Local Leopoldt's Problem for Rings of Integers in Abelian p-Extensions of Complete Discrete Valuation Fields

M. V. Bondarko

Received: April 12, 2000
Revised: December 8, 2000

Communicated by A. S. Merkurev

Abstract. Using the standard duality we construct a linear embedding of an associated module for a pair of ideals in an extension of a Dedekind ring into a tensor square of its fraction field. Using this map we investigate properties of the coefficient-wise multiplication on associated orders and modules of ideals. This technique allows to study the question of determining when the ring of integers is free over its associated order. We answer this question for an Abelian totally wildly ramified p-extension of complete discrete valuation fields whose different is generated by an element of the base field. We also determine when the ring of integers is free over a Hopf order as a Galois module.

1991 Mathematics Subject Classification: 11S15, 11S20, 11S31
Keywords and Phrases: Complete discrete valuation (local) fields, additive Galois modules, formal groups, associated Galois modules

Introduction

0.1. Additive Galois modules and especially the ring of integers of local fields are considered from different viewpoints. Starting from H. Leopoldt [L] the ring of integers is studied as a module over its associated order. To be precise, if K is an extension of a local field k with Galois group being equal to G and $\mathfrak{O}_K$ is the ring of integers of K, then $\mathfrak{O}_K$ is considered as a module over $\mathfrak{A}_{K/k}(\mathfrak{O}_K) = \{\lambda \in k[G],\ \lambda\mathfrak{O}_K \subset \mathfrak{O}_K\}$.
One of the main questions is to determine when $\mathfrak{O}_K$ is free as an $\mathfrak{A}_{K/k}(\mathfrak{O}_K)$-module. Another related problem is to describe explicitly the ring $\mathfrak{A}_{K/k}(\mathfrak{O}_K)$ (cf. [Fr], [Chi], [CM]).

This question was actively studied by F. Bertrandias and M.-J. Ferton (cf. [Be], [B-F], [F1-2]) and more recently by M. J. Taylor, N. Byott and G. Lettl (cf. [T1], [By], [Le1]).

In particular, G. Lettl proved that if $K/\mathbb{Q}_p$ is Abelian and $k \subset K$, then $\mathfrak{O}_K \approx \mathfrak{A}_{K/k}(\mathfrak{O}_K)$ (cf. [Le1]). The proof was based on the fact that all Abelian extensions of $\mathbb{Q}_p$ are cyclotomic. So the methods of that paper and of most of preceding ones are scarcely applicable in more general situations.

M. J. Taylor [T1] considers intermediate extensions in the tower of Lubin-Tate extensions. He proves that for some of these extensions $\mathfrak{O}_K$ is a free $\mathfrak{A}_{K/k}(\mathfrak{O}_K)$-module. Taylor considers a formal Lubin-Tate group $F(X,Y)$ over the ring of integers $\mathfrak{o}$ of a local field k. Let π be a prime element of the field k and T_m be equal to $\operatorname{Ker}[\pi^m]$ in the algebraic closure of the field k. For $1 \le r \le m$, let L be equal to $k(T_{m+r})$, and let K be equal to $k(T_m)$, . Lastly, let q be the cardinality of the residue field of k.

Taylor proves that

(1) the ring $\mathfrak{O}_L$ is a free $\mathfrak{A}_{L/K}(\mathfrak{O}_L)$-module and any element of L whose valuation is equal to $q^r - 1$ generates it, and

(2) $\mathfrak{A}_{L/K}(\mathfrak{O}_L) = \mathfrak{O}_K + \sum_{i=0}^{q^r-2} \mathfrak{O}_K \sigma_i$, where $\sigma_i \in K[G]$ and are described explicitly (cf. the details in [T1], subsection 1.4).

This result was generalized to relative formal Lubin-Tate groups in the papers [Ch] and [Im]. Results of these papers were proved by direct computation. So these works do not show how one can obtain a converse result, i.e., how to find all extensions, that fulfill some conditions on the Galois structure of the ring of integers. To the best of author's knowledge the only result obtained in this direction was proved in [By1] and refers only to cyclotomic Lubin-Tate extensions.

0.2. In the examples mentioned above the associated order is also a Hopf order in the group algebra (i.e., it is an order stable under comultiplication). Several authors are interested in this situation. The extra structure allows to deal with wild extensions as if they were tame (in some sense). This is why in this situation, following Childs, one speaks of "taming wild extensions by Hopf orders". In the paper [By1], Byott proves that the associated order can be a Hopf order only in the case when the different of the extension is generated by an element of the smaller field. The present paper is also dedicated to extensions of this sort. More precisely, Theorem 4.4 of the paper [By1] implies that the order $\mathfrak{A}_{K/k}(\mathfrak{O}_K)$ can be a Hopf order (in the case when the ring $\mathfrak{O}_K$ is $\mathfrak{o}[G]$-indecomposable) only if K/k fulfills the stated condition on the different and $\mathfrak{O}_K$ is free over $\mathfrak{A}_{K/k}(\mathfrak{O}_K)$. Our main Theorem settles completely the question to determine when the order $\mathfrak{A}_{K/k}(\mathfrak{O}_K)$ is a Hopf order. It also describes completely Hopf orders that can be obtained as associated Galois orders. We shall also prove in subsection 3.4 that under the present assumptions if $\mathfrak{O}_K$ is free over $\mathfrak{A}_{K/k}(\mathfrak{O}_K)$, then $\mathfrak{A}_{K/k}(\mathfrak{O}_K)$ is a Hopf order and determine when the inverse different of an Abelian totally ramified p-extension of a complete discrete valuation field is free over its associated order (cf. [By1] Theorem 3.10).

In the first section we study a more general situation. We consider a Galois extension K/k of fraction fields of Dedekind rings, with Galois group G. We prove a formula for the module

$$\mathfrak{C}_{K/k}(I_1, I_2) = \mathrm{Hom}_{\mathfrak{o}}(I_1, I_2)\ ,$$

where I_1, I_2 are fractional ideals of K (this set also can be defined for ideals that are not G-stable) in Theorem 1.3.1. We introduce two submodules of $\mathfrak{C}_{K/k}(I_1, I_2)$:

$$\mathfrak{A}_{K/k}(I_1, I_2) = \{f \in k[G] | f(I_1) \subset I_2\}$$
$$\mathfrak{B}_{K/k}(I_1, I_2) = \mathrm{Hom}_{\mathfrak{o}[G]}(I_1, I_2),\ .$$

These modules coincide in the case when K/k is Abelian (cf. Proposition 1.4.2). We call these modules the *associated modules* for the pair I_1, I_2. In case $I_1 = I_2$ we call the associated module *associated order*.
In subsection 1.5 we define a multiplication on the modules of the type $\mathfrak{C}_{K/k}(I_1, I_2)$ and show the product of two such modules lies in some third one. We have also used this multiplication in the study of the decomposability of ideals in extensions of complete discrete valuation fields with inseparable residue field extension (cf. [BV]).
Starting from the second section we consider totally wildly ramified extensions of complete discrete valuation fields with residue field of characteristic p with the restriction on the different:

$$\mathfrak{D}_{K/k} = (\delta), \delta \in k \qquad (*).$$

This second section is dedicated to the study of conditions ensuring that the ring of integers $\mathfrak{O}_K$ is free over its associated order $\mathfrak{A}_{K/k}(\mathfrak{O}_K)$ or $\mathfrak{B}_{K/k}(\mathfrak{O}_K)$.
Let $n = [K : k]$.
We prove the following statement.

Proposition. *If in the associated order $\mathfrak{A}_{K/k}(\mathfrak{O}_K)$ ($\mathfrak{B}_{K/k}(\mathfrak{O}_K)$ resp.) there is an element ξ which maps some (and so, any) element $a \in \mathfrak{O}_K$ with valuation equal to $n-1$ onto a prime element of the ring $\mathfrak{O}_K$, then $\mathfrak{O}_K \approx \mathfrak{A}_{K/k}$ (resp. $\mathfrak{B}_{K/k}$) and besides that $\mathfrak{A}_{K/k}$ (resp. $\mathfrak{B}_{K/k}$) has a "power" base (in the sense of multiplication $\overset{\Delta}{*}$, cf. the second section), which is constructed explicitly using the element ξ.*

The converse to this statement is also proved in the case when $\mathfrak{A}_{K/k}(\mathfrak{O}_K)$ (resp. $\mathfrak{B}_{K/k}(\mathfrak{O}_K)$) is indecomposable (cf. the Theorems 2.4.1, 2.4.2). An important part of our reasoning is due to Byott (cf. [By1]).

0.3. The third, fourth and fifth sections are dedicated to proving a more explicit form of the condition of the second section for the Abelian case. The main result of the paper is the following one. We will call an Abelian p-extension of complete discrete valuation fields of characteristic 0 *almost maximally ramified* if its degree divides the different.

Theorem A. *Let K/k be an Abelian totally ramified p-extension of p-adic fields, which in case* $\operatorname{char} k = 0$ *is not almost maximally ramified, and suppose that the different of the extension is generated by an element in the base field (see (*)). Then the following conditions are equivalent:*
1. The extension K/k is Kummer for a formal group F, that there exists a formal group F over the ring of integers $\mathfrak{o}$ of the field k, a finite torsion subgroup T of the formal module $F(\mathfrak{M}_{\mathfrak{o}})$ and a prime element π_0 of k such that $K = k(x)$, where x is a root of the equation $P(X) = \pi_0$, where

$$P(X) = \prod_{t \in T} (X \underset{F}{-} t) \ .$$

2. The ring $\mathfrak{O}_K$ is isomorphic to the associated order $\mathfrak{A}_{K/k}(\mathfrak{O}_K)$ as an $\mathfrak{o}[G]$-module.

Remark 0.3.1. Besides proving Theorem A we will also construct the element ξ explicitly and so describe $\mathfrak{A}_{K/k}(\mathfrak{O}_K)$ (cf. the theorems of §2).

Remark 0.3.2. IF k is of characteristic 0 the fact that $\mathfrak{O}_K$ is indecomposable as an $\mathfrak{o}[G]$-module if and only if K/k is not almost maximally ramified, was proved in [BVZ]. The case of almost maximally ramified extensions is well understood (cf., for example, [Be]). It is obvious, that in the case $\operatorname{char} k = p$ the ring $\mathfrak{O}_K$ is indecomposable as an $\mathfrak{o}[G]$-module, because in this case the algebra $k[G]$ is indecomposable.

Remark 0.3.3. In the paper [CM] rings of integers in Kummer extensions for formal groups are also studied as modules over their associated orders. In that paper Kummer extensions are defined with the use of homomorphisms of formal groups. For extensions obtained in this way freeness of the ring of integers over its associated orders is proved. Childs and Moss also use some tensor product to prove their results. Yet their methods seem to be inapplicable for proving inverse results.
Our notion of a Kummer extension for a formal group is essentially equivalent to the one in [CM]. We however only use one formal group and do not impose finiteness restriction on its height.
Besides we consider also the equal characteristic case i.e., $\operatorname{char} k = \operatorname{char} \overline{k} = p$. Using the methods presented here one can prove that we can actually take the formal group F in Theorem A of finite height. Yet such a restriction does not seem to be natural.

Remark 0.3.4. Theorem A shows which Hopf orders can be associated to Galois orders for some Abelian extensions. The papers of mathematicians that "tame wild extensions by Hopf orders" do not show that their authors know or guess that such an assertion is valid.
In the third section we study the fields that are Kummer in the sense of part 1 of Theorem A and deduce 2 from 1. In the fourth section we prove that we can suppose the coefficient b_1 in $\xi = \delta^{-1} \sum b_\sigma \sigma$ to be equal to 0. Further, if

b_1 is equal to 0, then we show that there exists a formal group F over $\mathfrak{o}$, such that for $\sigma \in G$ the b_σ, form a torsion subgroup in the formal module $F(\mathfrak{M}_\mathfrak{o})$, i.e.,

$$b_\sigma \underset{F}{+} b_\tau = b_{\sigma\tau} \ .$$

In the fifth section we prove that if $b_\sigma \underset{F}{+} b_\tau$ is indeed equal to $b_{\sigma\tau}$, then K/k is Kummer for the group F.

0.4. This paper is the first in a series of papers devoted to associated orders and associated modules. The technique introduced in this paper (especially the map ϕ and the multiplication $*$ defined below) turns out to be very useful in studying The Galois structure of ideals. It allows the author to prove in another paper some results about freeness of ideals over their associated orders in extensions that do not fulfill the condition on the different (*). In particular, using Kummer extensions for formal groups we construct a wide variety of extensions in which some ideals are free over their associated orders. These examples are completely new. We also calculate explicitly the Galois structure of all ideals in such extensions. Such a result is very rare. In a large number of cases the necessary and sufficient condition for an ideal to be free over its associated order is found.

The author is deeply grateful to professor S. V. Vostokov for his help and advice.
The work paper is supported by the Russian Fundamental Research Foundation N 01-00-000140.

§1 General results

Let
$\mathfrak{o}$ be a Dedekind ring,
k be the fraction field of the ring $\mathfrak{o}$,
K/k be a Galois extension with Galois group equal to G,
$\mathfrak{D} = \mathfrak{D}_{K/k}$ be the different of the extension K/k,
$n = [K : k]$,
tr be the trace operator in K/k.
We also define some associated modules.
For I_1 and I_2 G-stable ideals in K put
$\mathfrak{B}_{K/k}(I_1, I_2) = \mathrm{Hom}_{\mathfrak{o}[G]}(I_1, I_2)$. For I_1, I_2 not being G-stable one can define

$$\mathfrak{B}_{K/k}(I_1, I_2) = \{f \in \mathrm{Hom}_{\mathfrak{o}[G]}(K, K),\ f(I_1) \subset I_2\}.$$

For arbitrary $I_1, I_2 \subset K$ we define
$\mathfrak{A}_{K/k}(I_1, I_2) = \{f \in k[G] | f(I_1) \subset I_2\}$,
$\mathfrak{C}_{K/k}(I_1, I_2) = \mathrm{Hom}_\mathfrak{o}(I_1, I_2)$.
Obviously, any $\mathfrak{o}$-linear map from I_1 into I_2 can be extended to a k-linear homomorphism from K into K. The dimension of $\mathrm{Hom}_k(K, K)$ over k is equal to n^2. Now we consider the group algebra $K[G]$. This algebra acts on K and

the statement in (Bourbaki, algebra, §7, no. 5) implies that a non-zero element of $K[G]$ corresponds to a non-zero map from K into K. Besides the dimension of $K[G]$ over k is also equal to n^2. It follows that any element of $\mathrm{Hom}_k(K,K)$ can be expressed uniquely as an element of $K[G]$. So we reckon $\mathfrak{C}_{K/k}(I_1,I_2)$ being embedded in $K[G]$.

1.1. We consider the G-Galois algebra $K\otimes_k K$. It is easily seen that the tensor product $K\otimes_k K$ is isomorphic to a direct sum of n copies of K as a k-algebra. Being more precise, let $K_\sigma,\ \sigma\in G$ denote a field, isomorphic to K.

Lemma 1.1.1. *There is an isomorphism of K-algebras*

$$\psi:\ K\otimes_k K\to\sum_{\sigma\in G}K_\sigma,$$

where $\psi=\sum_\sigma\psi_\sigma$ and ψ_σ is the projection on the coordinate σ, defined by the equality

$$\psi_\sigma(x\otimes y)=x\sigma(y)\in K_\sigma.$$

The proof is quite easy, you can find it, for example, in "Algebra" of Bourbaki. Also see 1.2 below.
Now we construct a map ϕ from the G-Galois algebra $K\otimes_k K$ into the group algebra $K[G]$:

$$\phi: K\otimes_k K\to K[G]$$

(1)
$$\alpha=\sum_i x_i\otimes y_i\to\phi(\alpha)=\sum_i x_i\left(\sum_{\sigma\in G}\sigma(y_i)\sigma\right).$$

It is clear that $\phi(\alpha)$ as a function acts on K as follows:

(2)
$$\phi(\alpha)(z)=\sum_i x_i tr(y_i z),\ z\in K.$$

Besides that, the map ϕ may be expressed through ψ_σ in the form

(3)
$$\phi(\alpha)=\sum_\sigma\psi_\sigma(\alpha)\sigma,\ \alpha\in K\otimes_k K.$$

Proposition 1.1.2. *The map ϕ is an isomorphism of k-vector spaces between $K\otimes_k K$ and $K[G]$.*

Cf. the sketch of the proof in Remark 1.2 below.

1.2 Pairings on $K\otimes_k K$ and $K[G]$.
There is a natural isomorphism of the k-space K and its dual space of k-functionals:

$$K\to\widehat{K}$$
$$a\to f_a(b)=\mathrm{tr}(ab).$$

We define a pairing $\langle , \rangle_\otimes$ on $K \otimes_k K$, that takes its values in k:

$$(K \otimes_k K) \times (K \otimes_k K) \to k$$
$$\langle a \otimes b, c \otimes d \rangle_\otimes \to (f_a \otimes f_c)(b \otimes d) = (\operatorname{tr} ac)(\operatorname{tr} bd).$$

This pairing is correctly defined and is non-degenerate. The second fact is easily proved with the use of dual bases.
We also define a pairing on $K[G]$ that takes its values in k:

$$K[G] \times K[G] \to k$$
$$\alpha = \sum_\sigma a_\sigma \sigma,\ \beta = \sum_\sigma b_\sigma \sigma \to \sum_\sigma \operatorname{tr} a_\sigma b_\sigma = \langle \alpha, \beta \rangle_{K[G]}.$$

The pairing $\langle , \rangle_{K[G]}$ is also non-degenerate because it is a direct sum of $n = [K : k]$ non-degenerate pairings

$$K \times K \to k$$
$$(a, b) \to \operatorname{tr} ab.$$

We check that for any two x, y the following equality is fulfilled:

$$\langle x, y \rangle_\otimes = \langle \phi(x), \phi(y) \rangle_{K[G]}. \tag{4}$$

Indeed, it follows from linearity that it is sufficient to prove that for $x = a \otimes b,\ y = c \otimes d$. In that case we have

$$\langle a \otimes b, c \otimes d \rangle_\otimes = \operatorname{tr} ac \operatorname{tr} bd,$$

and besides that

$$\begin{aligned} &\langle \phi(a \otimes b), \phi(c \otimes d) \rangle_{K[G]} \\ &= \langle a \sum_\sigma \sigma(b)\sigma, c \sum_\sigma \sigma(d)\sigma \rangle_{K[G]} \\ &= \sum_\sigma \operatorname{tr}(ac\sigma(bd)) = \sum_\sigma \sum_\tau \tau(ac\sigma(bd)) \\ &= \sum_\tau \sum_\sigma \tau(ac)\tau\sigma(bd) = \operatorname{tr} ac \operatorname{tr} bd. \end{aligned}$$

and the equality (4) is proved.

Remark 1.2. It follows from (4) that the map ϕ from (1) is an injection. Indeed, let $\phi(\alpha)$ be equal to 0 for $\alpha \in K \otimes_k K$, then $\langle \phi(\alpha), \phi(\beta) \rangle_{K[G]} = 0$ for any $b \in K \otimes_k K$. So, according to (4), $\langle \alpha, \beta \rangle_\otimes = 0$ for any $\beta \in K \otimes_k K$. From the non-degeneracy of the pairing $\langle , \rangle_\otimes$ it follows that $\alpha = 0$. That implies $\operatorname{Ker}(\phi) = 0$.
Using the equality of dimensions we can deduce that ϕ is an isomorphism.

1.3 Modules of homomorphisms for a pair of ideals.
Let I_1, I_2 be fractional ideals of the field K.

Theorem 1.3.1. *Let ϕ be the bijection from (1) and let $I_1^* = \mathfrak{D}^{-1}I_1^{-1}$ (this is dual of I_1 for the bilinear trace form on K). For the associated modules the following equality holds:*

$$\mathfrak{C}_{K/k}(I_1, I_2) = \phi(I_2 \otimes_{\mathfrak{o}} I_1^*) \ .$$

Proof. First we show that $\phi(I_2 \otimes_{\mathfrak{o}} I_1^*) \subset \mathfrak{C}_{K/k}(I_1, I_2)$. If $x \in I_2,\ y \in I_1^*$, then for any $z \in I_1$ we have, according to the definition (2):

$$\phi(x \otimes y)(z) = x\,\mathrm{tr}(yz) \in I_2,$$

since $x \in I_2$ and $\mathrm{tr}(yz) \in \mathfrak{o}$, which follows from the definition of I_1^* and of the different $\mathfrak{D}$.
Conversely, let $f \in \mathfrak{C}_{K/k}(I_1, I_2)$. We define a map θ_f and show that it is sent onto f by ϕ. Let:

$$\begin{aligned} \theta_f :\ & I_2^* \otimes_{\mathfrak{o}} I_1 \to \mathfrak{o} \\ & x \otimes y \to \mathrm{tr}(xf(y)). \end{aligned} \tag{5}$$

This map is correctly defined since $x \in I_2^* = \mathfrak{D}^{-1}I_2^{-1}$ and $f(y) \in I_2$, thus

$$\mathrm{tr}(xf(y)) \in \mathfrak{o}.$$

For a $\mathfrak{o}$-module M we denote by $\widehat{M}$ the module of $\mathfrak{o}$-linear functions from M into $\mathfrak{o}$. It is clear that

$$\theta_f \in (\widehat{I_2^* \otimes_{\mathfrak{o}} I_1}). \tag{6}$$

We identify the ideal I_2 with the $\mathfrak{o}$-module $\widehat{I_2^*}$ via:

$$\begin{aligned} I_2 &\to \widehat{I_2^*} \\ a \to f_a &= \sum_{\sigma \in G} \sigma(a)\sigma. \end{aligned}$$

Obviously $f_a(z) = \mathrm{tr}(az)$ for any $z \in \widehat{I_2}$.
In a completely analogous way we identify I_1^* with $\widehat{I_1^*}$
Using these identifications and the fact that I_1 and I_2^* are projective $\mathfrak{o}$-modules we obtain an isomorphism

$$\begin{aligned} I_2 \otimes_{\mathfrak{o}} I_1^* &\to (\widehat{I_2^* \otimes_{\mathfrak{o}} I_1}) \\ a \otimes b &\to h_{a,b}, \end{aligned} \tag{7}$$

where $h_{a,b}(x \otimes y) = \langle a \otimes b, x \otimes y \rangle_\otimes = (\operatorname{tr} ax)(\operatorname{tr} by)$ for all x in I_2^* and y in I_1. The map θ_f in (5) lies in $(\widehat{I_2^* \otimes_\mathfrak{o} I_1})$ (cf. (6)), and so, according to the isomorphism (7), it corresponds to an element α_f in $I_2 \otimes_\mathfrak{o} I_1^*$, i.e.,

$$\alpha_f = \sum_i a_i \otimes b_i, \; a_i \in I_2, \; b_i \in I_1^*.$$

Then (7) implies that the functional h_{α_f}, that corresponds to the element α_f, is defined in the following way:

$$h_{\alpha_f}(x \otimes y) = \langle \alpha_f, x \otimes y \rangle_\otimes = \sum_i \operatorname{tr} a_i x \operatorname{tr} b_i y.$$

On the other hand, from the definition of θ_f (cf. (5)) we obtain:

$$h_{\alpha_f}(x \otimes y) = \theta_f(x \otimes y) = \operatorname{tr}(xf(y)).$$

It follows that $f(y) = \sum_i a_i \operatorname{tr}(b_i y)$. So we have

$$f = \phi(\sum a_i \otimes b_i),$$

and for any f in $\mathfrak{C}_{K/k}(I_1, I_2)$ we have found its preimage in $I_2 \otimes I_1^*$, i.e.,

$$\mathfrak{C}_{K/k}(I_1, I_2) \subset \phi(I_2 \otimes_\mathfrak{o} I_1^*).$$

The theorem is proved. □

Remark 1.3.2. In the same way as above we can prove, that if we replace the ideals I_1, I_2 by two arbitrary free $\mathfrak{o}$-submodules X and Y of K of dimension n, then we will obtain the following formula:

$$\mathfrak{C}_{K/k}(X, Y) = \phi(Y \otimes \widehat{X}),$$

where $\widehat{X}$ is the dual module to X in K with respect to the pairing $K \times K \to k$ defined by the trace tr.

Remark 1.3.3. All elements in $\mathfrak{C}_{K/k}(I_1, I_2)$, $\mathfrak{A}_{K/k}(I_1, I_2)$, $\mathfrak{B}_{K/k}(I_1, I_2)$ have unique extensions to k-linear maps from K to K. To be more precise, if $f : I_1 \to I_2$ is an $\mathfrak{o}$-homomorphism, then for all $x \in K$ we can assume $f(x) = \alpha f(a)$ if $x = \alpha a$, $\alpha \in k$, $a \in I_1$. It is easily seen that the map we obtained in this way is a correctly defined k-linear homomorphism from K into K.

1.4. Now we compare the modules $\mathfrak{A}$ and $\mathfrak{B}$.

Proposition 1.4.

$$\mathfrak{A}_{K/k}(I_1, I_2) = \mathfrak{B}_{K/k}(I_1, I_2) \tag{8}$$

if and only if K/k is an Abelian extension.

Proof. 1. Let K/k be an Abelian extension. To verify the equality (8) in this case, let first f belong to $\mathfrak{A}_{K/k}(I_1, I_2)$, then f is an $\mathfrak{o}$-homomorphism from I_1 into I_2. Besides that, f commutes with all elements of G since G is an Abelian group, i.e., $\sigma f(a) = f(\sigma(a))$ for all $\sigma \in G$ and $a \in I_1$. So we obtain that f is an $\mathfrak{o}[G]$-homomorphism from I_1 into I_2, thus $f \in \mathfrak{B}_{K/k}(I_1, I_2)$.
For the reverse inclusion, let f belong to $\mathfrak{B}_{K/k}(I_1, I_2)$. Then f induces an $\mathfrak{o}[G]$-homomorphism from K into K. We take an element x that generates a normal base of the field K over k. Then there exists an element $g \in k[G]$ such that $f(x) = g(x)$, to be more precise, if $f(x) = \sum_\sigma a_\sigma \sigma(x),\ a_\sigma \in k$ then we take $g = \sum a_\sigma \sigma$. We consider the $\mathfrak{o}[G]$-homomorphism g from K into K. Since G is an Abelian group, $f(\sigma(x)) = \sigma(f(x)) = \sigma(g(x)) = g(\sigma(x))$ for any $\sigma \in G$. We obtain that k-homomorphisms f and g coincide on the basic elements and so $f = g \in k[G]$ and $f(I_1) \subset I_2$, i.e., $f \in \mathfrak{A}_{K/k}(I_1, I_2)$.
2. Now we suppose that $\mathfrak{A}_{K/k}(I_1, I_2) = \mathfrak{B}_{K/k}(I_1, I_2)$ and check that K/k is an Abelian extension. Indeed, since $k\mathfrak{A}_{K/k}(I_1, I_2) = k[G]$, $\mathfrak{A}_{K/k}(I_1, I_2)$ contains elements of the form $a\sigma$, where $a \in k^*$, for any $\sigma \in G$. It follows from our assumption that $a\sigma \in \mathfrak{B}_{K/k}(I_1, I_2)$, and so $a\sigma$ is an $\mathfrak{o}[G]$-homomorphism. We obtain that G commutes with all elements $\sigma \in G$. Proposition is proved. $\square$

Proposition 1.5. *If we assume the action of G on $K \otimes_k K$ to be diagonal, then*

$$\mathfrak{B}_{K/k}(I_1, I_2) = \phi((I_2 \otimes_o I_1^*)^G)\ .$$

Proof. Let α belong to $(I_2 \otimes_\mathfrak{o} I_1^*)^G$. We have to show that $\phi(a)$ is an $\mathfrak{o}[G]$-homomorphism from I_1 into I_2. This means that

$$\sigma\phi(a)(z) = \phi(a)(\sigma(z))$$

for all $z \in I_1$. Let α be equal to $\sum a_i \otimes b_i,\ a_i \in I_2,\ b_i \in I_1^*$. Then from the definition of ϕ (cf. (2)) it follows that

$$\begin{aligned}\phi(a)(\sigma(z)) &= \sum_i a_i \operatorname{tr}(b_i\sigma(z)) \\ &= \sum_i a_i \operatorname{tr}(\sigma^{-1}(b_i)\sigma(z)) = \phi\left(\sum_i a_i \otimes \sigma^{-1}(b_i)\right)(z).\end{aligned}$$

On the other hand,

$$\sigma\phi(a)(z) = \sigma\left(\sum a_i \operatorname{tr}(b_i z)\right)$$
$$= \sum(\sigma(a_i)\operatorname{tr}(b_i z)) = \phi\left(\sum \sigma(a_i) \otimes b_i\right)(z).$$

From the G-invariance of the element α it follows that

$$\phi\left(\sum a_i \otimes \sigma^{-1}(b_i)\right) = \phi\left(\sum \sigma(a_i) \otimes \sigma(\sigma^{-1}(b_i))\right) = \phi\left(\sum \sigma(a_i) \otimes b_i\right).$$

Thus $\phi(\alpha)(\sigma(z)) = \sigma\phi(\alpha)(z)$ for any $\sigma \in G$, i.e., $\phi(\alpha) \in \mathfrak{B}_{K/k}(I_1, I_2)$.
Conversely, let f belong to $\mathfrak{B}_{K/k}(I_1, I_2)$, then $f \in \mathfrak{C}_{K/k}(I_1, I_2)$ and so, according to Theorem 1.3.1, there is an $\alpha \in I_2 \otimes I_1^*$, such that $f = \phi(\alpha)$. It remains to check that α is G-invariant. We use the fact that f is an G-homomorphism, i.e., $\sigma f(z) = f(\sigma z)$ for all $\sigma \in G$ and $z \in I_1$. We obtain an equality $\sigma\phi(\alpha)(z) = \phi(\alpha)(\sigma z)$. By writing the left and the right side of the equality as above we obtain for $\alpha = \sum a_i \otimes b_i$:

$$\begin{aligned}\sigma\phi(\alpha)(z) &= \phi\left(\sum \sigma a_i \otimes \sigma(\sigma^{-1} b_i)\right)(z)\\ \phi(\alpha)(\sigma z) &= \phi\left(\sum a_i \otimes \sigma^{-1} b_i\right)(z).\end{aligned}$$

It follows that

$$\phi\left(\sum \sigma a_i \otimes \sigma(\sigma^{-1} b_i)\right) = \phi\left(\sum a_i \otimes \sigma^{-1} b_i\right).$$

Now using the fact that ϕ is a bijection we obtain

$$\sum \sigma a_i \otimes \sigma(\sigma^{-1} b_i) = \sum a_i \otimes \sigma^{-1} b_i.$$

We apply to both sides of the equality the map

$$\begin{aligned}1 \otimes \sigma :\ K \otimes_k K &\to K \otimes_k K\\ a \otimes b &\to a \otimes \sigma(b)\end{aligned},$$

that obviously is an homomorphism. We have

$$\sum \sigma a_i \otimes \sigma b_i = \sum a_i \otimes b_i,$$

i.e., $\sigma(\alpha) = \alpha$. □

1.6 The multiplication $*$ on $K[G]$.
On the algebra $K \otimes_k K$ there is a natural multiplication: $(a \otimes b) \cdot (c \otimes d) = ac \otimes bd$. Using it and the bijection ϕ we define a multiplication on $K[G]$. To be more precise, if $f, g \in K[G]$, then we define

$$f * g = \phi(\phi^{-1}(f) \cdot \phi^{-1}(g)) \in K[G]. \tag{9}$$

Proposition 1.6.1. *If* $f=\sum_\sigma a_\sigma\sigma$ *and* $g=\sum_\sigma b_\sigma\sigma$, *then*

$$f*g=\sum_\sigma a_\sigma b_\sigma\sigma.$$

Proof. Let f be equal to $\phi(\alpha)$, g be equal to $\phi(\beta)$, where $\alpha,\beta\in K\otimes_k K$. If $\alpha=\sum x_i\otimes y_i$, $\beta=\sum u_j\otimes v_j$, then from the definition of ϕ (cf. (1)) we obtain

$$\phi(\alpha)=\sum x_i\sum_\sigma \sigma y_i\sigma,\ \phi(\beta)=\sum u_j\sum_\sigma \sigma v_j\sigma.$$

It follows that

$$\sum_\sigma a_\sigma b_\sigma\sigma=\sum_{i,j}x_iu_j\sigma(y_iv_j)\sigma.$$

On the other hand,

$$f*g=\phi(\alpha\beta)=\phi\left(\sum_{i,j}(x_iu_i\otimes y_iv_j)\right)=\sum_{i,j}x_iu_j\sigma(y_iv_j)\sigma$$

and we obtain the proof of Proposition. □

Remark 1.6.2. The formula from Proposition 1.6.1 will be used further as an another definition of the multiplication $*$.

1.7 Multiplication on associated modules.
Now we consider the multiplication (9) on the different associated modules. Here we will see appearing the different which we will suppose to be induced from the base field in the following sections.

Proposition 1.7.1. *Let* f *belong to* $\mathfrak{C}_{K/k}(I_1,I_2)$, *and let* g *belong to* $\mathfrak{C}_{K/k}(I_3,I_4)$. *Then*

$$f*g\in\mathfrak{C}_{K/k}(I_1I_3\mathfrak{D},I_2I_4).$$

Proof. It is clear that $\phi^{-1}(f)$ and $\phi^{-1}(g)$ belong to $I_2\otimes_o I_1^*$ and $I_4\otimes I_3^*$ respectively. So we obtain that $\phi^{-1}(f)\phi^{-1}(g)$ lies in the product

$$(I_2\otimes_o I_1^*)(I_4\otimes_o I_3*)=I_2I_4\otimes_o(I_1^*I_3^*)$$
$$=I_2I_4\otimes_o\mathfrak{D}^{-2}I_1^{-1}I_3^{-1}=I_2I_4\otimes_o(\mathfrak{D}I_1I_3)^*.$$

So from the Theorem 1.3.1 it follows that $f*g$ belongs to $\mathfrak{C}_{K/k}(I_1I_3\mathfrak{D},I_2I_4)$. □

Now we study the multiplication $*$ on the modules $\mathfrak{B}_{K/k}$.

Proposition 1.7.2. *Let f belong to $\mathfrak{B}_{K/k}(I_1, I_2)$ and let g belong to $\mathfrak{B}_{K/k}(I_3, I_4)$, then*

$$f * g \in \mathfrak{B}_{K/k}(I_1 I_3 \mathfrak{D},\ I_2 I_4).$$

Proof. Since $\mathfrak{B}_{K/k}(I, J)$ is a submodule in $\mathfrak{C}_{K/k}(I, J)$, from Proposition 1.7 it follows that $f * g \in \mathfrak{C}_{K/k}(I_1 I_3 \mathfrak{D},\ I_2 I_4)$. From Proposition 1.5 we deduce that f and g belong to $phi(K \otimes_k K^G),\ g \in \phi(K \otimes_k K^G)$. So $f * g \in \phi(K \otimes_k K^G)$, and this implies that

$$f * g \in \mathfrak{C}_{K/k}(I_1 I_3 \mathfrak{D},\ I_2 I_4) \cap \phi(K \otimes_k K^G) = \mathfrak{B}_{K/k}(I_1 I_3 \mathfrak{D},\ I_2 I_4).$$

□

Proposition 1.7.3. *Let f belong to $\mathfrak{A}_{K/k}(I_1, I_2)$ and LET g belong to $\mathfrak{A}_{K/k}(I_3, I_4)$, then*

$$f * g \in \mathfrak{A}_{K/k}(I_1 I_3 \mathfrak{D},\ I_2 I_4).$$

Proof. From Proposition 1.7 it follows that

$$f * g \in \mathfrak{C}_{K/k}(I_1 I_3 \mathfrak{D},\ I_2 I_4) \tag{10}$$

since $\mathfrak{A}_{K/k}(I_1, I_2)$ and $\mathfrak{A}_{K/k}(I_3, I_4)$ are submodules OF $\mathfrak{C}_{K/k}(I_1, I_2)$ and $\mathfrak{C}_{K/k}(I_3, I_4)$ respectively.
From the definition of $\mathfrak{A}_{K/k}$ it follows that f and g belong to $k[G]$. So the coefficients of f and g lie in k, and from Proposition 1.6.1 it follows that $f * g$ also belongs to $k[G]$. Then (10) implies that

$$f * g \in \mathfrak{C}_{K/k}(I_1 I_3 \mathfrak{D},\ I_2 I_4) \cap k[G] = \mathfrak{A}_{K/k}(I_1 I_3 \mathfrak{D},\ I_2 I_4),$$

and thus the proposition is proved. □

§2 Isomorphism of rings of integers of totally wildly ramified extensions of complete discrete valuation fields with their associated orders.

2.1. Let K/k be a totally wildly ramified Galois extension of a complete discrete valuation field with residue field of characteristic p. Let $\mathfrak{D}$ be the different of the extension and let $\mathfrak{O}_K$ be the ring of integers of the field K. From this moment and up to the end of the paper we will suppose the condition (*) of the introduction to be fulfilled, i.e., that $\mathfrak{D} = (\delta)$, with $\delta \in k$. We will write $\mathfrak{A}_{K/k}(\mathfrak{O}_K),\ \mathfrak{B}_{K/k}(\mathfrak{O}_K)$ instead of $\mathfrak{A}_{K/k}(\mathfrak{O}_K, \mathfrak{O}_K),\ \mathfrak{B}_{K/k}(\mathfrak{O}_K, \mathfrak{O}_K)$.
We denote prime elements of the fields k and K by π_0 and π respectively, and their maximal ideals by $\mathfrak{M}_0$ and $\mathfrak{M}$.

PROPOSITION 2.1. *The modules $\mathfrak{C}_{K/k}(\mathfrak{O}_K)$, $\mathfrak{A}_{K/k}(\mathfrak{O}_K)$, $\mathfrak{B}_{K/k}(\mathfrak{O}_K)$ are $\mathfrak{o}$-algebras with a unit with respect to the multiplication*

$$f \overset{\Delta}{*} g = \delta f * g = \delta^{-1}\phi(\phi^{-1}(\delta f)\phi^{-1}(\delta g))$$

(cf. (9)). The unit is given by $\delta^{-1}tr$.

The motivation for the above definition is given by Theorem 2.4.1 below.

Proof. Let f and g belong to $\mathfrak{C}_{K/k}(\mathfrak{O}_K)$, then according to Proposition 1.7, the product $f * g$ maps the different $\mathfrak{D}$ into the ring $\mathfrak{O}_K$. It follows that $f \overset{\Delta}{*} g$ maps $\mathfrak{D}$ into $\mathfrak{D}$, and so it also maps $\mathfrak{o}$ into itself since $\mathfrak{D} = \delta\mathfrak{O}_K$. We obtain that $\overset{\Delta}{*}$ defines a multiplication on the each of the modules associated to $\mathfrak{O}_K$. Now we consider the element $\delta^{-1}\,\mathrm{tr}$ and prove that it is the unit for the multiplication $\overset{\Delta}{*}$ in each of these modules. It is clear that $\delta^{-1}\,\mathrm{tr}$ maps $\mathfrak{O}_K$ into itself and that $\delta^{-1}\,\mathrm{tr}$ belongs to $k[G]$, so $\delta^{-1}\,\mathrm{tr}$ belongs to $\mathfrak{A}_{K/k}(\mathfrak{O}_K)$. Besides that, $\delta^{-1}\,\mathrm{tr}$ commutes with all elements of G and so $\delta^{-1}\,\mathrm{tr}$ lies in $\mathfrak{B}_{K/k}(\mathfrak{O}_K)$.
Let now f belong to $K[G]$, then

$$f = \sum_\sigma a_\sigma \sigma,\ a_\sigma \in K,\ \delta^{-1}\,\mathrm{tr} = \sum_\sigma \delta^{-1}\sigma.$$

So, according to proposition 1.6.1,

$$f * (\delta^{-1}\,\mathrm{tr}) = \sum_\sigma \delta^{-1} a_\sigma \sigma$$

and we obtain

$$f \overset{\Delta}{*} (\delta^{-1}\,\mathrm{tr}) = \sum a_\sigma = f.$$

Since $\mathfrak{A}_{K/k}(\mathfrak{O}_K), \mathfrak{B}_{K/k}(\mathfrak{O}_K)$ are $\mathfrak{o}$-submodules in $\mathfrak{C}_{K/k}(\mathfrak{O}_K)$, $\delta^{-1}\,\mathrm{tr} \in \mathfrak{A}_{K/k}(\mathfrak{O}_K)$, $\mathfrak{B}_{K/k}(\mathfrak{O}_K)$, $\delta^{-1}\,\mathrm{tr}$ is also an identity in $\mathfrak{A}_{K/k}(\mathfrak{O}_K)$, $\mathfrak{B}_{K/k}(\mathfrak{O}_K)$ with respect to the multiplication $\overset{\Delta}{*}$.

2.2. Let as before n be equal to $[K : k]$.

LEMMA 2.2.1. *Let x be an element of the ring $\mathfrak{O}_K$ whose valuation equals $n-1$, i.e., $v_K(x) = n-1$. Then*

$$v_k(\mathrm{tr}\, x) = v_k(\delta)\ .$$

In particular, there is an element a in $\mathfrak{O}_K$ with $v_K(a) = n-1$ and such that $\mathrm{tr}\, a = \delta$.

Proof. Let $\mathfrak{M}$ and $\mathfrak{M}_\mathfrak{o}$ be the maximal ideals of K and k respectively. From the definition of the different and surjectivity of the trace operator it follows that $\mathrm{tr}(\mathfrak{M}^{-1}\mathfrak{D}^{-1}) = \mathfrak{M}_\mathfrak{o}^{-1}$. Moreover any element of $\mathfrak{M}^{-1}\mathfrak{D}^{-1}$, that does not belong to $\mathfrak{D}^{-1}$, has a non-integral trace. So the trace of the element $z = \pi_0^{-1}\delta^{-1}x$ is equal to

$$\mathrm{tr}\, z = \pi_0^{-1}\delta^{-1}\,\mathrm{tr}\, x = \pi_0^{-1}\varepsilon,\ \varepsilon \in \mathfrak{o}^*.$$

Thus $\mathrm{tr}\, x = \varepsilon\delta$. Further, if we multiply the element x by $\varepsilon^{-1} \in \mathfrak{o}^*$, then we get the element a. $\square$

Lemma 2.2.2. *In the ring $\mathfrak{O}_K$ we can choose a basis $a_0, a_1, \dots, a_{n-2}, a$, where a is as in Lemma 2.2.1, and the a_i for $0 \le i \le n-2$ are such that $v_K(a_i) = i$, and satisfy* $\operatorname{tr}\ a_i = 0$.

Proof. The kernel $\operatorname{Ker}\operatorname{tr}(\mathfrak{O}_K)$ has $\mathfrak{o}$-rank equal to $n-1$. Let $x_0, \dots, x_{n-2}$ be an $\mathfrak{o}$-basis of $\operatorname{Ker}\operatorname{tr}(\mathfrak{O}_K)$. Along with the element a they form a $\mathfrak{o}$-base of the ring $\mathfrak{O}_K$. By elementary operations in $\operatorname{Ker}\operatorname{tr}(\mathfrak{O}_K)$ we can get from $x_0, \dots, x_{n-2}$ a set of elements with pairwise different valuations. Their valuations have to be less than $n-1$. Indeed, otherwise by subtracting from the element x_0 of valuation $n-1$ an element a of the same valuation multiplied by a coefficient in $\mathfrak{o}^*$ we can obtain an element of $\mathfrak{M}^n$, which is impossible. $\square$

2.3. Let a be an element of $\mathfrak{O}_K$ with valuation equal to $n-1$, where $n = [K:k]$, and let

$$\operatorname{tr} a = \delta, \tag{12}$$

where δ is a generator of the different $\mathfrak{D}_{K/k}$ (cf. Lemma 2.2.1).

Proposition 2.3.1. *1. The module $\mathfrak{A}_{K/k}(\mathfrak{O}_K)(a) \mod \mathfrak{M}^n$ is a subring with an identity in $\mathfrak{O}_K \mod \mathfrak{M}^n$ (with standard multiplication).*

2. The multiplication $\overset{\Delta}{*}$ in $\mathfrak{A}_{K/k}(\mathfrak{O}_K)$ (cf. (11)) induces the standard multiplication in the ring $\mathfrak{A}_{K/k}(\mathfrak{O}_K)(a) \mod \mathfrak{M}^n$, i.e.,

$$f \overset{\Delta}{*} g(a) \equiv f(a)g(a) \mod \mathfrak{M}^n.$$

Proof. Let f and g belong to $\mathfrak{A}_{K/k}(\mathfrak{O}_K)$. Then the preimages $\phi^{-1}(\delta f)$, $\phi^{-1}(\delta g)$ with respect to the bijection ϕ belong to $\mathfrak{O}_K \otimes_o \mathfrak{O}_K$, since

$$\mathfrak{D} \otimes_o \mathfrak{D}^{-1} = \delta\mathfrak{O}_K \otimes_o \delta^{-1}\mathfrak{O}_K = \mathfrak{O}_K \otimes_o \mathfrak{O}_K.$$

We prove that

$$\phi^{-1}(\delta a) = x \otimes 1 + y, \tag{13}$$

where $x \in \mathfrak{O}_K$ and $y \in \mathfrak{O}_K \otimes \mathfrak{M}$.
Indeed, $\phi^{-1}(\delta a) = \sum a_i \otimes b_i$. If $b_i \in \mathfrak{M}$, then $a_i \otimes b_i \in \mathfrak{O}_K \otimes \mathfrak{M}$, otherwise $b_i = c_i + d_i$, where $c_i \in \mathfrak{o}$, $d_i \in \mathfrak{M}$ and so $a_i \otimes b_i = a_i \otimes c_i + a_i \otimes d_i = c_i x_i \otimes 1 + y_i$, where $c_i x_i \in \mathfrak{O}_K$, since $c_i \in \mathfrak{o}$ and $y_i \in \mathfrak{O}_K \otimes \mathfrak{M}$. So (13) follows.
Similarly

$$\phi^{-1}(\delta g) = x' \otimes 1 + y', \tag{14}$$

where $x' \in \mathfrak{O}_K$, $y' \in \mathfrak{O}_K \otimes \mathfrak{M}$.
Thus

$$\begin{aligned} \phi^{-1}(\delta f)\phi^{-1}(\delta g) &= (x \otimes 1 + y)(x' \otimes 1 + y') \\ &= xx' \otimes 1 + y((x' \otimes 1) + y') + (x \otimes 1)y' \\ &= xx' \otimes 1 + z, \text{ where } z \in \mathfrak{O}_K \otimes \mathfrak{M}. \end{aligned} \tag{15}$$

We consider the action of the element $f \in \mathfrak{A}_{K/k}(\mathfrak{O}_K)$ on the element a with valuation equal to $n-1$. From (13) we obtain $f = \delta^{-1}\phi(x \otimes 1 + y)$, where $x \in \mathfrak{O}_K$, $y \in \mathfrak{O}_K \otimes \mathfrak{M}$. Then from the definition of the map ϕ we have:

$$\begin{aligned} f(a) &= \delta^{-1}\phi(x \otimes 1 + y)(a) \\ &= \delta^{-1}(\phi(x \otimes 1)(a) + \phi(y)(a)) \\ &= \delta^{-1} x \operatorname{tr} a + \delta^{-1}\phi(y)(a). \end{aligned}$$

We show that $\delta^{-1}\phi(y)(a) \in \mathfrak{M}^n$,
i.e.,

$$f(a) = \delta^{-1} x \operatorname{tr} a + z, \text{ where } z \in \mathfrak{M}^n. \tag{16}$$

Indeed, let y be equal to $\sum a_i \otimes b_i$, then from the definition of ϕ we deduce that

$$\phi(y)(a) = \sum a_i \operatorname{tr}(b_i a).$$

Moreover $\operatorname{tr} b_i a \in \mathfrak{D}\mathfrak{M}_{\mathfrak{o}}$, thus $\delta^{-1} a_i \operatorname{tr}(b_i a) \in \mathfrak{M}^n$, i.e., $z = \delta^{-1}\phi(y)(a) \in \mathfrak{M}^n$ and we obtain (16).
Our assumptions imply that $\operatorname{tr} a = \delta$, so

$$f(a) \equiv x \mod \mathfrak{M}^n$$

and similarly

$$g(a) \equiv x' \mod \mathfrak{M}^n,$$

where x' is the element from (14). Then

$$f(a)g(a) \equiv xx' \mod \mathfrak{M}^n.$$

On the other hand from the definition of the multiplication $f \overset{\Delta}{*} g$ (cf. (11)) it follows that

$$f \overset{\Delta}{*} g(a) = \delta^{-1}\phi(\phi^{-1}(\delta f)\phi^{-1}(\delta g))(a).$$

Using this and keeping in mind (15) and (16) we obtain

$$f \overset{\Delta}{*} g(a) = \delta^{-1}\phi(xx' \otimes 1 + z)(a) \equiv xx' \mod \mathfrak{M}^n.$$

So we have the congruence

$$f \overset{\Delta}{*} g(a) \equiv f(a)g(a) \mod \mathfrak{M}^n.$$

Also, the element $\delta^{-1} \operatorname{tr}$ in $\mathfrak{A}_{K/k}(\mathfrak{O}_K)$ gives us an identity element in the ring $\mathfrak{A}_{K/k}(\mathfrak{O}_K)(a) \mod \mathfrak{M}^n$, since $\delta^{-1} \operatorname{tr} a = 1$ (cf. (12)). $\square$

Remark 2.3.2. For any other element a' in the ring $\mathfrak{O}_K$ with valuation equal to $n-1$ we have $\mathfrak{A}_{K/k}(\mathfrak{O}_K)(a') \equiv \varepsilon \mathfrak{A}_{K/k}(\mathfrak{O}_K)(a) \mod \mathfrak{M}^n$, $\varepsilon \in \mathfrak{o}^*$.

Remark 2.3.3. A similar statement also holds for the module $\mathfrak{B}_{K/k}(\mathfrak{O}_K)(a)$ mod $\mathfrak{M}^n$.

2.4. Now we formulate the statements which we will begin to prove in the next subsection.
We will investigate the following condition:
in the order $\mathfrak{A}_{K/k}(\mathfrak{O}_K)$ *(resp.* $\mathfrak{B}_{K/k}(\mathfrak{O}_K)$ *) there exists an element* ξ *such that*

$$\xi(a) = \pi, \tag{17}$$

where π *is a prime element of the field* K *and* a *is some element with valuation equal to* $n-1$.

Theorem 2.4.1. *If in the ring* $\mathfrak{A}_{K/k}(\mathfrak{O}_K)$ *(resp.* $\mathfrak{B}_{K/k}(\mathfrak{O}_K)$*) the condition (17) is fulfilled, then the element* ξ *generates a "power" basis of* $\mathfrak{A}_{K/k}(\mathfrak{O}_K)$ *(*$\mathfrak{B}_{K/k}(\mathfrak{O}_K)$ *resp.) over* $\mathfrak{o}$ *with respect to the multiplication* $\overset{\Delta}{*}$ *(cf. 11), i.e.,*

$$\mathfrak{A}_{K/k}(\mathfrak{O}_K) = \langle \xi^0, \xi^1, \ldots, \xi^{n-1} \rangle,$$

where $\xi^0 = \delta^{-1}\,\mathrm{tr}$ *is the unit and* $\xi^i = \xi \overset{\Delta}{*} \xi^{i-1}$.

Theorem 2.4.2. *1. If for the ring* $\mathfrak{A}_{K/k}(\mathfrak{O}_K)$ *(resp.* $\mathfrak{B}_{K/k}(\mathfrak{O}_K)$*) the condition (17) is fulfilled, then the ring* $\mathfrak{O}_K$ *is a free* $\mathfrak{A}_{K/k}(\mathfrak{O}_K)$*-module (resp. free* $\mathfrak{B}_{K/k}(\mathfrak{O}_K)$*-module).*
2. If the ring $\mathfrak{O}_K$ *is a free module over the ring* $\mathfrak{A}_{K/k}(\mathfrak{O}_K)$ *(resp.* $\mathfrak{B}_{K/k}(\mathfrak{O}_K)$*) and if moreover the order* $\mathfrak{A}_{K/k}(\mathfrak{O}_K)$ *(resp.* $\mathfrak{B}_{K/k}(\mathfrak{O}_K)$*) is indecomposable (i.e does not contain non-trivial idempotents), then for the ring* $\mathfrak{A}_{K/k}(\mathfrak{O}_K)$ *(resp.* $\mathfrak{B}_{K/k}(\mathfrak{O}_K)$*) the condition (17) and so also the assertions of the theorem 2.4.1 are fulfilled.*

Remark 2.4.3. If ξ maps some element with valuation equal to $n-1$ onto an element with valuation equal to 1, then ξ also maps any other element with valuation equal to $n-1$ onto an element with valuation equal to 1.
Indeed, if $a \in K$, $v_k(a) = n-1$ and $v_K(\xi(a)) = 1$, then any other element $a' \in \mathfrak{O}_K$, for which $v_K(a') = n-1$, is equal to $\varepsilon a + b$, where $\varepsilon \in \mathfrak{o}^*$, $b \in \mathfrak{M}^n$, so $b = \pi_0 b'$, where π_0 is a prime element in k. Besides that $b' \in \mathfrak{O}_K$ and we obtain $\xi(b) = \pi_0 \xi(b')$ and this implies $v_K(\xi(b)) \geq n$.
We also have $v_K(\xi(\varepsilon a)) = v_K(\varepsilon\xi(a)) = v_K(\varepsilon) + 1 = 1$ i.e., $\varepsilon \in \mathfrak{o}^*$, and so $v_K(\xi(a')) = 1$.

Remark 2.4.4. Any element ξ in $\mathfrak{A}_{K/k}(\mathfrak{O}_K)$ (resp. in $\mathfrak{B}_{K/k}(\mathfrak{O}_K)$) that fulfills the condition (17) generates a power base of the $\mathfrak{o}$-module $\mathfrak{A}_{K/k}(\mathfrak{O}_K)$ (resp. $\mathfrak{B}_{K/k}(\mathfrak{O}_K)$) with respect to the multiplication $\overset{\Delta}{*}$.

2.5 Proof of Theorem 2.4.1 and of the first part of Theorem 2.4.2..
We take the element a in the ring $\mathfrak{O}_K$ such that $v_K(a) = n-1$ and $\mathrm{tr}\, a = \delta$ (cf. (12)). By assumption we have $\xi(a) = \pi$, where π is a prime element of the field K. We check that

$$\xi^i(a) \equiv \pi^i \mod \mathfrak{M}_K^n. \tag{18}$$

Indeed, if $i = 0$, then for the usual product $\xi^0(a)\delta^{-1}\operatorname{tr}(a) = 1$. Let further $\xi^{i-1}(a)$ be equal to $\pi^{i-1} \mod \mathfrak{M}_K^n$, then according to Proposition 2.3.1 we have

$$\pi^i \equiv \xi^{i-1}(a)\xi(a) \equiv (\xi^{i-1} \overset{\Delta}{*} \xi)(a) \equiv \xi^i(a) \mod \mathfrak{M}_K^n$$

and the congruence (18) is proved. This equality implies that $\xi^i(a),\ 0 \le i \le n-1$, generate $\mathfrak{O}_K$, i.e., $\mathfrak{O}_K = \mathfrak{o}\xi^0(a) \oplus \cdots \oplus \mathfrak{o}\xi^{n-1}(a)$. Now we show that

$$\mathfrak{A}_{K/k}(\mathfrak{O}_K) = \langle \xi^0, \ldots, \xi^{n-1} \rangle.$$

If there exists an element $\eta \in \mathfrak{A}_{K/k}(\mathfrak{O}_K)$ that does not belong to a $\mathfrak{o}$-module $\langle \xi^0, \ldots, \xi^{n-1} \rangle$, then $\eta(a) = b \in \mathfrak{O}_K$. So we obtain

$$\eta(a) = \sum_{i=0}^{n-1} \alpha_i \xi^i(a),\ \ \alpha_i \in \mathfrak{o},$$

i.e.,

$$(\eta - \sum \alpha_i \xi^i)(a) = 0 \tag{19}$$

Now we show that

$$\eta = \sum \alpha_i \xi^i. \tag{20}$$

Indeed the spaces $k\mathfrak{A}_{K/k}(\mathfrak{O}_K)$ and $k\langle \xi^0, \ldots, \xi^{n-1} \rangle$ have equal dimensions and so coincide. It follows from (19) that

$$\eta - \sum \alpha_i \xi^i \in \mathfrak{A}_{K/k}(\mathfrak{O}_K) \subset k\mathfrak{A}_{K/k}(\mathfrak{O}_K) = k\langle \xi^0, \ldots, \xi^{n-1} \rangle,$$

and so

$$\eta - \sum \alpha_i \xi^i = \sum_{i=0}^{n-1} \alpha_i' \xi^i,$$

where $\alpha_i' \in k$. Since $\alpha_i' \in k$ and the valuations of the elements $\xi^i(a),\ 0 \le i \le n-1$ are pairwise non-congruent $\mod n$ (cf. (16)), the valuations $v_K((\alpha_i'\xi^i)(a))$ are also pairwise non-congruent $\mod n$, and so $\sum \alpha_i' \xi^i(a) \neq 0$ if not all the α_i' are equal to 0. This reasoning proves (20).

So we have obtained that the ring $\mathfrak{O}_K$ is a free $\mathfrak{A}_{K/k}(\mathfrak{O}_K)$-module:

$$\mathfrak{O}_K = \mathfrak{A}_{K/k}(\mathfrak{O}_K)(a)$$

and we have proved Theorem 2.4.1 and the first part of Theorem 2.4.2.

Lemma 2.6. *Let x be an element of the ring $\mathfrak{O}_K$ such that $\operatorname{tr} x = 0$, then for any $f \in \mathfrak{A}_{K/k}(\mathfrak{O}_K)$ and $g \in \mathfrak{B}_{K/k}(\mathfrak{O}_K)$ the following equalities hold:*

$$\operatorname{tr} f(x) = 0 = \operatorname{tr} g(x) = 0.$$

Proof. If $f \in \mathfrak{A}_{K/k}(\mathfrak{O}_K)$, then $f = \sum_{\sigma \in G} a_\sigma \sigma,\ a_\sigma \in k$, and so

$$\operatorname{tr} f(x) = \operatorname{tr}(\sum a_\sigma \sigma(x)) = \sum a_\sigma \operatorname{tr} \sigma(x) = 0.$$

If $g \in \mathfrak{B}_{K/k}(\mathfrak{O}_K)$, then $\operatorname{tr} g(x) = g(\operatorname{tr}(x)) = g(0) = 0$, since g is an $\mathfrak{o}[G]$-homomorphism. $\square$

2.7. Proof of necessity in Theorem 2.4.2.
Let $\mathfrak{O}_K$ be a free $\mathfrak{A}_{K/k}(\mathfrak{O}_K)$-module and assume the order $\mathfrak{A}_{K/k}(\mathfrak{O}_K)$ IS indecomposable. We prove that in the order $\mathfrak{A}_{K/k}(\mathfrak{O}_K)$ there exists an element ξ that fulfills the condition (17) of 2.4. We take elements $a_0, \ldots, a_{n-2}$ such that $v_K(a_i) = i$ and such that $\operatorname{tr} a_i = 0$ (cf. Lemma 2.2.2 and also [By1]). We take further an element a with valuation equal to $n-1$. Let $\chi : \mathfrak{O}_K \to \mathfrak{A}_{K/k}(\mathfrak{O}_K)$ be an isomorphism of $\mathfrak{o}[G]$-modules, then

$$\mathfrak{A}_{K/k}(\mathfrak{O}_K) = \langle \chi(a_0), \ldots, \chi(a) \rangle_{\mathfrak{o}}.$$

Thus, in particular, there exist $\alpha_i, \alpha \in \mathfrak{o}$ such that

$$1 = \alpha_0 \chi(a_0) + \cdots + \alpha_{n-2} + \alpha \chi(a).$$

The ring $\mathfrak{A}_{K/k}(\mathfrak{O}_K)$ is indecomposable by assumption, and so, according to the Krull-Schmidt Theorem, it is a local ring. We obtain that one of the $\chi(a_i)$ OR $\chi(a)$ has to be invertible in the ring $\mathfrak{A}_{K/k}(\mathfrak{O}_K)$. The elements $\chi(a_i)$ cannot be invertible since, according to Lemma 2.6, $\mathfrak{A}_{K/k}(\mathfrak{O}_K)(a_i) \in \operatorname{Ker} \operatorname{tr} \mathfrak{O}_K$. Thus $\chi(a)$ is invertible and it follows that $\mathfrak{A}_{K/k}(\mathfrak{O}_K)(a) = \mathfrak{O}_K$. We obtain that there exists a ξ in $\mathfrak{A}_{K/k}(\mathfrak{O}_K)$ such that $\xi(a) = \pi$. Theorem 2.4.2 is proved.

Remark 2.7. The corresponding reasoning for the ring $\mathfrak{B}_{K/k}(\mathfrak{O}_K)$ almost literally repeats the one we used above.

§3 Kummer extensions for formal groups. The proof of sufficiency in Theorem A.

Starting from this section we assume that the extension K/k is Abelian.

3.1. We denote the valuation on k by v_0. We also denote by v_0 the valuation on K that coincides with v_0 on k.
We suppose that the field k fulfills the conditions of §2 and that F is some formal group over the ring $\mathfrak{o}$ (the coefficients of the series $F(X,Y)$ may, generally speaking, lie, for example, in the ring of integers of some smaller field). On the maximal ideal $\mathfrak{M}_{\mathfrak{o}}$ of the ring $\mathfrak{o}$ we introduce a structure of a formal $\mathbb{Z}_p$-module using the formal group F by letting for $x, y \in \mathfrak{M}_{\mathfrak{o}}$ and $\alpha \in \mathbb{Z}_p$

$$x \underset{F}{+} y = F(x,y),$$
$$\alpha x = [\alpha](x).$$

We denote the $\mathbb{Z}_p$-module obtained in this way by $F(\mathfrak{M}_{\mathfrak{o}})$. Let T be a finite torsion subgroup in $F(\mathfrak{M}_{\mathfrak{o}})$ and let $n = \operatorname{card} T$ be the cardinality of the group T. Obviously, n is a power of p.
We construct the following series:

$$P(X) = \prod_{t \in T} (X \underset{F}{-} t). \tag{21}$$

Remark 3.1.1. The constant term of the series $P(X)$ is equal to zero, the coefficient at X^n is invertible in $\mathfrak{o}$, and the coefficients at the powers, not equal to n, belong to the ideal $\mathfrak{M}_{\mathfrak{o}}$.

Lemma 3.1.2. *Let a be a prime element of the field k and $K = k(x)$ be the extension obtained from k by adjoining the roots of the equation $P(X) = a$, where the series P is as in (21). Then the extension K/k is a totally ramified Abelian extension of degree n and the different $\mathfrak{D}$ of the extension K/k is generated by an element of the base field, i.e., $\mathfrak{D} = (\delta)$, $\delta \in k$. The ramification jumps of the extension K/k are equal to $h_l = nv_0(t_l) - 1$, $t_l \in T$.*

Proof. Using the Weierstrass Preparation Lemma we decompose the series $P(X) - a$ into a product

$$P(X) - a = cf(X)\varepsilon(X),$$

where $\varepsilon(X) \in \mathfrak{o}[[X]]^*$ is an invertible series (with respect to multiplication), $f(X)$ is A unitary polynomial, $c \in \mathfrak{o}$. Then, according to Remark 3.1.1, $f(X)$ is an Eisenstein polynomial of degree n. The series $P(X) - a$ has the same roots (we consider only the roots of $P(X) - a$ with positive valuation) as the polynomial $f(X)$, and so there are exactly n roots. It is obvious that if $P(x) = a$, then

$$P(x \underset{F}{+} \tau) = \prod_{t \in T} (x \underset{F}{-} t \underset{F}{+} \tau) = \prod_{t \in T} (x \underset{F}{-} t) = P(x) = a, \ \tau \in T$$

and so the roots of $P(X) - a$ and $f(X)$ are exactly the elements $x \underset{F}{+} \tau$, $\tau \in T$. Thus we proved that all roots of $f(X)$ lie in K and are all distinct. It follows that K/k is a Galois extension. We denote the Galois group of the extension K/k by G. Obviously if $\sigma_1, \sigma_2 \in G$, $\sigma_1(x) = x \underset{F}{+} t_1$, $\sigma_2(x) = x \underset{F}{+} t_2$, then $\sigma_2(\sigma_1(x)) = \sigma_2(x \underset{F}{+} t_1) = \sigma_2(x) \underset{F}{+} t_1 = x \underset{F}{+} t_2 \underset{F}{+} t_1$ (as $F(X,Y)$ is defined over $\mathfrak{o}$, $t_1 \in T$). Since the addition $\underset{F}{+}$ is commutative, the extension K/k is Abelian. We also have that $\prod \sigma(x) = a$, $v_k(a) = 1$, and so $v_0(x) = \frac{e(K/k)}{n}$. This implies that the extension K/k is totally ramified and that x is a prime element in K. Now we compute the ramification jumps of the extension K/k. Let $F(X,Y) = X + Y + \sum_{i,j>0} a_{ij} X^i Y^j$ be the formal group law, then we have

$$x - \sigma_l(x) = x - (x \underset{F}{+} t_l) = t_l + \sum_{i,j>0} a_{ij} x^i t^j = t_l \varepsilon_t,$$

where ε_t is a unit of the ring $\mathfrak{O}_K$. It follows that the ramification jumps of the extension K/k are equal to $nv_k(t_l) - 1$. Hence the exponent of the different is equal to $\sum_{t_l \in T} (h_l + 1) = n \sum_{t_l \in T} v_k(t_l)$ (cf., for example, [Se], Ch. 4, Proposition 4) and so $v_k(\mathfrak{D}) \equiv 0 \mod n$. □

3.2. Before beginning the proof of Theorem A we prove that the first condition of Theorem A is equivalent to a weaker one.

Proposition 3.2. *Let a belong to $\mathfrak{o}$, $v_k(a) = ns + 1$, where $0 \le s < \min_{t \in T} v_k(t)$. Then the extension $k(x)/k$, where x is A root of the equation $P(X) = a$, has the same properties as the extensions from the first condition of Theorem A.*

Proof. We consider the series

$$F_s(X, Y) = \pi_0^{-s} F(\pi_0^s X, \pi_0^s Y).$$

It is easily seen that F_s also defines a formal group law and the elements of $T_s = \{\pi_0^{-s} t,\ t \in T\}$ form some torsion subgroup in the formal module $F_s(\mathfrak{M}_{\mathfrak{o}})$. Indeed, if $F(X, Y) = \sum a_{ij} X^i Y^j$, then $F_s(X, Y) = \sum \pi_0^{s(i+j-1)} a_{ij} X^i Y^j$, and so the coefficients of $F_s(X, Y)$ are integral. Since $\pi_0^{-s} X \underset{F_s}{+} \pi_0^{-s} Y = \pi_0^{-s}(X \underset{F}{+} Y)$, F_s indeed defines an associative and commutative addition. Besides that if $u_1, u_2 \in T_s$, then $u_1 \underset{F_s}{+} u_2 = \pi_0^{-s}(\pi_0^s u_1 \underset{F}{+} \pi_0^s u_2) \in T_s$ and so T_s is indeed a subgroup in $F(\mathfrak{M}_{\mathfrak{o}})$.
Now we compute the series $P_{F_s}(X)$ for the formal group F_s. We obtain:

$$\begin{aligned} P_{F_s}(X) &= \prod_{t \in T} (X \underset{F_s}{-} \pi_0^{-s} t) = \prod_t (\pi_0^{-s}(\pi_0^s X) \underset{F_s}{-} \pi_0^{-s} t) \\ &= \prod_t \pi_0^{-s}(\pi_0^s X \underset{F}{-} t) = \pi_0^{-sn} P_F(\pi_0^s X). \end{aligned}$$

Thus the equation $P_f(X) = a$ is equivalent to $P_{F_s}(\pi_0^{-s} X) = a\pi_0^{-sn}$. Besides that $v(\pi_0^{-sn} a) = v(a) - sn$, i.e., $\pi_0^{-sn} a$ is a prime element in k.
Now it remains to note that a root of the equation $P_f(X) = a$ can be obtained by multiplication of a root of the equation $P_{F_s}(Y) = a\pi_0^{-sn}$ by π_0^s, and so the extensions obtained by adjoining the roots of these equations coincide. □

3.3 The proof of Theorem A: $1 \implies 2$.
Let K/k be an extension obtained by adjoining the roots of the equation $P(X) = \pi_0$. So $K = k(x)$ for some root x. We consider the maximal ideal $\mathfrak{M}_\otimes$ of the tensor product $\mathfrak{O}_K \otimes \mathfrak{O}_K$. Obviously $\mathfrak{M}_\otimes = \mathfrak{O}_K \otimes \mathfrak{M} + \mathfrak{M} \otimes \mathfrak{O}_K$. We also have $\mathfrak{M}_\otimes^i = \sum_{j=0}^i \mathfrak{M}^j \otimes \mathfrak{M}^{i-j}$, $i > 0$, and so it is easily seen that $\cap_{i>0} \mathfrak{M}_\otimes^i = 0$. It follows that we can introduce $\mathbb{Z}_p$-module structure $F(\mathfrak{M}_\otimes)$ on $\mathfrak{M}_\otimes$. We consider the element

$$\alpha = x \otimes 1 \underset{F}{-} 1 \otimes x \in \mathfrak{M}_\otimes\ .$$

We can define ξ in the following way:

$$\xi = \delta^{-1} \phi(\alpha). \tag{22}$$

We check the following properties of the element ξ:

1. $\xi \in \mathfrak{A}_{K/k}(\mathfrak{O}_K)$
2. If y belongs to $\mathfrak{O}_K$ and $v(y) = n-1$, then $\xi(y)$ is a prime element in K.

For (1):
Let $X \underset{F}{-} Y$ be equal to $\sum b_{ij} X^i Y^j$, then the equalities

$$\phi(\alpha) = \sum b_{ij}\phi(x^i \otimes 1^i) * \phi(1^j \otimes x^j)$$
$$= \sum_{\sigma\in G,\ i,j} b_{ij} x^i \sigma(x^j)\sigma = \sum (x \underset{F}{-} \sigma x)\sigma = \sum t_\sigma \sigma \in k[G]$$

follow from the definitions of ϕ and $*$. It also follows from Theorem 1.3.1 that ξ belongs to $\mathfrak{C}_{K/k}(\mathfrak{O}_K)$. Thus $\xi \in k[G] \cap \mathfrak{C}_{K/k}(\mathfrak{O}_K) = \mathfrak{A}_{K/k}(\mathfrak{O}_K)$.
For (2):
It easily seen that

$$(x \otimes 1) \underset{F}{-} (1 \otimes x) = x \otimes 1 + y, \tag{23}$$

where $y \in \mathfrak{M} \otimes \mathfrak{M}$. Indeed,

$$x \otimes 1 \underset{F}{-} 1 \otimes x = x \otimes 1 + \sum_{i\geq 1, j\geq 0} b_{ij} x^i \otimes x^j.$$

Since $b_{ij} \in \mathfrak{o}$, $b_{ij}x^i \otimes x^j \in \mathfrak{O}_K \otimes \mathfrak{M}$ and we obtain (23).
We can assume that $\mathrm{tr}(xa) = \delta$ (cf. Remark 2.4.3).
Then, as in Proposition 2.3.1, we have

$$\xi(a) = \delta^{-1}\phi(x \otimes 1 + y)(a) \equiv x \mod \mathfrak{M}^n.$$

Since $v(x) = 1$, we have proved the property 2.

3.4. Now we construct explicitly a basis of an associated order for extensions that fulfill the condition 1 of Theorem A. We have proved above that we can take the element ξ to be equal to $\delta^{-1}\sum t_\sigma \sigma$. Then it follows from Theorem 2.4.1 that

$$\mathfrak{A}_{K/k}(\mathfrak{O}_K) = \langle \delta^{-1} \sum_\sigma t_\sigma^i \sigma,\ i = 0, \ldots, n-1\rangle.$$

Now suppose that K is generated by a root of the equation $P(X) = b$, where $v_k(b) = sn + 1,\ s < \min v_0(t_l)$. In 3.2 we proved that K may be generated by a root of the equation $P_s(X) = b\pi_0^{-sn}$, and so it follows in this case that

$$\mathfrak{A}_{K/k}(\mathfrak{O}_K) = \langle \delta^{-1}\pi_0^{-si} t_\sigma^i \sigma,\ i = 0, \ldots, n-1\rangle.$$

Proposition 3.4.1. *Suppose that the extension K/k fulfills the condition 1 of Theorem A. Then $\mathfrak{A}_{K/k}(\mathfrak{O}_K)$ is a Hopf order in the group ring $k[G]$ with respect to the standard Hopf structure.*

Proof. $\mathfrak{A}_{K/k}(\mathfrak{O}_K)$ is an order in the group ring. It is easily seen, that if $f = \sum_{\sigma\in G} c_\sigma \sigma \in \mathfrak{A}_{K/k}(\mathfrak{O}_K)$, then $\sum c_\sigma \sigma^{-1} \in \mathfrak{A}_{K/k}(\mathfrak{O}_K)$. Indeed, we have $\phi^{-1}(f) \in \delta^{-1}\mathfrak{O}_K \otimes_o \mathfrak{O}_K$. Now consider the $\mathfrak{o}$-linear map $i : K \otimes_k K \to K \otimes_k K$, that maps $x \otimes y$ into $y \otimes x$. Obviously, $i(\phi^{-1}(f)) \in \delta^{-1}\mathfrak{O}_K \otimes_o \mathfrak{O}_K$. Besides, we have $\phi(x \otimes y) = \sum_{\sigma\in G} x\sigma(y)$, $\phi(y \otimes x) = \sum_{\sigma\in G} y\sigma(x) = \sum_{\sigma\in G} \sigma(x\sigma^{-1}(y)$. Thus we have

$$\sum c_\sigma \sigma^{-1} = \phi(i(\phi^{-1}(f))) \in \mathfrak{A}_{K/k}(\mathfrak{O}_K).$$

Thus it is sufficient to prove that for any $f \in \mathfrak{A}_{K/k}(\mathfrak{O}_K)$ we have

$$\Delta(f) \in \mathfrak{A}_{K/k}(\mathfrak{O}_K) \otimes \mathfrak{A}_{K/k}(\mathfrak{O}_K)\ ,$$

, where $\Delta(\sum c_\sigma \sigma) = \sum c_\sigma \sigma \otimes \sigma$. Theorem 2.4.1 implies immediately that it is sufficient to check this assertion for $f = \xi^l,\ l \geq 0$, the power is taken with respect to multiplication $\overset{\Delta}{*}$.

We consider the polynomial

$$J(X) = \prod_{t\in T\setminus\{0\}} \frac{t - X}{t}.$$

We have $J(0) = 1$, $J(t) = 0$ for $t \in T \setminus \{0\}$. The standard formula for the valuation of the different (cf. [Se]) and the last assertion of Lemma 3.1.2 imply that $J(X) \in \delta^{-1}\mathfrak{o}[X]$.

The fact that $\mathfrak{A}_{K/k}(\mathfrak{O}_K)$ is an $\mathfrak{o}$-algebra with a unit with respect to the multiplication $\overset{\Delta}{*}$ implies that for $f_1, f_2 \in \mathfrak{A}_{K/k}(\mathfrak{O}_K)\otimes\mathfrak{A}_{K/k}(\mathfrak{O}_K)$ their product $f_1 * f_2$ which is defined coefficient-wise lies in $\delta^{-2}\mathfrak{A}_{K/k}(\mathfrak{O}_K) \otimes \mathfrak{A}_{K/k}(\mathfrak{O}_K)$. Thus for the element $I = \sum_{\tau,\sigma\in G} t_{\sigma\tau^{-1}}\sigma\tau$ belongs to $\delta^2\mathfrak{A}_{K/k}(\mathfrak{O}_K) \otimes \mathfrak{A}_{K/k}(\mathfrak{O}_K)$ since

$$I = \sum_{\tau,\sigma\in G} (t_\sigma \underset{F}{-} t_\tau) = \delta^2 \sum_{i,j\geq 0} b_{ij}\xi^i \otimes \xi^j,$$

where the powers are taken with respect to $\overset{\Delta}{*}$ and b_{ij} are the coefficients in the expansion of the formal difference $X \underset{F}{-} Y$ into the powers of X and Y.

We also obtain that the element

$$L = \Delta(\mathrm{tr}) = \sum_{\sigma\in G} \sigma \otimes \sigma = J(I)$$

belongs to $\delta\mathfrak{A}_{K/k}(\mathfrak{O}_K) \otimes \mathfrak{A}_{K/k}(\mathfrak{O}_K)$. Then we have the equality

$$\Delta(\xi^l) = (\xi^l \otimes \mathrm{tr}) * L \in \mathfrak{A}_{K/k}(\mathfrak{O}_K) \otimes \mathfrak{A}_{K/k}(\mathfrak{O}_K)$$

since $\mathrm{tr} \in \delta\mathfrak{A}_{K/k}(\mathfrak{O}_K)$. $\square$

In a future paper we will prove a similar statement for an extension that fulfills the second condition of Theorem A not supposing K/k to be Abelian.

§4 Construction of a formal group

4.1. We suppose that in the associated order $\mathfrak{A}_{K/k}(\mathfrak{O}_K)$ there exists an element ξ such that it maps an element $a \in \mathfrak{O}_K,\ v_K(a) = n-1$ into a prime element π of the field K, i.e.,

$$\xi(a) = \pi \tag{24}$$

(cf. Lemma 2.2.1 and Theorem 2.4.2). We choose an element a such that $\operatorname{tr} a = \delta$ (cf. Lemma 2.2.1). Let

$$\begin{aligned} \psi_1 : K \otimes_k K &\to K \\ x \otimes y &\to xy \end{aligned} \tag{25}$$

be the map from 1.1, and let ϕ be the bijection between $K \otimes_k K$ and $K[G]$, that was defined in subsection 1.1.

Lemma 4.1.1. *We can choose an element ξ in $\mathfrak{A}_{K/k}(\mathfrak{O}_K)$ fulfilling (4) so that*
1. $\phi^{-1}(\delta\xi) = \pi \otimes 1 - 1 \otimes \pi + z$, where z belongs to the maximal ideal $\mathfrak{M}$ of the ring $\mathfrak{O}_K$.
2. In the expansion $\xi = \sum_{\sigma\in G} a_\sigma \sigma$, we have $a_1 = 0$ and $\delta a_\sigma \in \mathfrak{M}_\mathfrak{o}$ for $\sigma \neq 1$, where $\mathfrak{M}_\mathfrak{o}$ is the maximal ideal in $\mathfrak{o}$.

Proof. Theorem 1.3.1 implies that the preimage $\phi^{-1}(\xi)$ belongs to $\mathfrak{O}_K \otimes \mathfrak{D}^{-1}$. From our assumptions we also have $\mathfrak{D} = (\delta),\ \delta \in k$ (cf. (*)), so $\phi^{-1}(\delta\xi) \in \mathfrak{O}_K \otimes \mathfrak{O}_K$. As in 2.3, we can prove that

$$\phi^{-1}(\delta\xi) = x \otimes 1 + y,$$

where $x = \xi(a)\delta\operatorname{tr}(a)^{-1} = \pi,\ y \in \mathfrak{O}_K \otimes \mathfrak{M}$. It follows that

$$\phi^{-1}(\delta\psi) = \pi \otimes 1 + y,\ y \in \mathfrak{O}_K \otimes \mathfrak{M}.$$

We compute the coefficient at $1 = \mathrm{id}_K$ of the element $\xi = \phi(\delta^{-1}(\pi \otimes 1 + y))$. From the definition of ϕ it follows that it is equal to $\psi_1(\delta^{-1}\alpha)$. We have

$$\psi_1(\delta^{-1}(\pi \otimes 1 + y)) = \delta^{-1}(\pi + \psi_1(y)). \tag{26}$$

We decompose the element y in the base of $\mathfrak{O}_K \otimes \mathfrak{M}$:

$$y = \sum_{i\geq 0,\ j\geq 1} a_{ij}(\pi^i \otimes \pi^j),\ a_{ij} \in \mathfrak{o}.$$

Then

$$\psi_1(\sum a_{ij}\pi^i \otimes \pi^j) = \sum_{ij} a_{ij}\pi^{i+j} \tag{27}$$

If $\xi = \sum a_\sigma \sigma,\ a_\sigma \in k$, then $\psi_1(\delta^{-1}\alpha) = a_1 \in k$.

This implies that in order for the element (26) to lie in $\mathfrak{A}_{K/k}(\mathfrak{O}_K)$ it is necessary that the coefficient a_{01} in (27) is congruent with $-1 \mod \pi_0$, where π_0 is the prime element of k. It follows that $y = -1 \otimes \pi + z$ where $z \in \mathfrak{M} \otimes \mathfrak{M}$. The first claim of the lemma is proved.
Now we consider

$$\xi' = \xi - \psi_1(\xi)\,\mathrm{tr} = \sum_{\sigma \in G} (a_\sigma - a_1)\sigma = \sum_{\sigma \in G,\ \sigma \neq 1} (a_\sigma - a_1)\sigma.$$

We have $\psi_1(\xi') = 0$. Besides that, $\delta a_1 = \pi + \sum a_{ij}\pi^{i+j}$, $a_1 \in k$, and it follows that $\delta a_1 \in \mathfrak{M}_\mathfrak{o}$. Thus $a_1\,\mathrm{tr} \in \mathfrak{M}_0 \mathfrak{A}_{K/k}(\mathfrak{O}_K)$, and it follows that $\xi' \in \mathfrak{A}_{K/k}(\mathfrak{O}_K)$ and $\xi'(a) \equiv \xi(a) \mod \mathfrak{M}^n$. So ξ may be replaced by ξ'.
It remains to prove that in the expansion $\xi = \sum a_\sigma \sigma$ all δa_σ lie in $\mathfrak{M}$.
From the definition of ψ_σ we have

$$\delta a_\sigma = \psi_\sigma(\delta\xi) = \psi_\sigma(\pi \otimes 1) = \psi_\sigma(1 \otimes \pi) + \psi_\sigma(z) = \pi - \sigma(\pi) + \psi_\sigma(z) \in \mathfrak{M} \quad (28)$$

since $z \in \mathfrak{M} \otimes \mathfrak{M}$. Yet $a_\sigma \in k$ and it follows that $a_\sigma \in \mathfrak{M} \cap k = \mathfrak{M}_\mathfrak{o}$. $\square$

Corollary 4.1.2. We introduce the following notation: $\delta\xi = \sum_\sigma b_\sigma \sigma$. If $\phi^{-1}(\delta\xi) = \pi \otimes 1 - 1 \otimes \pi + \sum_{1 \le i,j \le n} a_{ij}\pi^i \otimes \pi^j,\ a_{ij} \in \mathfrak{o}$, then we have

$$b_\sigma = \pi - \sigma(\pi) + \sum a_{ij}\pi^i \sigma\pi^j \quad (29)$$

and

$$b_{\sigma^{-1}\tau} = \sigma\pi - \tau\pi + \sum a_{ij}\sigma\pi^i \tau\pi^j. \quad (30)$$

(the last statement follows from (29) and an obvious equality $\sigma b_{\sigma^{-1}\tau} = b_{\sigma^{-1}\tau}$).

4.2 A preliminary group law.
We consider the expansion

$$\phi^{-1}(\delta\xi) = \pi \otimes 1 - 1 \otimes \pi + \sum_{1 \le i,j < n} a_{ij}\pi^i \otimes \pi^j,\ a_{ij} \in \mathfrak{o}. \quad (31)$$

We replace $\pi \otimes 1$ in this decomposition by X, and $1 \otimes \pi$ by Y and decompose $\pi^i \otimes \pi^j$ into the product $(\pi^i \otimes 1)(1 \otimes \pi^j)$. Then from the expansion (31) we obtain a polynomial in two variables of degree not greater than n; we denote it by

$$R(X, Y) = X - Y + \sum_{1 \le i,j \le n} a_{ij}X^iY^j,\ a_{ij} \in \mathfrak{o}. \quad (32)$$

Now we identify $\pi \otimes 1$ with π, and $1 \otimes \pi$ with Z and obtain from (31) a polynomial in Z of degree not greater than n. We denote it by $s(Z)$:

$$s(Z) = \pi - Z + \sum_{1 \le j \le n} (\sum_{1 \le i \le n} a_{ij}\pi^i)Z^j. \quad (33)$$

All the coefficients of this polynomial except the coefficient at Z belong to $\mathfrak{M}$, and the coefficient at Z is invertible, so the polynomial $s(Z)$ is invertible in $\mathfrak{O}_K[[Z]]$ with respect to composition. We denote the inverse to s by $s^{-1}(Z)$.
It follows from (28) and (31) that

$$b_\sigma = \delta a_\sigma = (\pi - \sigma(\pi)) + \sum_{1\le i,j\le n} a_{ij}\pi^i\sigma\pi^j.$$

So, keeping in mind (33), we obtain

$$s(\sigma\pi) = b_\sigma,\ \ s^{-1}(b_\sigma) = \sigma\pi.$$

Besides that, (32) and (30) imply:

$$G(b_\sigma, b_\tau) = R(s^{-1}(b_\sigma), s^{-1}(b_\tau)) = b_{\sigma^{-1}\tau},$$

we also know that the series $G(X,Y) = R(s^{-1}(X), s^{-1}(Y)) \in \mathfrak{O}_K[[X,Y]]$ and

$$G(b_\sigma, b_\tau) \equiv (b_\sigma - b_\tau) \mod \mathfrak{M}\mathfrak{O}_K[[X,Y]].$$

So the series $G(b_\sigma, b_\tau)$ is invertible with respect to composition as a series in b_τ. We denote this inverse series by $H(b_\sigma, b_\tau) \in \mathfrak{O}_K[[b_\sigma, b_\tau]]$. We also note that $H(b_\sigma, b_\tau) = b_{\sigma\tau}$.
We introduce the following notation:

$$M(X) = \prod_{\sigma\in G}(X - b_\sigma). \tag{34}$$

Consider the reduction of the series $H(X,Y)$ modulo the ideal $(M(X), M(Y))$. We obtain a polynomial $J(X,Y)$, whose degree in each variable is less than n. Since $M(b_\sigma) = 0$,

$$J(b_\sigma, b_\tau) = b_{\sigma\tau}. \tag{35}$$

Proposition 4.2. $J(X,Y) \in \mathfrak{o}[[X,Y]]$.

Proof. We denote by $f(X,Y)$ the interpolation polynomial whose degree in each variable is less than n and that fulfills the system of relations

$$f(b_\sigma, b_\tau) = b_{\sigma\tau},\ \ \sigma,\tau\in G. \tag{36}$$

The polynomial J also fulfills the system of equalities (36) and so

$$f(X,Y) = J(X,Y).$$

Since $f \in k[X,Y],\ J \in \mathfrak{O}_K[X,Y]$, the coefficients of J belong to $k \cap \mathfrak{O}_K = \mathfrak{o}$. $\square$

4.3 THE MAIN STATEMENT CONCERNING FINITE TORSION SUBMODULES OF FORMAL MODULES OVER FORMAL GROUPS.

Let G be an Abelian group and suppose that for any $\sigma \in G$ there is an element $b_\sigma \in \mathfrak{M}_\mathfrak{o}$ chosen, and suppose that $b_1 = 0$.

THEOREM 4.3.1. *The following conditions are equivalent*

1 There exists a formal group $F(X,Y)$ over the ring of integers $\mathfrak{o}_E$ of some extension E of the field k such that $b_\sigma \underset{F}{+} b_\tau = b_{\sigma\tau}$ for all $\sigma, \tau \in G$.

2. There exists a formal group $F(X,Y)$ over the ring $\mathfrak{o}$, fulfilling the same conditions: $b_\sigma \underset{F}{+} b_\tau = b_{\sigma\tau}$.

3. The coefficients of the interpolation polynomial $f(X,Y)$, of degree less than n in X and Y and such that for $\sigma, \tau \in G$

$$f(b_\sigma, b_\tau) = b_{\sigma\tau}$$

belong to $\mathfrak{o}$.

Remark 4.3.2. This Theorem gives us a schematic description of finite subsets of $\mathfrak{M}_\mathfrak{o}$ that are finite groups with respect to an addition defined by some formal group with integral coefficients.

Additive Galois modules are not mentioned in the stating of this theorem and so it can be used without them.

Proof of Theorem 4.3.1: $2 \implies 1 \implies 3$. The condition 2 obviously implies 1. Now we prove that 1 implies 3. We consider the reduction of $F(X,Y)$ modulo the ideal $(M(X), M(Y))$ (cf. (34)) and denote it by $F_{\text{red}}(X,Y)$. It follows from the condition 1 that $F_{\text{red}}(b_\sigma, b_\tau) = b_{\sigma\tau}$, since $M(b_\sigma) = 0$. So $F_{\text{red}}(X,Y)$ coincides with the interpolation polynomial $f(X,Y)$, whose coefficients belong to k. Yet $F_{\text{red}}[X,Y] \in \mathfrak{o}_E[X,Y]$, so the coefficients of $f(X,Y)$ lie in $\mathfrak{o} = k \cap \mathfrak{o}_E$. It remains to prove that 3 implies 2.

4.4 SOME UNIVERSAL FORMAL GROUP LAWS.

We construct a formal group law in the same way as Hazewinkel (cf. [Ha], Ch. I, §3, subsection 3.1).

Consider the ring of polynomials $\mathbb{Z}_p[S_2, S_3, \ldots, S_n] = \mathbb{Z}_p[S] \subset \mathbb{Q}_p[S]$. We introduce the following notation:

$$\sigma : \mathbb{Q}_p[S] \to \mathbb{Q}_p[S], \; S_i \to S_i^p.$$

We consider the series $f_S(X)$, whose coefficients are found from the equation

$$f_S(X) = g(X) + \sum_{i \geq 1} \frac{S_{p^i}}{p} \sigma_*^i f_S(X^{p^i}), \; g(X) = X + \sum_{i \geq 2} S_i X^i - \sum_{i \geq 1} S_{p^i} X^{p^i},$$

where $\sigma_*^i f_S$ is the series obtained from f_S by applying the homomorphism σ^i to the coefficients, for $i > n$ we reckon S_i being equal to 0. It is easily seen that

$f_S = X + \sum_{i>1} a_i X^i,\ a_i \in Q[S]$. Then the Hazewinkel's Functional Equation Lemma implies that

$$F_S(X,Y) = f_S^{-1}(f_S(X) + f_S(Y))$$

is a formal group law over $\mathbb{Z}_p[S]$. Besides that

$$\begin{aligned} F_S[X,Y] \equiv & X + Y + S_m v_p(m)^{-1} B_m(X,Y) \\ & \bmod (S_2, \dots, S_{m-1}, \deg(m+1)),\ 2 \le m \le n, \end{aligned} \tag{37}$$

where $v_p(m) = p$ if $m = p^r,\ r \in \mathbb{Z},\ r > 0$, else $v_p(m) = 1$, and

$$B_m(X,Y) = X^m + Y^m - (X+Y)^m.$$

We note that the series F_S is a formal group law also in the case $\operatorname{char} k = p$ (in that case we should compute the coefficients of $v_p(m)^{-1} B_m(X,Y)$ 'formally' in $\mathbb{Z}$). This formal group differs from Hazewinkel's only because $S_i = 0$ for $i > n$. Now we modify the formal group law we have obtained. To be more precise, we make the following change of variables.
Now we define some values r_m in the following way. Let r^m be equal to s if $m = p^s m_0$ and $(m_0, p) = 1,\ m_0 > 1$ or $m_0 = p$.
Then

$$F_S(X,Y) = X + Y + \sum_{2 \le m \le n} d_m X^{p^{r_m}} Y^{m - p^{r_m}} + \text{summands of other degrees.}$$

We consider the ring

$$\mathbb{Z}_p[V] = \mathbb{Z}_p[V_2, \dots, V_n],\ V_i = d_i. \tag{38}$$

Lemma 4.4. *We can express the variables S_i as polynomials in V_i with integral coefficients and so obtain a new formal group law over $\mathbb{Z}_p[V]$.*

Proof. We have the equality $V_2 = S_2$
Besides that, for $i > 2$ the equality $V_i = S_i + f_i(S_2, \dots, S_{i-1}),\ f_i \in \mathbb{Z}_p[S_2, \dots, S_{i-1}]$ is fulfilled (cf. (37)). It follows that we can express S_i as a polynomial in $d_i, S_2, \dots, S_{i-1}$ with integral coefficients. Making all such changes we obtain an expression of S_i as a polynomial in $V_2, \dots, V_{i-1}$. Lemma is proved. $\square$

We note that the formal group law we constructed has the form

$$\begin{aligned} F_V(X,Y) = X + Y + & \sum_{2 \le m \le n} V_m X^{p^{r_m}} Y^{m - p^{r_m}} \\ & + \text{summands of other degrees.} \end{aligned} \tag{39}$$

4.5. In the Abelian group G we choose a family of subgroups $1 = G_0 \subset G_1 \subset G_2 \subset \cdots \subset G_l = G$, where $n = p^l$ and the cardinality of G_i is equal to p^i. In each subgroup G_i we choose an element $\sigma_{p^{i-1}}$ such that the coset $\sigma_{p^{i-1}}$ mod G_{i-1} generates the cyclic group G_i/G_{i-1} of cardinality p. We obtain a set of generators $\sigma_1, \sigma_p, \dots, \sigma_{p^{l-1}}$ for the group G. By induction on the cardinality of G it can be easily proved that any element σ of G can be expressed uniquely in the form

$$\sigma = \prod_{0 \le i \le l-1} \sigma_{p^i}^{c_i}, \text{ where } 0 \le c_i \le p-1. \tag{40}$$

We introduce the following notation:

$$c_\sigma = c_0 + pc_1 + \cdots + p^{l-1}c_{l-1} \in \mathbb{Z},\ 0 \le c_\sigma \le n-1.$$

We obtain a one-to-one correspondence $\sigma \to c_\sigma$. We also use the inverse notation: $\sigma_c = \sigma \iff c = c_\sigma$. We will construct the desired formal group by induction On the m-th step we 'get rid' of the variable V_m and adjoin the m-th relation.

First we prove a simple lemma about relations in an arbitrary Abelian group.

LEMMA 4.5. *Let H be an Abelian group, f be a map from G into H, $f(1) = 1_H$. Then the following statements are fulfilled*
1. If the relation

$$f(\sigma_i)f(\sigma_j) = f(\sigma_i\sigma_j) \tag{41}$$

is fulfilled for all $i = p^{r_s},\ j = s - p^{r_s}, 2 \le s \le m$, then it is also fulfilled for $0 \le i \le p^{r_m} - 1,\ 0 \le j \le m-1$ and for $i = p^{r_m},\ 0 \le j \le m - p^{r_m} - 1$.
2. If (41) is fulfilled for $i = p^{r_s},\ j = s - p^{r_s}, 2 \le s \le n$, then it is also fulfilled for all $0 \le i < n,\ 0 \le j < n$.

Proof. 1. First we prove by induction that (41) is fulfilled for $0 \le i \le p^t,\ 0 \le j \le m-1$, for all $0 \le t \le r_m$, i.e the restriction f_t of f onto G_t is a group homomorphism and $F_{tx} = \{f_i = f(\sigma_i),\ i = p^t x + u,\ 0 \le u \le p^t - 1\},\ 0 < x < \frac{m}{p^t}$ are cosets modulo the subgroup $F_t = f(G_t)$.
This is fulfilled for $t = 0$ since $f(1_G) = 1_H$.
We suppose that such statement is fulfilled for $t = w$. Now we prove it for $t = w+1$. Since F_{wx} are cosets modulo the subgroup F_w, it is sufficient to check that (41) is fulfilled for $i = p^w a, j = p^w b,\ 0 < a \le p-1, 0 < b < \frac{m}{p^w}$. If $0 < b \le p$, then $r_{bp^w} = w$, and so for $i = (b-1)p^w, j = p^w$ the relation (41) is fulfilled. Thus we obtain

$$f_{bp^w} = f_{p^w}^b,\ b < p,\ f_{(p-1)p^w} f_{p^w} = f_{p^w} = f(\sigma_{p^w}^p)$$

and f_{w+1} is a group homomorphism. Besides that, for $b > p, (b,p) = 1$ we also have $r_{bp^w} = w$, and so $f_{(b-1)p^w} f_{p^w} = f_{bp^w}$. For $b = pc$ we have:

$$f_{(pc-1)p^w} f_{p^w} = f_{(pc-p)p^w} f_{p^w}^p = f(\sigma_{(pc-1)p^w}\sigma_{p^w}),$$

since $\sigma_{p^w}^p \in G_w$. It follows that (41) is fulfilled indeed for all $i = p^w a, j = p^w b,\ 0 < a \le p-1, 0 < b < \frac{m}{p^w}$, and so $F_{w+1x},\ 0 < x < \frac{m}{p^{w+1}}$ indeed form cosets modulo F_{w+1}.
The relation (41) for $i = p^w,\ w = r_m\ 0 \le j \le m - p^w - 1$ is also sufficient to prove for $j = p^w b$, since F_{wx} are cosets modulo F_w. We argue in the same way as in the previous reasoning. We have again the equality $r_{bp^w} = w$ for $0 < b \le p$. It follows that if $\frac{m}{p^w} \le p$, then we obtain the desired assumption. If $\frac{m}{p^w} > p$, then for $\frac{m}{p^w} \ge b > p, (b,p) = 1$ also $r_{bp^w} = w$, and so $f_{(b-1)p^w} f_{p^w} = f(\sigma_{(b_1)p^w}\sigma_{p^w})$. For $p \mid b$ this is also fulfilled as $f_{(p-1)p^w} = f_{p^w}^{p-1}$. It follows that for $pc + p - 1 < \frac{m}{p^w}$ we have

$$f_{(pc+p-1)p^w} f_{p^w} = f_{pc} f_{p^w}^p = f(\sigma_{(pc+p-1)p^w}\sigma_{p^w}),$$

since $\sigma_{p^w}^p \in G_w$.
2. In the proof of the first part from the relation (41) for $i = p^{r_s},\ j = s - p^{r_s}, 2 \le s \le m$ we deduced that $F_t,\ p^t \mid m$ is a group homomorphism, the same proof for $m = n$ gives us the desired statement. $\square$

4.6 The proof of $3 \implies 2$ in Theorem 4.3.1.
In the beginning we are in the following situation. We have a formal group $F_V(X,Y)$, for which the following relations are fulfilled: $F(b_1, b_\sigma) = b_\sigma$ for all $\sigma \in G$, since $b_1 = 0$ from our assumptions.
We describe the second step.
We take the generator σ_1 of the group G_1 and try to fit the relation

$$F_V(b_{\sigma_1}, b_{\sigma_1}) = b_{\sigma_1^2}. \tag{42}$$

The interpolation polynomial $f(X,Y)$ from our condition 3 can be written in the form $f(X,Y) = X + Y + XY\psi(X,Y)$, where $\psi(X,Y) \in \mathfrak{o}[X,Y]$. We denote the ring of all series in $\mathfrak{o}[[V_i]]$, that converge at all (integral) values of V_i, by $\tilde{\mathfrak{o}}[[V_i]]$, and its ideal, consisting of series with coefficients in $\mathfrak{M}_\mathfrak{o}$, by $\tilde{\mathfrak{M}}_\mathfrak{o}[[V_i]]$. We have $b_{\sigma_1^2} = b_{\sigma_1} + b_{\sigma_1} + b_{\sigma_1}^2 c,\ c \in \mathfrak{o}$. On the other hand, if the relation (42) is fulfilled, then

$$b_{\sigma_1^2} = b_{\sigma_1} \underset{F}{+} b_{\sigma_1} = b_{\sigma_1} + b_{\sigma_1} + b_{\sigma_1}^2 V_2 + b_{\sigma_1}^3(\dots),\ (\dots) \in \tilde{\mathfrak{o}}[[V_2, V_3, \dots, V_n]].$$

We obtain

$$V_2 + b_{\sigma_1}(\dots) = \text{const} \in \mathfrak{o}$$

where $(\dots) \in \tilde{\mathfrak{o}}[[V_2, V_3, \dots, V_n]]$. Using the last relation we express V_2 in $V_3, \dots, V_n$, i.e., $V_2 = c + g(V_3, V_4, \dots, V_n),\ g \in \tilde{\mathfrak{M}}_\mathfrak{o}[[V_3, ;V_n]]$. This is possible, since in this relation the coefficient at the first power of V_2 is invertible, and coefficients at all other powers contain b_{σ_1}. We denote the formal group we obtained in this way by $F_V^2(X,Y)$. It depends on variables $V_3, \dots, V_n$ and fits the relations:

$$F_V^2(b_1, b_\sigma) = b_\sigma,\ \sigma \in G$$
$$F_V^2(b_{\sigma_1}, b_{\sigma_1}) = b_{\sigma_1^2}.$$

The second step is ended.
Now we describe the m-th step. We suppose that at the $m-1$-step we obtained a formal group $F_V^{m-1}(X,Y)$ that depends on the variables $V_m, V_{m+1}, \dots, V_n$ and fits the relations:

$$b_{\sigma_i} \underset{F}{+} b_{\sigma_j} = b_{\sigma_i \sigma_j} \tag{43}$$

for $0 \le i \le p^{r_m} - 1,\ 0 \le j \le m-1$ and $i = p^{r_m},\ 0 \le j \le m - p^{r_m} - 1$.
Thus we have $(m-1)(p^{r_m}+1)+1$ relations.
We denote by A_{m-1} the set of points $(b_{\sigma_i}, b_{\sigma_j})$ in (43). We need some lemma about interpolation. We introduce the following notation:

$$\chi_{m-1} = F_V^{m-1}(X,Y) - f(X,Y), \tag{44}$$

where $f(X,Y)$ is an interpolation polynomial from the formula (36). The relations for $f(X,Y)$ imply that $\chi_{m-1}(b_{\sigma_i}, b_{\sigma_j}) = 0$ for the indices (i,j) mentioned in (43).

Lemma 4.6.1. *Let R be an integral domain, b_{σ_i} be a set of elements in R, I be an ideal IN $R[X,Y]$, consisting of all polynomials that take the value zero at all pairs $(b_{\sigma_i}, b_{\sigma_j})$ in A_{m-1}. Then $I = (M,N,L)$, where $M = \prod_{0\le i\le p^{r_m}}(X - b_i)$, $N = \prod_{0\le j\le m-1}(Y - b_{\sigma_j})$, $L = \prod_{0\le i\le p^{r_m}-1}(X-b_i)\prod_{0\le j\le m-p^{r_m}-1}(Y - b_{\sigma_j})$.*

Proof. Let $\psi(X,Y)$ be an arbitrary polynomial in the ideal I. It is easily seen that it can be reduced uniquely modulo the ideal (M,N,L) to a polynomial ψ_{red}, since the higher coefficients of L,M,N are equal to 1. By its reduction we mean a polynomial that is congruent to it modulo (M,N,L) and has a non-zero coefficient at X^iY^j only if $(b_{\sigma_{i+1}}, b_{\sigma_{j+1}}) \in A_{m-1}$.
Now we have to prove that a polynomial ψ_{red} that belongs to I and contains non-zero coefficients only at powers mentioned above has to be equal to 0. It is sufficient to prove this statement for polynomials over the field R_0 that is the fraction field of R since it does not depend on the ring. We note that if we take for all $g(X,Y) \in R_0(X,Y)$ their values $G(b_{\sigma_i}, b_{\sigma_j})$, $(b_{\sigma_i}, b_{\sigma_j})$ in A_{m-1}, then we obtain a vector subspace of values in $R_0^{(p^{r_m}+1)(m-1)+1}$. It is easily seen that any set of values corresponds to some polynomial in $R_0(X,Y)$. A similar statement is obvious for polynomials in one variable and is easily carried on by induction to the case of any number of variables. It follows that the dimension of the space of values is equal to $(p^{r_m}+1)(m-1)+1$. The map $R_0[X,Y] \to C$, where C is the $(p^{r_m}+1)(m-1)+1$-dimensional space of values of polynomials in $R_0[X,Y]$ in points of A_{m-1}, factorizes through the space I' of reduction polynomials in $R_0[X,Y]$. So it follows from the equality of the dimensions that $\operatorname{Ker}(I' \to C) = \{0\}$ and thus $\psi_{\text{red}} = 0$. Lemma is proved. $\square$

It is easily seen that we may also use this lemma for the ring of power series. Indeed, we can reduce series modulo $\prod_{i<n}(X - b_i)\prod_{i<n}(Y - b_i)$ and obtain polynomials.

Now we make the m-th step of formal group construction.
According to Lemma, the series from (44) can be represented in a form

$$\chi_{m-1}(X,Y) = fM + gN + hL, \tag{45}$$

where $f,g,h \in R[[X,Y]]$, and $R = \tilde{\mathfrak{o}}[[V_m,\dots,V_n]]$.
We consider the following relation:

$$\chi_{m-1}(b_{p^{rm}}, b_{m-p^{rm}}) = 0.$$

It follows from the definition of M and N that $fM(b_{p^{rm}}, b_{m-p^{rm}}) = gN(b_{p^{rm}}, b_{m-p^{rm}}) = 0$. We need h to be equal to 0. We consider $h(X,Y)$ in the point $(b_{p^{rm}}, b_{m-p^{rm}})$. It is clear that $h(b_{p^{rm}}, b_{m-p^{rm}}) \in R[b_{p^{rm}}, b_{m-p^{rm}}] \subset R$. Besides that

$$h(b_{p^{rm}}, b_{m-p^{rm}}) \equiv \text{ absolute term of } (X,Y) \mod \tilde{\mathfrak{M}}_{\mathfrak{o}}[[V_m,\dots,V_n]].$$

Since in M,N,L only higher coefficients are invertible, in the relation (45) the coefficient at $X^{p^{rm}}Y^{m-p^{rm}}$ of the series $\chi_{m-1}(X,Y)$ is equal to

$$\text{the absolute term of } h(X,Y) + \text{an element of } \tilde{\mathfrak{M}}_{\mathfrak{o}}[[V_m,\dots,V_n]].$$

On the other hand it is equal to $V_m + \text{const}, \ \text{const} \in \mathfrak{o}$, as $\chi_{m-1}(X,Y) = F_V(X,Y) - f(X,Y)$. Thus we obtain

$$V_m + c = h(b_{p^{rm}}, b_{m-p^{rm}}) + d,$$

where $c \in \mathfrak{o}, \ d \in \tilde{\mathfrak{M}}_{\mathfrak{o}}[[V_m,\dots,V_n]]$. We chose V_m so that $h(b_{p^{rm}}, b_{m-p^{rm}}) = 0$ (in the formal group we replace V_m by a series in $V_{m+1},\dots,V_n$). So we made the m-th step. Since all the formal group laws F_V^m are commutative and associative, we can apply to the group $H = F_V^m(\tilde{\mathfrak{M}}_{\mathfrak{o}})[[V_{m+1},\dots,V_n]], \ f : \sigma \to b_\sigma$ the first part of Lemma 4.5 and so indeed after the $m-1$-th step the group F_V^{m-1} fits the relations (43) that are necessary for the m-th step. From the second part of Lemma 4.5 it follows that after the last (n-th) step all the relations for $b_{\sigma_i}, b_{\sigma_j}$ are fulfilled and all the variables V_i are got rid of and thus we obtained the desired formal group law $F = F_V^n$ in $\mathfrak{o}[[X,Y]]$.

Remark 4.6.2. The proof of Theorem 4.3.1 also implies that the formal group law F that fits the relations $b_\sigma \underset{F}{+} b_\tau = b_{\sigma\tau}, \ \sigma,\tau \in G$ and for which all the $S_i, \ i > n$ in expression $F(X,Y)$ through $F_S(X,Y)$, is unique. Besides that when we started instead of fixing $S_i = 0, \ i > n$ we could demand $S_i, \ i > n$ to be equal to arbitrary convergent series in $S_2,\dots,S_n$ with integral coefficients and obtain a similar statement.

§5 The proof of necessity in Theorem A

Now we show that our extension is indeed Kummer for the formal group we constructed.
We have a formal group $F(X,Y)$ such that

$$F(b_\sigma, b_\tau) = b_{\sigma\tau}. \tag{46}$$

We introduce again the addition with the means of the formal group F on the maximal ideal $\mathfrak{M}_\otimes = \mathfrak{O}_K \otimes \mathfrak{M} + \mathfrak{M} \otimes \mathfrak{O}_K$ of the tensor product $\mathfrak{O}_K \otimes \mathfrak{O}_K$. We denote the formal module obtained by $F(\mathfrak{M}_\otimes)$.
Now let $\xi = \sum a_\sigma \sigma$ act as in (4). Let α be equal to $\delta\phi^{-1}(\xi)$. Our aim in the remaining subsections is the proof of the following statement.

Proposition 5.1. *There are elements x and y in $\mathfrak{M}$ such that*

$$\alpha = x \otimes 1 \underset{F}{+} 1 \otimes y.$$

Here we show that the statement of Proposition implies theorem A.
Suppose that 5.1 is fulfilled. We can express y as $1 \otimes z,\ z \in \mathfrak{M}$ and so $\alpha = x \otimes 1 \underset{F}{+} 1 \otimes z$. Using the formula for ψ_1 and the fact that $b_1 = 0$ we obtain that $0 = b_1 = \psi_1(\alpha) = x \underset{F}{+} z$. Thus z is equal to $[-1]_F(x)$ ($[-1]_F(x)$ is the inverse to x in $F(\mathfrak{M})$) and it follows that $\alpha = x \otimes 1 \underset{F}{-} 1 \otimes x$. Similarly

$$b_\sigma = \psi_\sigma(\alpha) = \psi_\sigma(x \otimes 1) \underset{F}{-} \psi_\sigma(1 \otimes x) = x \underset{F}{-} \sigma(x).$$

We obtain that the conjugates of x in the extension K/k are exactly the elements of the form $x \underset{F}{+} b_\sigma$. Then $\prod (x \underset{F}{+} b_\sigma) \in \mathfrak{o}$ and $v_k(\prod (x \underset{F}{+} b_\sigma)) = 1$, thus the extension K/k is Kummer for the formal group F and is generated by a root of the equation $P(X) = w$ while $v_k(w) = 1$. Theorem A of the introduction is proved.

5.2. Now we start proving 5.1.
Let n be equal to $p^l = [K : k]$. Consider a tower of intermediate extensions:

$$k = k_0 \subset k_1 \subset k_2 \subset \cdots \subset k_l = K,\ [k_i : k_{i-1}] = p.$$

We take representatives τ_i for the generators of the Galois groups $G_i = \mathrm{Gal}(k_i/k_{i-1})$. For all $\tau \in G$ we prove the following equality:

$$\tau(\alpha) = \alpha \underset{F}{-} b_\tau \tag{47}$$

(we assume here that the group G acts only on the first component of the tensor product).

Indeed, for any $z \in K$ we have

$$\phi(\tau(x) \otimes y)(z) = \tau(x) \operatorname{tr} yz = \tau(x \operatorname{tr} yz) = \tau(\phi(x \otimes y)(z)),$$

and so for each $\beta \in K \otimes_k K$ the equality

$$\phi((\tau \otimes 1)\beta(z)) = \tau(\phi(\beta)(z)) \tag{48}$$

is also fulfilled. Thus we obtain

$$\tau(\delta\xi) = \sum_\sigma b_\sigma \tau\sigma = \sum_\sigma (b_{\tau\sigma} \underset{F}{-} b_\tau)\sigma_\tau = \sigma\xi \underset{F}{-} (b_\tau \operatorname{tr}).$$

The formula (48) now implies (47).

5.3. Let $\mathfrak{o}_i$ be the ring of integers of the field k_i. For each $i: \ 0 \le i \le l$ we prove by induction the following lemma.

Lemma 5.3. *There is an equality*

$$\alpha = x \otimes 1 \underset{F}{+} y, \ \ y \in \mathfrak{o}_i \otimes \mathfrak{M} \tag{49}$$

Proof. For $i = l$ the claim is obvious.
Let the claim be fulfilled for $i = s + 1$.
We can expand the element y in the base of the formal module $F(\mathfrak{o}_{s+1} \otimes \mathfrak{M})$:

$$y = \sum_{0 \le i \ \ 0 \le j < n} {}_{(F)} a_{ij} \pi_{s+1}^i \otimes \pi^j, \tag{50}$$

where π_{s+1} is a prime element of the field k_{s+1}, the coefficients a_{ij} are either equal to 0, or $a_{ij} \in \mathfrak{o}^*$ (for $j \ge n$ we extract the prime element π_0 of the field k from π^n and convert it into the first component).
For the automorphism τ_{s+1} we have the equality (47):

$$\tau_{s+1}(\alpha) = \alpha \underset{F}{-} b_{\tau_{s+1}}. \tag{51}$$

Now we express α in the form

$$x \otimes 1 \underset{F}{+} \sum_{0 \le i \ \ 0 \le j < n} {}_{(F)} b_{ij} \pi_s^i \otimes \pi^j \underset{F}{+} \sum_{0 \le i \ \ 0 \le j < n} {}_{(F)} a_{ij} \pi_{s+1}^i \otimes \pi^j. \tag{52}$$

We consequently convert the third summand in (52) into the first and the second, increasing the minimum of $ni + j$ for i, j such that $a_{ij} \ne 0$. Out of all pairs (i, j) for which $a_{ij} \ne 0$ we chose a pair with the least i, which we denote by i_0, further out of all pairs (i_0, j) such that $a_{i_0 j} \ne 0$ we chose the pair with the least j and denote it by j_0. We call the corresponding ordering of (i, j) by order.

We have three cases.
Case I. If $j_0 = 0$, then

$$a_{i_0 j_0}(\pi_{s+1}^{i_0} \otimes \pi^{j_0}) = a_{i_0 0}(\pi_{s+1}^{i_0} \otimes 1) \tag{53}$$

and we import this term into the first summand in (52). It is clear that subtracting with respect to F the term $a_{i_0 0}(\pi_{s+1}^{i_0} \otimes 1)$ gives only the terms of greater order (since $X \underset{F}{-} Y = (X-Y)(1+r(X,Y)),\ r(X,Y) \in (X,Y)\mathfrak{o}[[X,Y]]$) and so we increase the value of $ni_0 + j_0$.

Case II. Now let j_0 be not equal to 0. If $p \mid i_0$ then $\pi_{s+1}^{i_0} = \pi_s^{\frac{i_0}{p}} + r$, where $v_{s+1}(r) > i_0$ and $\frac{i_0}{p} \in \mathbb{Z}$ and thus

$$a_{i_0 j_0}(\pi_{s+1}^{i_0} \otimes \pi^{j_0}) = a_{i_0 j_0}\pi_s^{\frac{i_0}{p}} \otimes \pi^{j_0} \underset{F}{+} \text{terms of greater order.} \tag{54}$$

It follows that we can import the term $a_{i_0 j_0}\pi_s^{\frac{i_0}{p}} \otimes \pi^{j_0}$ into the second summand of the formula (52) and increase the minimum of $ni + j$ again.
Case III. It remains to consider the case $(i_0, p) = 1,\ j_0 \neq 0$, We consider

$$\begin{aligned} \tau_{s+1}(\alpha) \underset{F}{-} \alpha = \tau_{s+1}(x \otimes 1) \underset{F}{-} (x \otimes 1) \underset{F}{+} (\tau_{s+1} \underset{F}{-} 1) a_{i_0 j_0}(\pi_{s+1}^{i_0} \otimes \pi^{j_0}) \\ \underset{F}{+} (\tau_{s+1} \underset{F}{-} 1)(\text{terms of greater order}). \end{aligned}$$

We have:

$$\begin{aligned} \tau_{s+1}(x \otimes 1) \underset{F}{-} (x \otimes 1) = (\tau_{s+1}(x) \underset{F}{-} x) \otimes 1 \in \mathfrak{M} \otimes \mathfrak{o} \\ a_{\tau_{s+1}} = a_{\tau_{s+1}} \otimes 1 \in \mathfrak{M} \otimes \mathfrak{o}. \end{aligned} \tag{55}$$

So the element $(\tau_{s+1} \underset{F}{-} 1) a_{i_0 j_0}(\pi_{s+1}^{i_0} \otimes \pi^{j_0}) \underset{F}{+} (\tau_{s+1} \underset{F}{-} 1)$ (terms of greater order) also belongs to $\mathfrak{M} \otimes \mathfrak{o}$. Yet that is impossible since

$$\begin{aligned} (\tau_{s+1} \underset{F}{-} 1) a_{i_0 j_0}(\pi_{s+1}^{i_0} \otimes \pi^{j_0}) \equiv a_{i_0 j_0}(\tau_{s+1}\pi_{s+1}^{i_0} - \pi_{s+1}^{i_0}) \otimes \pi^{j_0} \\ \text{mod (terms of greater order).} \end{aligned}$$

The remaining terms indeed have greater $ni + j$ since $(i_0, p) = 1$ and so the valuation of $\tau_{s+1}\pi_{s+1}^{i_0} - \pi_{s+1}^{i_0}$ in k_{s+1} is equal to $i_0 + h_{s+1,s+1}$, where $h_{s+1,s+1}$ is the ramification jump of τ_{s+1} in the field K_{s+1}. Thus we obtain

$$a_{i_0 j_0}(\tau_{s+1}\pi_{s+1}^{i_0} - \pi_{s+1}^{i_0}) \otimes \pi^{j_0} \underset{F}{+} (\text{terms of greater order}),$$

and this sum cannot belong to $\mathfrak{M} \otimes \mathfrak{o}$ since j_0 does not contain n from our assumptions (it can be easily proved by considering the expansion of an element of $\mathfrak{M} \otimes \mathfrak{o}$ in the base $\mathfrak{O}_K \otimes \mathfrak{O}_K$ over $\mathfrak{o}$.) So this case is impossible. Thus our assertion is valid for $i = s$. Lemma 5.3 is proved. $\square$

Now by applying the lemma 5.3 for $i = 0$ we obtain $\alpha = x \otimes 1 \underset{F}{+} y,\ y \in \mathfrak{o} \otimes \mathfrak{M}$. Theorem A is proved completely.

References

[**Be**] F. Bertrandias, *Sur les extensions cycliques de degré p^n d'un corps local*, Acta arithmetica **34** (1979), 361–377.

[**B-F**] F. Bertrandias and M.-J. Ferton, *Sur l'anneau des entiers d'unextension cyclique de degré premier d'uncorps locai*, C. R. Acad. Sc. Paris **274** (1972), A1330–A1333.

[**BVZ**] M. V. Bondarko, S. V. Vostokov, I. B. Zhukov, *Additive Galois module*, Algebra and Analysis **9** (1997), no. 4, 28–46.

[**BV**] M. V. Bondarko, S. V. Vostokov, *Decomposability of ideals in Abelian p-extensions of plenal fields I to appear.*

[**By1**] N. Byott, *Galois structure of ideals in wildly ramified Abelian p-extensions of a p-adic Field and some applications*, Journal de Theorie des nombres de Bordeaux **9** (1997), 201–219.

[**By2**] N. Byott, *On Galois isomorphisms between ideals in extensions of local fields*, Manuscripta Math. **73** (1991), 289–311.

[**By3**] N. Byott, *Tame and Galois extensions with respect to Hopf orders*, Math. Z. **220** (1995), 495–522.

[**Ch**] Shin-Ping Chan, *Relative Lubin-Tate formal groups and Galois module structure*, Manuscripta Math. **75** (1991), 109–113.

[**Chi**] L. N. Childs, *Taming wild extensions with Hopf algebras*, Trans. Am. Math. Soc. **304** (1987), 111–140.

[**CM**] L. N. Childs, D. J. Moss, *Hopf algebras and local Galois module theory*, Advances in Hopf algebras, Lect. Notes on pure and applied Math. **158** (1994), 1–14.

[**F1**] M.-J. Ferton, *Sur les idéaux d'une extension cyclique de degré premier d'un corps local*, C. R. Acad. Sc. Paris **276** (1973), no. A, 1483-1486.

[**F2**] M.-J. Ferton, *Sur l'anneau des entiers de certaines extensions cycliques d'un corps local Soc. Mathem.de France,*, Asterisque **24-25** (1975), 21–27.

[**Fr**] A. Fröhlich, *Galois module structure of algebraic integers*, Springer, Ergeb. Math. Grenzgeb, 1983.

[**G**] G. Greither, *Extensions of finite group schemes and Hopf Galois theory over a complete discrete valuation ring*, Math. Z. **210** (1992), 37–67.

[**Ha**] Michiel Hazewinkel, *Formal groups and applications*, 1978.

[**Im**] Tsunchisa Imada, *Galois module stucture of local rings of integers via relative Lubin-Tate groups*, Memoirs of the Faculty of Science, Kyushu University **47** (1993), no. A, 71–77.

[**L**] Heinrich W. Leopoldt, *Über die Hauptordnung der ganzen Elemente eines abelschen Zahlkörpers*, J. Reine Angew. Math. **201** (1959), 119–149.

[**Le1**] G. Lettl, *Relative Galois module structure of integers of local Abelian fields*, Acta Arithmetica **85** (1998), no. 3, 235–248.

[**Le2**] G. Lettl, *Note on the Galois module structure of quadratic extensions*, Col. Math. **LXVII** (1994).

[**N**] E. Noether, *Normalbasis bei Körpern ohne höhere Verzweigung*, J. Reine Angew. Math. **167** (1932), 147–152.

[**Se**] Jean-Pierre Serre, *Local fields*, Graduate Texts in Mathematics, vol. 67, Springer-Verlag, Berlin –Heidelberg–New York, 1979.

[**T1**] M. J. Taylor, *Formal groups and the Galois module structure of local rings of integers*, J. Reine Angew. Math. **358** (1985), 97–103.

[**T2**] M. J. Taylor, *Hopf structure and the Kummer theory for formal groups*, J. Reine Angew. Math. **375/376** (1987), 1–11.

Prof. M. Bondarko
Department of
Mathematics and Mechanics
St. Petersburg State University
Bibliotechnaya pl. 2,
St. Petersburg, 198904, Russia
m@vbond.usr.pu.ru