis of $C_L$.

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

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

(v) The map

$$\pi_L^M : M \otimes_L C_L \rightarrow C_M, \quad \lambda \otimes_L c \mapsto \lambda c,$$

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

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

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

$$H \otimes_R S \rightarrow \Hom_R(S, S), \quad h \otimes_R s \mapsto (t \mapsto (t \cdot h)s),$$

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 \( g \in G, f, f' \in C \), and \( \gamma \in \Gamma \). Then

\[
(f f')(\gamma) = (f f'(a \gamma)) = (f (a \gamma)) f'(a \gamma) = (f \cdot g)(\gamma)(f' \cdot g)(\gamma)
\]

thus, \((f f') \cdot g = (f \cdot g)(f' \cdot g)\) which is the statement in (G1) (i). Moreover, \((1c \cdot g)(\gamma) = 1c(\gamma) = 1 = 1c(\gamma)\), 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 \( \sum_{g \in G} g \otimes f_{g} \in A \otimes_{\bar{K}} C \) with arbitrarily chosen \( f_{g} \in C \) for \( g \in G \) such that it vanishes under the map in (G2). Then

\[
\sum_{g \in G} f(\gamma) f_{g}(\gamma) = 0, \quad \text{for all } f \in C \text{ and all } \gamma \in \Gamma.
\]

Let \( g_{0} \in G \) and \( \gamma \in \Gamma \). Then, choosing \( f \in C \) in such a way that \( f(\gamma) = 1 \) and \( f(\gamma') = 0 \) for \( \gamma' \neq \gamma \), 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 \( K \subseteq L \subseteq \bar{K} \), the following question arises naturally: Is \( C_{L} \) 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

\[
\mathcal{A}_{L}^{\text{ass}} := \{a \in A_{L} \mid C_{L} \cdot a \subseteq C_{L}\}
\]

of \( C_{L} \) in \( A_{L} \). Obviously, \( \mathcal{A}_{L}^{G} \subseteq \mathcal{A}_{L}^{\text{ass}} \subseteq A_{L} \). We will prove that, in the situation we consider in Section 6, \( C_{L} \) is free over \( \mathcal{A}_{L}^{\text{ass}} \). In the proof we make use of the resolvent

\[
(f, \chi)_{g_{0}} := \sum_{g \in G} f(\gamma) \chi(g^{-1}) \in \bar{K}
\]
attached to \( f \in \mathbb{C} \) and \( \chi \in \hat{G} \) for fixed \( \gamma_0 \in \Gamma \).

For an intermediate field \( K \subseteq L \subseteq \overline{K} \), let \( L' \subseteq \overline{K} \) now denote a finite extension of \( L \) such that \( \Omega L' \) acts trivially on \( \hat{G} \) and \( \Gamma \). We call such a field a splitting field for \( A_L \) and \( C_L \). Note that, since 
\[
\omega((f, \chi)_{\gamma_0}) = (\omega f, \omega \chi)^{\omega_{\gamma_0}},
\]
for all \( \omega \in \Omega', f \in \mathbb{C}, \chi \in \hat{G}, \) 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 \( C_L \) over \( \mathcal{O}_L \). Thus, in the notation of Proposition 5.1 we have 
\[
d_{C_L} = \prod_{m=1}^{t} d_{L_m/L'}.
\]

5.3. Proposition. Assume that \( G \) is abelian and fix \( \gamma_0 \in \Gamma \). Let \( K \subseteq L \subseteq \overline{K} \) be an intermediate field, let \( L \subseteq L' \subseteq \overline{K} \) 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 
\[
[C_L : f \cdot A_L^2] \mathcal{O}_L \mathcal{O}_{L'} = d_{B_L} d_{C_L}^{-1} \prod_{\chi \in \hat{G}} (f, \chi)^2_{\gamma_0} \mathcal{O}_{L'}.
\]

Proof. (a) Let \( \chi_k, \hat{L}_k, y_{k,l} \), and the \( L \)-basis 
\[
(x_{\gamma_k}, 1 \leq k \leq s, 1 \leq l \leq s_k)
\]
of \( A_L \) be given as in Lemma 2.2. Then the elements 
\[
((f \cdot \hat{a}_{k,l})(\gamma))_{\gamma \in \Gamma} \in \prod_{\gamma \in \Gamma} L'
\]
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 \( e_{\gamma}, \gamma \in \Gamma \), of \( \prod_{\gamma \in \Gamma} L' \) and obtain a transition matrix 
\[
M = ((f \cdot \hat{a}_{k,l})(\gamma))_{(k,l)} \in \prod_{\gamma \in \Gamma} L'
\]
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 
\[
(f \cdot \hat{a}_{k,l})(g_{\gamma_0}) = \frac{1}{|G|} \sum_{\omega \in \Omega_L/\text{stab}(x_k)} \sum_{g' \in G} \omega(y_{k,l}) (\omega \chi_k)(g'^{-1}) f(g'g_{\gamma_0})
\]
\[
= \frac{1}{|G|} \sum_{\omega \in \Omega_L/\text{stab}(x_k)} \sum_{h \in G} \omega(y_{k,l}) (\omega \chi_k)(gh^{-1}) f(h_{\gamma_0})
\]
\[
= \frac{1}{|G|} \sum_{\omega \in \Omega_L/\text{stab}(x_k)} \omega(y_{k,l}) (f, \omega \chi_k)_{\gamma_0} (\omega \chi_k)(g).
\]
We can write \( M = M_1 M_2 \), where \( M_1 \) is a block diagonal matrix, the blocks \( M_{1,k} \) indexed by \( k = 1, \ldots, s \), with

\[
M_{1,k} = (\omega(y_{k,l}))_{l \in \{1, \ldots, s_k\} \atop \omega \in \Omega_L / \text{stab}_{\Omega_L}(\chi_k)},
\]

and where

\[
M_2 = \frac{1}{|G|} \left( (f, \omega \chi_k) \tau_0 (\omega \chi_k)(g) \right)_{k, \omega \in \Omega_L / \text{stab}_{\Omega_L}(\chi_k)} = \frac{1}{|G|} \left( (f, \chi) \tau_0 \chi(g) \right)_{\chi \in \hat{G}}.
\]

Now, \( \det(M_{1,k})^2 \Omega_L = d_{L_k/L} \), hence \( \det(M_1)^2 \Omega_L = d_{A_L/L} \). Moreover,

\[
\det(M_2)^2 = \left( \prod_{\chi \in \hat{G}} (f, \chi)^2 \right)_{\chi \in \hat{G}} \frac{|G|^{-2|G|}}{s \in G} \det(\chi(g))^2_{\chi \in \hat{G}}
\]

\[
= \pm \left( \prod_{\chi \in \hat{G}} (f, \chi)^2 \right)_{\chi \in \hat{G}} |G|^{-|G|}
\]

by (7). Thus,

\[
\det(M)^2 \Omega_{L'} = d_{A_L} |G|^{-|G|} \prod_{\chi \in \hat{G}} (f, \chi)^2_{\tau_0} \Omega_{L'}.
\]

This shows that \( f \cdot A_L = C_L \) if and only if \( (f, \chi)_{\tau_0} \neq 0 \) for all \( \chi \in \hat{G} \).

(b) Next we show the assertion about \([C_L : f \cdot A_L^1]_{\Omega_L}\). Since both sides of the equation behave well under localization, we may assume that \( \Omega_L \) is local. We transport the two \( \Omega_{L'}\)-lattices \( \Omega_{L'} \otimes_{\Omega_L} C_L \) and \( \Omega_{L'} \otimes_{\Omega_L} f \cdot A_L^1 \) by the isomorphism \( \tau_{L'} \circ \pi_{L'}^1 \) into \( \prod_{\gamma \in \Gamma} L' \).

Retracing the calculations in (a) one observes that, if \( y_{k,1}, \ldots, y_{k,s_k} \) is an \( \Omega_{L'}\)-basis of \( \Omega_{L_k} \), for each \( k = 1, \ldots, s \), then the elements (12) form an \( \Omega_{L'}\)-basis of \( A_L \), and the elements in (13) form an \( \Omega_{L'}\)-basis of \( (\tau_{L'} \circ \pi_{L'}^1)(\Omega_{L'} \otimes_{\Omega_L} f \cdot A_L) \). Thus, the calculation in (a) shows that

\[
[\tau_{L'}(C_{L'}) : (\tau_{L'} \circ \pi_{L'}^1)(\Omega_{L'} \otimes_{\Omega_L} f \cdot A_L)]_{\Omega_{L'}}^2_{\Omega_{L'}} = d_{A_L} |G|^{-|G|} \prod_{\chi \in \hat{G}} (f, \chi)^2_{\tau_0} \Omega_{L'}.
\]

Moreover, we already know from Proposition 4.3 that

\[
[f \cdot A_L : f \cdot A_L^1]_{\Omega_L}^2 = [A_L : A_L^1]_{\Omega_L}^2 = d_{L_L} d_{A_L}^{-1} |G|^{|G|}.
\]

Now, it suffices to show that

\[
[\tau(C_{L'}) : (\tau_{L'} \circ \pi_{L'}^1)(\Omega_{L'} \otimes_{\Omega_L} C_L)]_{\Omega_{L'}}^2 = d_{C_L} \Omega_{L'},
\]

since then, dividing the product of (15) and (16) by (17) yields the result.
Let $\gamma_m, \tilde{L}_m, z_{m,n}$, and $c_{m,n}$ be given as in Lemma 5.1 such that, for each $m \in \{1, \ldots, t\}$, the elements $z_{m,1}, \ldots, z_{m,t_m}$ form an $O_L$-basis of $O_{\tilde{L}_m}$. Then, the elements $c_{m,n}$, $1 \leq m \leq t$, $1 \leq n \leq t_m$, form an $O_L$-basis of $C_L$. Thus, the elements $(\tau_{L'} \circ \pi_L')(c_{m,n})$ form an $O_{L'}$-basis of $(\tau_{L'} \circ \pi_L')(O_L' \otimes O_L C_L)$. We express this $O_{L'}$-basis by the canonical $O_{L'}$-basis of primitive idempotents $\varepsilon_\gamma, \gamma \in \Gamma$, of $\tau_{L'}(C_L') = \prod_{\gamma \in \Gamma} O_{L'}$ and obtain a transition matrix $M$. This is a block diagonal matrix with blocks $M_1, \ldots, M_t$, where

$$M_m = (\omega(z_{m,n}))_{\omega \in \Omega_L / \text{stab}_{\Omega_L}(\gamma_m)}^{n \in \{1, \ldots, t_m\}}$$

for $m \in \{1, \ldots, t\}$. Since $\det(M_m)^2 O_L = d_{\tilde{L}_m/L}$, we obtain (17), and the proof is complete. 

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

$$[C_L : f \cdot \tilde{A}_L]_p O_{L'} = d_{BL} d_{C_L}^{-1} [\tilde{A}_L : A_L]_p O_{L'} \prod_{\chi \in \hat{G}} (f, \chi)^2_{\gamma_0} O_{L'}$$

for each $O_L$-order $\tilde{A}_L$ of $A_L$. contained in $A_{L}^{\text{ass}}$. In particular, if $\tilde{A}_L \subset A_{L}^{\text{ass}}$ and if $f \in C_L$ is such that

$$[\tilde{A}_L : A_L]_p^2 d_{C_L} O_{L'} = d_{BL} \prod_{\chi \in \hat{G}} (f, \chi)^2_{\gamma_0} O_{L'},$$

then $C_L = f \cdot \tilde{A}_L$ is a free $\tilde{A}_L$-module of rank one with basis \{f\}, and consequently, $\tilde{A}_L = A_{L}^{\text{ass}}$.

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 $Q_p \subset L \subset Q_p$ we write $O_L$ for the integral closure of $Z_p$ in $L$ and $p_L$ for its maximal ideal. We fix a finite extension field $F$ of $Q_p$ and we set $q = |O_F / p_F|$. Let $d > 0$ be a fixed integer. We denote by $F'/F$ the unramified extension of degree $d > 0$ and write $\phi$ 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. $v_F(F^*) = Z$) of $F$. 

LUBIN-TATE FORMAL GROUPS 293
As in [dS, Ch. I] we set
\[
F_\xi = \{ f \in \mathcal{O}_{F'}[[X]] \mid f \equiv \pi'X \mod X^2, \\
N_{F'/F}(\pi') = \xi \text{ and } f \equiv X^q \mod p_{F'}[[X]] \}.
\]
For any power series \( g \) in one or more indeterminates over \( \mathcal{O}_{F'}[[X]] \) let \( g^\phi \) arise from applying \( \phi \) 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 \( f \in \text{Hom}(\mathcal{F}_f, \mathcal{F}_f^\phi) \). 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 \( f(X) = \pi_1X + \ldots, g(X) = \pi_2X + \ldots \) be in \( F_\xi \). Let \( a \in \mathcal{O}_{F'} \) satisfy
\[
[a]_{f,g} \equiv \lambda \mod X^2.
\]
Then there exists a unique power series \( [a]_{f,g} \in \mathcal{O}_{F'}[[X]] \) such that
\[
(i) \quad [a]_{f,g} \equiv aX \mod X^2,
(ii) \quad [a]_{f,g} \circ f = g \circ [a]_{f,g}.
\]
Moreover, \( [a]_{f,g} \in \text{Hom}(\mathcal{F}_f, \mathcal{F}_g) \). The map
\[
\{ a \in \mathcal{O}_{F'} \mid a^{\phi-1} = \pi_2/\pi_1 \} \to \text{Hom}(\mathcal{F}_f, \mathcal{F}_g), \quad a \mapsto [a]_{f,g}
\]
is a group isomorphism and in the case \( f = g \) a ring isomorphism \( \mathcal{O}_F \simeq \text{End}(\mathcal{F}_f) \). Furthermore, if \( h(X) = \pi_3X + \ldots \in F_\xi \) and \( b^{\phi-1} = \pi_3/\pi_2 \), then
\[
[ab]_{f,h} = [b]_{g,h} \circ [a]_{f,g}.
\]

In the sequel we shall always write \([a]_f \) for \([a]_{f,f} \). For \( f(X) = \pi'X + \ldots \in F_\xi \) and \( i \geq 0 \), we put \( f^{(i)} = f^{\phi-1} \circ \ldots \circ f^{\phi} \circ f \). Then \( f^{(i)} \in \text{Hom}(\mathcal{F}_f, \mathcal{F}_{f^{\phi^i}}) \) and if \( vF(\xi) = d \), then \( f^{(d)} = [\xi]_f \in \text{End}(\mathcal{F}_f) \). Moreover, for \( \alpha \in \mathcal{O}_{F'} \) we write \( \alpha^{(i)} = \alpha^{\phi-1} \cdots \alpha^{\phi} \cdot \alpha \). It follows that \( f^{(i)}(X) = [\pi'^{(i)}]_{f,f^{\phi^i}}(X) \).

As usual we endow the set \( p_F \) with the structure of an \( \mathcal{O}_F \)-module, denoted by \( \mathcal{F}_f(p_F) \), by setting
\[
x +_F y := \mathcal{F}_f(x, y), \quad a \cdot x := [a]_f(x),
\]
for \( x, y \in p_F \) and \( a \in \mathcal{O}_F \).

We now fix \( \xi \in \mathcal{O}_F \) with \( vF(\xi) = d \) and a power series \( f(X) = \pi'X + \ldots \in F_\xi \). Let \( \pi \in \mathcal{O}_F \) be any prime element. For \( n \in \mathbb{N}_0 \) we define the group of \( p_F \)-torsion points of \( F_f \) by
\[
G_{f,n} = \{ x \in p_F \mid [a]_f(x) = 0, \forall a \in p_F^n \}
\]
\[
= \{ x \in p_F \mid [\pi^n]_f(x) = 0 \}
\]
\[
= \ker(f^{(n)} : \mathcal{F}_f(p_F) \to \mathcal{F}_{f^{\phi^n}}(p_F))
\]
(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 $\alpha \in G_{f,n} \setminus G_{f,n-1}$ generates $F_{\xi,n}$ over $F'$ and, in addition, $\alpha$ is a uniformizer for $F_{\xi,n}$. This implies that $O_{F_{\xi,n}} = O_{F'}[\alpha]$. 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 $r, m \geq 1$ and set $G = G_{f,m}$. We choose a primitive $p^r$-torsion point $\beta$ (i.e. $\beta \in G_{f,r} \setminus G_{f,r-1}$) and set

$$\Gamma = \{\gamma \in p^r \mid f^{(m)}(\gamma) = \beta\}.$$ 

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 $\Gamma$ now satisfy the axioms postulated in 1.1, where $\Omega := \Omega_K$ acts on $G$ and $\Gamma$ through Galois automorphisms (thus we also write $\omega(g)$ and $\omega(\gamma)$ instead of $\omega g$ and $\omega \gamma$), and where $G$ acts on $\Gamma$ by translation:

$$\omega \gamma = g + f \gamma,$$

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

As in Sections 1–5 we set

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

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 $r \geq m \geq 1$. Then the following assertions hold:

(a) The map

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

is an isomorphism of $K$-algebras.

(b) One has $A = KG$.

(c) The map

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

where $\omega_g$ is uniquely determined by $(\omega_g)_{\gamma_0} = g_{\gamma_0}$ ($= g + f \gamma_0$), is a group isomorphism.

(d) Identifying $G$ and $\text{Gal}(L/K)$ as in (c), the map $\tau$ 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 $\Omega$ acts transitively on $\Gamma$. 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 $\beta$ is a uniformizer in $K$, $h(x)$ is an Eisenstein polynomial and therefore irreducible. Hence the Galois group $\Omega$ 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
\[
\omega_{(g+h)}(\gamma_0) = (g + f h) + f \gamma_0 = g + f \omega_h(\gamma_0) = \omega_h(g + f \gamma_0) = \omega_h(\omega_g(\gamma_0)) = (\omega_g(\omega_h)(\gamma_0)),
\]
since $g \in K$ and $\Omega/\Omega_L$ is an abelian group. This implies that the map $g \mapsto \omega_g$ is a group homomorphism, which is bijective, since $G$ and $\Omega$ act transitively on $\Gamma$.

(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 $g \in G$. \hfill \Box

Of course, the map $\tau$ of Lemma 6.2 is an isomorphism of $K$-algebras for arbitrary $m \geq 1$. The map in (c), however, is then no longer a homomorphism, but still a bijection. Via $\tau$ 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 $\tau$; 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
\[
s_i = \sum_{g \in G} g^i \in p_{F'}^m.
\]
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 $\pi^m$.

We recall that the associated order of $C$ in $A$ is defined by
\[
A^{\text{ass}} = \{a \in A \mid C \cdot a \subseteq C\}.
\]
Motivated by [T1, Theorem 3] we will prove that $A^{gss}$ coincides with the Cartier dual of the $O_K$-Hopf order which represents the $O_K$-group scheme of $p_F$-torsion on $F_f$. This affine group scheme is represented by the $O_K$-Hopf order

$$B^{gs} = \frac{O_K[[X]]}{(f^m(X))}.$$ 

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

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

$$D^{-1}(B^{gs}) = \{ b \in B \mid Tr_{B/K}(bB^{gs}) \subseteq O_K \}.$$ 

6.4. Lemma. The inverse different of $B^{gs}$ is given by

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

Proof. The set $\{1, X, \ldots, X^{q^m-1}\}$ constitutes an $O_K$-basis of $B^{gs}$ and also an $K$-basis of $B$. Let $b = \sum_{i=0}^{q^m-1} a_i X^i \in B$, $a_i \in K$. Then:

\begin{equation}
 b \in D^{-1}(B^{gs}) \iff \sum_{i=0}^{q^m-1} a_i \sum_{g \in G} g^{i+j} \in O_K \text{ for } j = 0, \ldots, q^m - 1.
\end{equation}

From Proposition 6.3 it follows immediately that $\frac{1}{\pi'(m)} B^{gs} \subseteq D^{-1}(B^{gs})$. For the converse inclusion we set $v_0 = \min\{v_P(a_i) \mid i = 0, \ldots, q^m - 1\}$ and $i_0 = \min\{i \mid v_P(a_i) = v_0\}$, where $v_P$ is the extension to $\overline{F}$ of the normalized valuation $v_F$. Then (18) implies for $j = q^m - 1 - i_0$:

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

Again from Proposition 6.3 we conclude that the $v_P$-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 $D^{-1}(B^{gs}) \subseteq \frac{1}{\pi'(m)} B^{gs}$.  

In what follows, the elements of $G$ play two different roles in the group algebra $\overline{F}G$: 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

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

It is immediate that these elements are $\Omega$-invariant.

6.5. **Proposition.** The Cartier dual $A^{gs}$ of $B^{gs}$ is given by

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

**Proof.** For the proof of the first equality we follow very closely the proof of [T2, Prop. 1]. Since the trace pairing

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

is non-degenerate we have a natural isomorphism

$$\xi : D^{-1}(B^{gs}) \to \text{Hom}_{\mathcal{O}_K}(B^{gs}, \mathcal{O}_K),$$

$$d \mapsto (b \mapsto \xi(d)(b) = \text{Tr}_{B/K}(db)).$$

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

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

if $h(b) = \sum_{g \in G} a_g b(g), \forall b \in B^{gs}$. Thus for $d \in D^{-1}(B^{gs})$ 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 $l \in B^{gs}$ by

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

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 \( \{1, \ldots, \bar{x}^{q^m-2}, l\} \) also forms an \( \mathcal{O}_K \)-basis of \( B_{g^s} \). Now the second equality is an immediate consequence of the first one and Lemma 6.3.

Our aim is to show that \( A_{g^s} \) is equal to the associated order \( A_{\text{ass}} \). The following lemma is a first step in this direction.

6.6. Lemma. ([CT, Ch. X, Lemma 3.5] The elements \( \sigma_i, i \geq 0 \), are contained in \( A_{\text{ass}} \). In particular, \( A_{g^s} \subseteq A_{\text{ass}} \).

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 \( C \) identifies via \( \tau \) with the ring of integers \( \mathcal{O}_L \) in \( L \). Since \( \mathcal{O}_L = \mathcal{O}_K[\gamma_0] \), it suffices to show that

\[
\tau(c_{\gamma_0^k} \cdot \sigma_i) \in C
\]

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

\[
\tau(c_{\gamma_0^k} \cdot \sigma_i) = \frac{1}{\pi^i(m)} \sum_{g \in G} x_g^i (c_{\gamma_0^k}(\gamma_0 + f g) - c_{\gamma_0^k}(\gamma_0))
\]

\[
= \frac{1}{\pi^i(m)} \sum_{g \in G} x_g^i ((\omega g)^k - \gamma_0^k)
\]

\[
= \frac{1}{\pi^i(m)} \sum_{g \in G} x_g^i (\mathcal{F}_f(\gamma_0, g)^k - \gamma_0^k)
\]

\[
= \frac{1}{\pi^i(m)} \sum_{g \in G} x_g^i \cdot g \mathcal{F}_1(\gamma_0, g),
\]

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

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

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

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 \( i \geq 0 \). Then

\[
\frac{1}{\pi^i(m)} \sum_{g \in G} g^i \chi(g) \in \mathcal{O}_F.
\]

Proof. Each \( \chi \in \hat{G} \) induces a homomorphism \( A \to \bar{F} \) of \( F \)-algebras, which we again denote by \( \chi \). Together with Lemma 6.6, this implies that

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

is integral over \( \mathcal{O}_F \). Now we easily deduce the integrality of \( \frac{1}{\pi^i(m)} \sum_{g \in G} g^i \chi(g) \) from Proposition 6.3. \( \square \)

Now that we know that the Hopf order \( \mathcal{A}^{gs} \) acts on \( C \) we can apply the results of [CH] to show that \( C \) is a free \( \mathcal{A}^{gs} \)-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

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

Recall the definition of \( \sigma_i \) 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 "\( \supset \)" 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 \( \mathcal{A}^{gs} \) is generated by \( g_0, \sigma_0, \ldots, \sigma_{q^m-1} \) we obtain the condition

\[
a \in I \iff \sigma_i \cdot \sum_{g \in G} \lambda_g g = 0 \quad \text{for } i = 0, \ldots, q^m - 2.
\]

On multiplying and comparing coefficients we derive

\[
\sum_{g \in G \setminus \{g_0\}} x_i^g (\lambda_{hg^{-1}} - \lambda_h) = 0,
\]

for all \( i = 0, \ldots, q^m - 2 \) and \( h \in G \). The Vandermonde matrix \( (x_i^g)_{i=0,\ldots,q^m-2, g \in G \setminus \{g_0\}} \) 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 \( \pi^m \) is the highest possible denominator for elements in \( \mathcal{A}^{gs} \). \( \square \)
6.9. Corollary. The associated order $A^{\text{ass}}$ is equal to $A^{\text{gs}}$ and $C$ is free of rank one over $A^{\text{ass}}$.

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

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

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

6.10. Theorem. For each $\chi \in \hat{G}$ one has

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

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

Proof. First we note that

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

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

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

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

$$\frac{f^{(m)}(g + fX)}{g + fX} = \sum_{i=0}^{\infty} q_i(g) X^i,$$
where \( q_i \in \mathcal{O}_{F^v}[[X]] \), \( i \in \mathbb{N}_0 \), are power series depending only on the formal group \( \mathcal{F}_f \). Hence we may deduce

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

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

Consider the map

\[ c : \Gamma \to \bar{F}, \quad \gamma \mapsto \frac{f^{(m)}(\gamma)}{\gamma}. \]

Since \( f^{(m)}(X) \in \mathcal{O}_{F^v}[[X]] \), it is \( \Omega \)-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:

\[
(c, \chi)_{\gamma_0} = \sum_{g \in G} c(g \gamma_0) \chi(g^{-1}) = \sum_{g \in G} \frac{f^{(m)}(g + f \gamma_0)}{g + f \gamma_0} \chi(g^{-1})
\]

\[
= \sum_{g \in G} \frac{f^{(m)}(\gamma_0)}{g + f \gamma_0} = R_X(\gamma_0).
\]

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

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

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

for all \( \chi \in \hat{G} \).

(b) Any function \( c_x \in C \) with \( x \in L^X \) having \( v_L \)-valuation \( q^m - 1 \) is an \( \mathcal{A}^{\text{ass}} \)-basis of \( C \). In particular,

\[ C = c \cdot \mathcal{A}^{\text{ass}}. \]

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

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

with \( \mathcal{A}^\circ = (\mathcal{O}_F G)\Omega \). 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

$$[A^{\text{ass}} : A^0]^2 = d_B \pi^{mq^m}.$$  

(25)

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

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

(26)

and

$$[\mathcal{O}_{L'}G : \mathcal{O}_{L'} \otimes_{\mathcal{O}_K} A^0]_{\mathcal{O}_{L'}}^2 = d_B.$$  

(27)

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

$$\sum_{\omega \in \Omega / \text{stab}_\Omega(g_i)} \omega(x_{i,j}) \omega_i \quad (1 \leq i \leq r, 1 \leq j \leq r_i)$$

constitute an $\mathcal{O}_K$-basis of $A^0$, where $\{g_1, \ldots, g_r\} \subseteq G$ is a set of representatives for the $\Omega$-orbits of $G$ and $x_{i,1}, \ldots, x_{i,r_i}$ is an $\mathcal{O}_K$-basis of $\mathcal{O}_{K_i}$, with $K_i$ being the fixed field of $\text{stab}_\Omega(g_i)$.

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 $\{1 \otimes_{\mathcal{O}_K} g_0\} \cup \{1 \otimes_{\mathcal{O}_K} \sigma_1 \mid i = 0, \ldots, q^m - 2\}$ of $\mathcal{O}_{L'} \otimes_{\mathcal{O}_K} A^{\text{ass}}$ by means of the matrix

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

where we have set $G = \{g_0, g_1, \ldots, g_N\}$ 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

$$\det(S)^2 \sim \pm \pi^{-2mN} \prod_{j=1}^N \left. \left( \frac{d}{dX} \frac{h_m(X)}{X} \right) \right|_{X=g_j} = \pm \pi^{-2mN} \prod_{j=1}^N \frac{h'_m(g_j)}{g_j}.$$
Adapting the proof of [CT, Ch. X, Lemma 2.5] we can show that $h'_m(g_j) \sim \pi^{r(m)}$ for $j = 1, \ldots, N$. Furthermore $\prod_{j=1}^{N} g_j$ is associated to the leading coefficient of $f^{(m)}(X)$, which is $\pi^{r(m)}$. 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 $C = c \cdot \mathcal{A}^{\text{ass}}$. Note that $v_L(\theta) = q^m - 1$ since $\gamma_0$ (resp. $\beta$) is a uniformizing element in $L$ (resp. $K$).

Let $x \in L^\times$ have $p_L$-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
\[ x \equiv u\theta \mod p_K \mathcal{O}_L \quad \text{resp.} \quad c_x \equiv uc_\theta \mod p_K \mathcal{O}_L. \]
Together with (23) this implies
\[ C = c_x \cdot \mathcal{A}^{\text{ass}} + p_L \mathcal{O}_L. \]
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 $\mathcal{A}^{\text{ass}}$ is the maximal order $\mathcal{A}$ in $A$, and $d_A = \mathcal{O}_K$.

Proof. From Lemma 4.3 we know that
\[ [\mathcal{A} : \mathcal{A}^\circ]_{\mathcal{O}_K}^2 = dBd_A^{-1}p^{mp^m}, \]
whereas from (25) we obtain
\[ [\mathcal{A}^{\text{ass}} : \mathcal{A}^\circ]_{\mathcal{O}_K}^2 = dBp^{mp^m}. \]
Therefore $[\mathcal{A} : \mathcal{A}^{\text{ass}}]_{\mathcal{O}_K}^2 = d_A^{-1}$, which forces $\mathcal{A} = \mathcal{A}^{\text{ass}}$ and $d_A = \mathcal{O}_K$. \(\square\)

REFERENCES


LUBIN-TATE FORMAL GROUPS


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