DECOMPOSITION OF IDEALS AS GALOIS MODULES IN COMPLETE DISCRETE VALUATION FIELDS

by M.V. BONDARKO, S.V. VOSTOKOV, O.V. DEMCHENKO

Introduction

This work is a direct continuation of the work [ВВЖ], in which there were obtained the necessary and sufficient condition when all the ideals of an abelian p-extension of a complete discrete valuation field of characteristic p are simultaneously indecomposable (or, which is the same, the necessary and sufficient condition of the existence of decomposable ideals in such p-extension).

The authors are very grateful to Prof. Panchishkin and all the staff of the Fourier Institute (Grenoble) for their hospitality and the excellent conditions for the creative work.
Remark that the problem of studing of the Galois modules of number and local fields is due, as many other number problems, to D. Hilbert who in 1897 proved that in an abelian tame extension $K/\mathbb{Q}$ with the Galois group G the ring of integers $\mathcal{O}_K$ as $\mathbb{Z}[G]$-module is a free module of rank 1.

The following generalization of these results in number fields gave only the necessary, not sufficient conditions when the ring of integers $\mathcal{O}_K$ is a free $o_k[G]$-module in the extension K/k (here $\mathcal{O}_K$ and o_k are the rings of integers of the fields K and k correspondently).

Naturally, in the local fields (that is in the complete discrete valuation fields) the situation should be more easier and really, a complete answer to the corresponding local question was given by Emmi Nœther ([N]) in 1932:

THEOREM. — *Let K/k be a finite extension of local fields, $G = \mathrm{Gal}(K/k)$. Then two conditions are equivalent:*

1) $\mathcal{O}_K \cong o_k[G]$ (we say: $\mathcal{O}_K$ has a normal basis over o_k);

2) K/k is tamely ramified.

A more general question, when the given ideal $\mathcal{M}_K^i$ in $\mathcal{O}_K$ has normal basis over $\mathcal{O}_k$ also has a complete answer.

THEOREM. — *$\mathcal{M}_K^i \cong \mathcal{O}_k[G]$ as an $\mathcal{O}_k[G]$-module if and only if $\mathcal{M}_K^i \cap k = \mathrm{tr}_{K/k}\, \mathcal{M}_K^i$.*

This was proved by S. Ullom in 1970 ([U]) and in explicit form by S. Vostokov in 1976 ([V3]).

The following studying of ideals as Galois modules in local fields were developed in three directions.

The series of works which are due to G.V. Leopoldt ([L]) studied the ring of integers $\mathcal{O}_K$ as module over the corresponding order Λ in $k[G]$ for the Galois extension K/k with the Galois group G where

$$\Lambda = \{\lambda \in k[G] \mid \lambda \mathcal{O}_K \subset \mathcal{O}_K\}.$$

This direction was developed intensively by A.M. Bergé, F. Bertrandias, B. Martel, M.T. Ferlon and today by Byott, Lettl.

Another approach is to describe the structure of $\mathcal{O}_K$ over $\mathbb{Z}_p[G]$ rather then over $\mathcal{O}_K[G]$. The essential role here is played by the circumstance that A. Jones (1962) described all the indecomposable $\mathbb{Z}_p[G]$-modules, in particular

$$\left\{\begin{array}{l}\text{Number of isomorphism classes of}\\ \text{indecomposable } \mathbb{Z}_p[G]\text{-modules}\end{array}\right\} = \left\{\begin{array}{ll} 3, & \text{if } G = \mathbb{Z}/p\mathbb{Z}\\ 4p+1, & \text{if } G = \mathbb{Z}/p^2\mathbb{Z}\\ \infty, & \text{otherwise.}\end{array}\right.$$

Besides, it is used a variant of Krull-Schmidt theorem, proved by Z.I. Borevich and D.K. Faddeev.

There are many new results here, due to G.H. Elder and M.L. Madan (see [E], [EM]). The most interesting observation: if $G \cong \mathbb{Z}/p^m\mathbb{Z}$ then only finitely many different indecomposable modules can occur in decomposition of any $\mathcal{O}_K$ as a $\mathbb{Z}_p[G]$-module. (This is true under a restriction of such kind: the first jump of ramification is not too small.)

The third series of papers is aimed to get some information about $\mathcal{O}_K$ (or, more generally, about $\mathcal{M}_K^i$) as an $\mathcal{O}_k[G]$-module. We can try to answer as a first step, the following questions:

A) When $\mathcal{M}_K^i \cong \mathcal{M}_K^i$ as $\mathcal{O}_k[G]$-modules

B) When $\mathcal{M}_K^i$ has a non-trivial decomposition into a direct sum of $\mathcal{O}_k[G]$-submodules.

There is a following partial answer to question **A)** of N. Byott (see [B]).

THEOREM. — *Let K/k be an abelian extension with ramification index p^m, k a local field. Assume $h_1(K/k) \leq \frac{ep}{p-1}$ be the first jump of ramification. If $m \geq 2$, assume that $G = \mathrm{Gal}(K/k)$ is not cyclic. Then $\mathcal{M}_K^i \cong \mathcal{M}_K^j$ over $o_k[G] \Longleftrightarrow i \equiv j \bmod p^m$.*

The answer to the second question for abelian extension of local field was given in the cycle of S. Vostokov's papers (see [BV], [V1], [V2]). In this case there were determinated the necessary and sufficient conditions of decomposability of ideals.

The works of Y. Migata (see [M1]–[M3]) should also be mentioned, where there were obtained some results of [BV], [V1], [V2] in other way. In his recent paper [M4] Y. Migata considered abelian extension K'/k and K''/k with the same Galois group G and studied the question in which condition $\mathcal{O}_{K'} \approx \mathcal{O}_{K''}$ as $\mathcal{O}_K[G]$-modules.

When we pass on from local fields to arbitrary complete discrete valuation field then there appear two essential difficulties. Firstly, the residue field becomes an arbitrary field (of characteristic p) and secondly, for such fields practically there is not the ramification theory which is the essential part of the proofs of [V1], [V2].

The difference between this work, the preceding one [БВЖ] and the first works [BV], [V1], [V2] is that here there is the unique approach to the proof of the main results without difference of the cases when there is or there is not the p-roots in the ground field as it was in the paper [V1] and [V2].

Besides, the theory of ramification in complete discrete valuation fields is being developed.

The main theorem of the work [БВЖ] is following.

THEOREM A. — *Let K/k be an abelian p-extension of complete discretely valuated fields of characteristic* 0 *with residue field of characteristic p.*

It is assumed that the corresponding extension of residue field is separable. Let $G = \mathrm{Gal}(K/k)$ and let o be the ring of integers in k. Then some of ideals in K are decomposable as $o[G]$-modules if and only if the ramification index of K/k divides the different of K/k.

As we have seen in the formulation of the theorem the condition of decomposability is connected with the different of the extension or, in other words, with the ramification jumps. Remark that when the ramification index of the extension divides the different then there are only two possibilities.

Or p divides all the ramification jumps or all of them are relatively prime to p (see [FV], Ch. III, Prop. (2.3)).

We prove the following main result:

THEOREM B. — *Under assumptions of the theorem A we have got*

1) If p divides all the ramification jumps of the extension K/k then all the ideals $\mathcal{M}_K^i$ in the ring $\mathcal{O}_K$ are decomposable as $o_k[G]$-modules.

2) If the ramification index p^m of the extension K/k divides the different $\nabla_{K/k}$ of the extension and all the ramification jumps are relatively prime to p then the ideals $\mathcal{M}_K^i$ are decomposable if and only if p divides i or in the p-adic decomposition of $i \bmod p^m$ there is a digit which is more than e_*, where e_* is the remainder of division of the absolute ramification index e of the field k by $p-1$ in the positive residue system.

Notation

We use such a notation

p : the fixed prime;

$\bar{a}$: the remainder of division an integer a by p;

ζ_n : the primitive n-th root of the unity;

ν_F : the valuation in the given discrete valuated field F;

$\mathcal{O}_F$: the ring of integer of the given discrete valuated field F;

$\mathcal{M}_F$: the maximal integral of the ring $\mathcal{O}_F$;

e_F : $e_F = \nu_F(p)$; if $\operatorname{char} F = 0$, $\operatorname{char} \overline{F} = p$.

1. Auxiliary and also known results

1.0. — In this paragraph we use the following notation:

k : a complete discrete valuation field of characteristic 0 with arbitrary residue fields of prime characteristic p;

e : the absolute ramification index p;

e_*: the residue e modulo $p-1$ in the positive residue system;

K/k : a normal finite p-extension;

p^m : ramification index of K/k;

G : the Galois group K/k;

∇ : the different of the extension K/k;

$d = \nu_K(\nabla)$: the exponent of the different of the extension K/k;

π : a prime element of the field K

$\mathrm{tr} = \mathrm{tr}_{K/k}$.

1.1. — Ramification subgroups G_i, $i \geq 1$ (see [Se], Ch. IV or [FV], ch. II, § 4) are defined in such a way

$$G_i = \{\sigma \in G \mid \nu_K(\pi^\sigma/\pi - 1) \geq i\}.$$

It is said that the natural number h is a ramification jump for K/k if $G_h \neq G_{h+1}$.

Remark. — The maximal ramification jump for K/k is not more than $p^m e/(p-1)$. This follows from [Se], Ch. IV, § 2, Ex. 3c or [FV], Ch. III, Prop. (2.3).

In the work [БВЖ] there was proved very important for the further considerations results from the ramification theory of complete discrete valuation fields, namely

Proposition 1.1. — *Let K/k be a normal p-extension, in which the minimal ramification jump is more then 1 if $p = 2$. Then the following three conditions are equivalent:*

1. *The different $\nabla = \nabla_{K/k}$ can be divided by p^m, that is $d = \nu_K(\nabla) \geq mep^m$.*
2. *The maximal ramification jump h for K/k is such that*
$$h - \left[\frac{h}{p}\right] = p^{m-1}e.$$
3. *The extension K/k is cyclic with the ramification jump $h_1 < \cdots < h_m = h$ such that*
$$h_i = \left[\frac{h_i}{p}\right] = p^{i-1}e, \;\; i = 1, 2, \ldots, m$$

(see [БВЖ], Prop. 1.5).

Corollary. — *Let in the extension K/k p^m divide the different, then the maximal ramification jump h is such that*

$$h \equiv \bar{h}(1 + p + \cdots + p^{m-1}) \bmod p^m$$
$$\bar{h} \equiv e \bmod (p-1).$$

In particular, if $(h, p) = 0$ then $\bar{h} = e_*$.

Proof. — The proposition 1.1 gives

$$h - \left[\frac{h}{p}\right] = p^{m-1}e$$

in our case; hence

$$h = \frac{p^m(e-\bar{h})}{p-1} + \frac{(p^m-1)\bar{h}}{p-1}$$

and the congruences of the corollary immediately follow from the last equality.

1.3. — Let F be an intermediate field in the extension K/k such that K/F is the cyclic extension of power p with the Galois group $H = \mathrm{Gal}(K/F) = \langle\sigma\rangle = \mathbb{Z}/p\mathbb{Z}$. Suppose that the ramification jump h of the extension K/F is relatively prime to p. Consider $o_k[H]$-the submodule $\mathfrak{N}$ in K, having o_k basis like this

$$\mathfrak{N} = \langle\xi, \lambda_1(\sigma-1)\xi, \ldots, \lambda_{p-1}(\sigma-1)^{p-1}\rangle,$$

where $\xi \in K$, $\nu_k(\xi) \equiv h \bmod p$, $\lambda_1, \ldots, \lambda_{p-1} \in k$, $-e \le \nu_k(\lambda_{p-1}) \le \cdots \le \nu_k(\lambda_1) \le 0$.

Proposition 1.3. — *The following conditions are equivalent:*

a) $\mathfrak{N}$ *is decomposible as* $o_k[H]$*-module;*

b) $\mathrm{tr}/p(\mathfrak{N}) \subset \mathfrak{N}$*, where* $\mathrm{tr} = \mathrm{tr}_{K/F}$*;*

c) $(p\lambda_{p-1})^{-1} \in \mathscr{O}_K$*, that is* $\nu_k(\lambda_{p-1}) + e \ge 0$.

For the proof see [БВЖ], lemma 3.1.

1.4. — Let $\mathscr{M}^\kappa$ be an ideal of K. Consider o_k-modules

$$\mathfrak{N}_i = \langle\xi_i, \lambda_{i,1}(\sigma-1)\xi_i, \ldots, \lambda_{i,p-1}(\sigma-1)^{p-1}\xi_i\rangle,$$

where $\nu_K(\xi_i) = \kappa + \overline{h-\kappa} + pi$, $0 \le i < p^{m-1}$;

$$\lambda_{ij} \in k,\ \ \nu_k(\lambda_{ij}) = -\left[\frac{\nu_k(\xi_i) + jh - x}{p^m}\right] = -\left[\frac{\overline{h-x} + jh + pi}{p^m}\right].$$

It's clear that

$$-e \le \nu_k(\lambda_{i,p-1}) \le \nu_k(\lambda_{i,p-2}) \le \cdots \le \nu_k(\lambda_{i,1}) \le 0$$

hence $\mathfrak{N}_i$ are $o_k[H]$-modules.

Besides, from $\nu(\xi_i) \equiv h \bmod p$ we've got that $\nu_K((\sigma-1)^j\xi_i) = \nu(\xi_i) + jh$, $0 \le i < p^{m-1}$, $0 \le j \le p-1$. These numbers form a complete residue system modulo p^m, hence the meanings

$$\nu_K(\lambda_{ij}(\sigma-1)^j\xi_i)$$

is a transposition of numbers $\kappa, \kappa+1 \leq \kappa+p^m-1$. Therefore the joining of o_k-basis of all $\mathfrak{N}_i$ is o_k-basis of all ideal $\mathscr{M}^\kappa$ and hence the ideal $\mathscr{M}^\kappa$ has the following $o_k[H]$-decomposition

$$\mathscr{M}^\kappa = \bigoplus_{i=1}^{p^m-1} \mathfrak{N}_i \,. \tag{1}$$

PROPOSITION 1.4.

a) If $p^m(e-1) < (p-1)h \leq p^m(e-1)+p$ then all $\mathfrak{N}_i$ except $\mathfrak{N}_{p^{m-1}-1}$ for every ideal $\mathscr{M}^\kappa$ in K are decomposable as $o_k[H]$-modules.

b) If $(p-1)h \leq p^m(e-1)$ then all $\mathfrak{N}_i$ for every ideal $\mathscr{M}^\kappa$ in K are decomposable as $o_k[H]$-modules.

c) If $p^m(e-1) < (p-1)h < p^m e-(p-1)$ or $(p-1)h = p^m e-(p-1)$ and $(p,x)=1$ then $\mathfrak{N}_0$ for every ideal $\mathscr{M}^\kappa$ in K is the only decomposable $o_k[H]$-module.

The statements can be checked directly using the condition **c)** of Proposition 1.3 (see also Lemma 3.3 from [БВЖ]).

LEMMA 1.4. — *Let in the extension K/k the ramification index p^m divide the different and all the ramification jumps of the extension K/k are relatively prime to p. Let for the ideal $\mathscr{M}^\kappa$ we've got*

$$0 < \bar{\kappa} < \bar{h} \,. \tag{2}$$

Then in the decomposition (1) there is only one undecomposable $o_k[H]$-module, namely $\mathfrak{N}_0$.

Proof. — According to Proposition 1.3 the undecomposability of $o_k[H]$-module $\mathfrak{N}_i$ is equivalent to the inequality

$$-v_k(\lambda_{i,p-1}) \leq e-1$$

that is

$$\left[\frac{\overline{h-\kappa}+pi+(p-1)h}{p^m}\right] \leq e-1 \,.$$

This, in his turn, is equivalent to

$$\overline{h-\kappa}+pi+(p-1)h \leq p^m e-1 \,. \tag{3}$$

As $p^m|\nabla$ then be have got $h-\left[\frac{h}{p}\right] = p^{m-1}-e$, hence $(p-1)h = p^m e-\bar{h}$. Besides, from (2) we have got

$$\overline{h-\kappa} = \bar{h}-\bar{\kappa} \,.$$

Taking into consideration these two equality the inequality (3) can be rewritten as

$$pi - \bar{\kappa} \leq -1$$

and it holds only for $i = 1$, that is only $o_k[H]$-module $\mathfrak{N}_0$ is undecomposable.

The lemma is proved.

1.5. — Let k be an arbitrary field of characteristic char $k \neq p$ and K/k be a cyclic extension of degree p^n; $G = \mathrm{Gal}(K/k) = \langle\sigma\rangle$.

Suppose that the order of the p-torsion in k^* is equal to p^s, $s \geq 1$.

Denote $\mu = \min(n, s)$, $\zeta = \zeta_{p^\mu}$. Let E be a subextension in K/k, $[K : E] = p^\mu$. Then $K = E(\theta)$, where $\theta^{p^\mu} \in E$.

Lemma 1.5.1 (see also lemma 4.1.1 from [ББЖ]). — *Consider* $E := \mathrm{Ker}(\sigma^{p^{n-\mu}} - \zeta^i) = E\theta^i$. *Then* $k[G]$*-modules* E_i *are undecomposable when* $(i, p) = 1$.

Proof. — It is known that $K \cong k[G]$ as $k[G]$-module . On the other hand, the ring isomorphism

$$k[G] \cong k[X]/(X^p - 1) = \bigoplus_{i=0}^{p^\mu - 1} k[X]/(X^{p^{n-\mu}} - \zeta^i)$$

makes E_i identical to $k[X]/(X^{p^{n-\mu}} - \zeta^i)$. If $(i, p) = 1$ then the polynomial $X^{p^{n-\mu}} - \zeta^i$ is undecomposable over k, hence $k[X]/(X^{p^{n-\mu}} - \zeta^i)$ is a prime $k[X]/(X^{p^n} - 1) \cong k[G]$-module and E_i is a prime $k[G]$-module.

From this lemma one can immediately obtain the following statement. Let the initial field k from 1.5 do not contain all the p-th roots of unity.

Suppose $k' = k(\zeta_p)$, $K' = K(\zeta_p)$

$$G' = \mathrm{Gal}(K'/K) \cong \mathrm{Gal}(k'/k).$$

Let E be a subextension in K/k of degree p^μ and $\mu = \min(n, s)$, p^s is the order of p-torsion in k'. If $E' = E(\zeta_p)$ then $K' = E'(\theta)$, where $\theta^{p^\mu} \in E'$.

Lemma 1.5.2. — *Let there is a* $k[G]$*-decomposition*

$$K = M \oplus N \tag{4}$$

and the field E *is in one of the decomposition component. Then the decomposition (4) is a* $E[G_E]$*-module decomposition where* $G_E = \mathrm{Gal}(K/E)$.

Proof. — If k contains all the p-th roots of the unity then the statement follows from Lemma 1.5.1. Otherwise, we can consider the extension K'/k'.

1.6. — Under assumption of 1.1 suppose that K/k is an abelian extension of degree p^n and the corresponding extension of the residue field is separable.

Let T be the inertia subfield, $G_T = \mathrm{Gal}(K/T)$, $\mathscr{O} = \mathscr{O}_K$.

PROPOSITION 1.6. — *Any $o[G]$-decomposition of an ideal of the field K is also a $\mathscr{O}_T[G_T]$-decomposition.*

(See [БВЖ], Prop. 4.6.1 and 4.6.2.)

1.7. — Let k be a complete discrete valuation field of characteristic 0 with the residue field of characteristic p, containing an primitive p^m-th root of unity $\zeta := \zeta_{p^m}$ and let K/k be a cyclic extension of degree p^m:

$$K = k(\theta),\ \ \theta^{p^m} \in k\,.$$

Let K_r be subextension in K/k such that $[K : K_r] = p^r$, $G^{(r)} = \mathrm{Gal}(K/K_r)$ and let σ be a generator of the Galois group $G = \mathrm{Gal}(K/k)$, $s = \sigma^{p^{m-r}}$ be a generator of the Galois group $G^{(r)}$.

LEMMA 1.7. — *Let I be an ideal in K and $I = \mathfrak{A} \oplus \mathscr{L}$ be an $\mathscr{O}_K[G]$-decomposition. Consider*

$$\begin{aligned} K^{(i)} &= \mathrm{Ker}(s - \zeta^i) = K_r\theta^i \\ I \cap K_r^{(i)} &= I_{r,i}\theta^i \\ \mathfrak{A} \cap K_r^{(i)} &= \mathfrak{A}_{r,i}\theta^i \\ \mathscr{L} \cap K_r^{(i)} &= \mathscr{L}_{r,i}\theta^i \end{aligned}$$

where $i = 0$ or $(i,p) = 1$. Then the ideal $I_{r,i}$ of the field K_r is the direct sum of $o_k[G/G_r]$-modules $\mathfrak{A}_{r,i}$ and $\mathscr{L}_{r,i}$.

Proof. — We have

$$\begin{aligned} I_{r,i}\theta^i &= \mathrm{Ker}(s - \zeta^i : \mathfrak{A} \oplus \mathscr{L} \mapsto \mathfrak{A} \oplus \mathscr{L}) \\ &= \mathrm{Ker}(s - \zeta^i : \mathfrak{A} \to \mathfrak{A}) \oplus \mathrm{Ker}(s - \zeta^i : \mathscr{L} \mapsto \mathscr{L}) \\ &= \mathfrak{A}_{r,i}\theta^i \oplus \mathscr{L}_{r,i}\theta^i\,. \end{aligned}$$

So $I_{r,i} = \mathfrak{A}_{r,i} \oplus \mathscr{L}_{r,i}$ as o_k-module.

Further, $\mathfrak{A}_{r,i}$ and $\mathscr{L}_{r,i}$ are contained in K_r therefore they are stable with respect to the action of $G^{(r)}$.

So now we have to check that $\mathfrak{A}_{r,i}$ and $\mathscr{L}_{r,i}$ are G-stable. Really, $\mathfrak{A}_{r,i}\theta^i$ and $\mathscr{L}_{r,i}\theta^i$ are G-stable. For every $g \in G$, $g(\theta^i) = \zeta^a\theta^i$ for some $a \in \mathbb{Z}$ and $\zeta^a \in o_k$. Lemma is proved.

1.8. Normal basis lemma. — Let K/k be a cyclic totally ramified extension of degree p^m with the maximal ramification jump $h := h_m$, $(h,p) = 1$ and let the corresponding extension K'/k', $k' = k(\zeta_p)$ be radical, that is $K' = k'(\theta)$, $\theta^{p^m} \in k'$; $d = [k' : k]$.

LEMMA 1.8.1. — *One can take a unit of K' as the radical element θ.*

Proof. — Let σ be a generator of the Galois group of the extension K'/k, g be a generator of the Galois group of the extension k'/k. Then we have $\theta^\sigma = \zeta\theta$, $\zeta^g = \zeta^r$, where ζ is some primitive p^m-th root of unity, r is a generator of the group of the p^m-th roots of unity in the group $(\mathbb{Z}/p^m\mathbb{Z})^*$. It is obviously that $r \not\equiv 1 \bmod p$. Consider the element $\varepsilon = \theta^r/\theta^g$ and check that $\varepsilon \in k'$. Really,

$$\varepsilon^\sigma = \theta^{r\sigma}/\theta^{g\sigma} = (\zeta\theta)^r/\zeta^r\theta^g = \theta^r/\theta^g = \varepsilon.$$

So $v'(\varepsilon) \equiv 0 \bmod p^m$, then $v'(\theta^r/\theta^g) = (r-1)v'(\theta) \equiv 0 \bmod p^m$, then $v'(\theta) \equiv 0 \bmod p^m$. Lemma is proved.

LEMMA 1.8.2 (normal basis lemma). — *An element x of the field K for which $v_K(x) \equiv h \bmod p^m$ generates a normal basis in the extension K/k.*

Proof. — Prove the lemma by induction in the degree of the extension K/k. If $m = 1$ then the elements $x, (\sigma-1)x, \dots, (\sigma-1)^{p-1}x$ have the orders which compose a complete set of residues modulo p. Hence they compose a basis of the extension K/k. Hence a $k[G]$-module X, generated by x is equal to K.

Furthermore, decompose an element x in the basis $1, \theta, \dots, \theta^{p-1}$ of the extension K/K_1:

$$x = x_0 + x_1\theta + \cdots x_{p-1}\theta^{p-1}, \ \ x_i \in K_1.$$

Let $X = \langle x \rangle$, $X_i = \langle x_i \rangle$, $0 \le i \le p-1$, $-k[G]$-modules, generated by $x, x_0, \dots, x_{p-1}$ correspondingly.

We have to check that

$$X = K.$$

In the paper [BV] there was proved that

$$v_{K_1}(x_i) = \frac{v_K(x) + (p-1)h}{p} + p^{m-1}e, \ \ 0 \le i \le p-1$$

so we have got

$$v_{K_1}(x_i) \equiv h \bmod p^{m-1}.$$

But $h := h_m \equiv h_{m-1} \bmod p^{m-1}$ (see Prop. 1.2), therefore the induction assumption holds for the elements $x_0, x_1, \dots, x_{p-1}$ and $k[G]$-modules X_i are equal to K_1.

Furthermore, for any element $g \in G$, $g(\theta^i) = \zeta^{a_i}\theta^i$, $a \in \mathbb{Z}$ holds and $\zeta^{a_i} \in k$. So $k[G]$-module, generated by $x_i\theta^i$, $0 \leq i \leq p-1$ is equal to $K_i\theta^i$. It is clear that these $k[G]$-modules are contained in X, so $X = K$. The lemma is proved.

2. The main theorem

2.1. — According to Proposition 1.6 we can suppose that the extension K/k is totally ramified. Throughout this paragraph we suppose that the ramification index p^m of the extension K/k divides the different ∇ of this extension, hence in particular Prop. 1.2 induces that K/k is cyclic.

Let

K_i be a supextension of degree p^i in K/k;

$\mathcal{M}_i$ be the maximal ideal in the ring of integers of the field K_i;

$d_{K/k} = \nu_K(\nabla)$ be the exponent of the different

e_* be the residue of the absolute ramification index e of the field k modulo $(p-1)$ in the positive residue system.

2.2. — Consider the ideal $\mathcal{M}^\kappa$ in the field K and let $\kappa = \kappa_0 + \kappa_1 p + \cdots$, $0 \leq i < p$ be the p-adic decomposition.

PROPOSITION 2.2.1. — *If for the ideal $\mathcal{M}^\kappa$ we have*

1) $p \mid \kappa$, or

2) $0 < \kappa_0 \leq \bar{h}$, $0 \leq \kappa_1 \leq \bar{h}, \ldots, 0 \leq \kappa_{r-2} \leq \bar{h}$, $x_{r-1} > \bar{h}$ for $1 \leq r \leq m$ then there is a $\alpha[G]$-decomposition

$$\mathcal{M}^\kappa = \frac{\mathrm{tr}_{K/K_r}}{p^r}(\mathcal{M}^\kappa) \oplus (\mathrm{Ker}\,\mathrm{tr}_{K/K_r} \cap \mathcal{M}^\kappa)\,.$$

Remark. — The residue $\bar{h}$ can be changed according to the congruence (5) to be residue e_*.

Proof. — Calculate the powers of the ideals

$$\mathcal{M}_j^{c_j} = \frac{\mathrm{tr}_{K/k_j}}{p^j}(\mathcal{M}^\kappa).$$

We've got

$$c_1 = \frac{\kappa + \overline{h-\kappa} + (p-1)h}{p} - p^{m-1}e = \left[\frac{\kappa}{p}\right] = \kappa_1 + p\kappa 0_2 + \cdots \tag{5}$$

(see [Se], ch. V, § 3) because $\overline{h-\kappa} = \bar{h} - \bar{\kappa}$ and $\bar{h} + (p-1)h = p^{m-1}e$.

Similarly $c_2 = \left[\frac{c_1}{p}\right] = \left[\frac{\kappa}{p^2}\right], \ldots, c_r = \left[\frac{\kappa}{p^r}\right] + 1$ because $\kappa_{r-1} > \bar{h}$.

This induces $p^r c_r \geq i$. Hence $\mathrm{tr}_{K/K_r}/p^r$ is an idempotent operator on the ideal $\mathscr{M}^\kappa$. This induces the statement of the proposition.

Corollary 2.2.2. — *If $h = \frac{p^m e}{p-1}$ then any ideal of the field K is a decomposable $o[G]$-module.*

The proof is obvious, since in this case $\bar{h} = 0$. Taking into consideration Corollary 1 further we can suppose that $(h, p) = 1$, hence

$$\frac{p^m e}{p-1} - 1 \leq h < \frac{p^m e}{p-1}.$$

2.3. Lemma 2.3. — *Let the ideal $\mathscr{M}^\kappa$ be decomposable as $o[G]$-module, that is*

$$\mathscr{M}^\kappa = \mathfrak{A} \oplus \mathscr{L}$$

and $0 < \bar{\kappa} \leq \bar{h} = e_*$. Then one of the decomposition component contains an element x such that

$$v_k\Big(\frac{\mathrm{tr}}{p}(x)\Big) = p\Big[\frac{\kappa}{p}\Big].$$

Proof. — Consider $o_k[H]$-decomposition (1) of the ideal $\mathscr{M}^\kappa$;

$$\mathscr{M}^\kappa = \bigoplus_{i=0}^{p^m-1} \mathfrak{N}_i,$$

where $H = \mathrm{Gal}(K/K_1)$. In this decomposition under our assumption all the $o_k[H]$-modules $\mathfrak{N}_i$ are decomposable except $\mathfrak{N}_0$ (see Lemme 1.4). The Krull-Schmidt theorem [see [BF], § 8] shows

$$\mathfrak{A} = \bigoplus_{i\in I} \mathfrak{N}'_i, \quad \mathscr{L} = \bigoplus_{i\in I} \mathfrak{N}'_i$$

where $I \subset \{0, 1, \ldots, p^{m-1} - 1\}$ and $\mathfrak{N}'_i \cong \mathfrak{N}_i$ as $o_k[H]$-modules. Suppose that $0 \in I$, that is $\mathfrak{N}'_0 \cong \mathfrak{N}_0$ is a direct summand in $\mathfrak{A}$.

It's easy to compute that the meaning of $\frac{\mathrm{tr}_{k/k'}}{p}$ for the generator ξ_0 of the module $\mathfrak{N}_0$ is equal to $p\left[\frac{\kappa}{p}\right]$, really

$$v_k(\xi_0) = \kappa + \overline{h-\kappa}.$$

But $\mathrm{tr} = 1 + \sigma + \cdots + \sigma^{p-1} = pf(\sigma) + (\sigma - 1)^{p-1}$, where $f(X)$ is a polynomial with the integer coefficients.

Since $\nu_k(\xi_0) \equiv h \bmod p$

$$\nu_k((\sigma-1)^{p-1}\xi_0) = \nu_k(\xi_0) + (p-1)h = \kappa + \overline{h-\kappa} + (p-1)h.$$

On the other hand,

$$\nu_k(pf(\sigma)(\xi_0)) \geq p^m e + \nu_k(\xi_0) = p^m e + \kappa + \overline{h-\kappa}\,.$$

But $(p-1)h < p^m e$, hence

$$\nu_k(\mathrm{tr}\,\xi_0) = \nu_k((\sigma-1)^{p-1}\xi_0) = \kappa + \overline{h-\kappa} + (p-1)h.$$

The condition $h - \left[\frac{h}{p}\right] = p^m e$ induces $(p-1)h = p^m e - \bar{h}$. Besides, $\overline{h-\kappa} = \bar{h} - \bar{\kappa}$ in our case; therefore

$$\nu_k\Big(\frac{\mathrm{tr}}{p}\xi_0\Big) = (\kappa + \overline{h-\kappa} + p^m e - \bar{h}) = p^m e = \kappa - \bar{\kappa} = p\Big[\frac{\kappa}{p}\Big]\,.$$

On the other hand for all the rest generators ξ_i, $i \neq 0$ we've got

$$\nu_k\Big(\frac{\mathrm{tr}}{p}\Big) \geq \kappa$$

because the corresponding $\mathscr{O}_k[H]$-modules $\mathfrak{N}_i$ are decomposable which is possible according to Prop. 1.3 if and only if

$$\frac{\mathrm{tr}}{p}\xi_i \in \mathfrak{N}_i \subset \mathscr{M}^{\kappa}\,.$$

Let ξ_i' be corresponding generators of isomorphic $\mathscr{O}_K[H]$-modules $\mathfrak{N}_i'$.

Since all the modules $\mathfrak{N}_i'$, $i \neq o$ are decomposable because they are isomorphic to the corresponding modules $\mathfrak{N}_i$ then again according to Prop. 1.3

$$\frac{\mathrm{tr}}{p}\xi_i' \in \mathfrak{N}_i' \subset \mathscr{M}^{\kappa},\ \ i \neq 0\,.$$

Then for the ideal $\frac{\mathrm{tr}}{p}\,\mathscr{M}^{\kappa}$ we've got two $\mathscr{O}_k$-bases:

$$\begin{aligned}\frac{\mathrm{tr}}{p}\,\mathscr{M}^{\kappa} &= \langle\frac{\mathrm{tr}}{p}\xi_i,\ \ i = 0,1,\ldots,p^{m-1}-1\rangle\\ &= \langle\frac{\mathrm{tr}}{p}\xi_i',\ \ i = 0,1,\ldots,p^{m-1}-1\rangle\,.\end{aligned}$$

In both bases the elements with the positive indexes are contained in the ideal $\mathscr{M}^{\kappa}$. The first basis contains the only element $\frac{\mathrm{tr}}{p}\xi_0$, which is not from $\mathscr{M}^{\kappa}$ therefore corresponding to it and also not included in the ideal $\mathscr{M}^{\kappa}$ element $\frac{\mathrm{tr}}{p}\xi_0'$ has the same order, that is $\nu_k\Big(\frac{\mathrm{tr}}{p}\xi_0\Big) = \nu_k\Big(\frac{\mathrm{tr}}{p}\xi_0'\Big)$ which induce (see (1.4))

$$\nu_k\Big(\frac{\mathrm{tr}}{p}\xi_0'\Big) = p\Big[\frac{\kappa}{p}\Big]\,.$$

Le lemma is proved.

2.4. — Let the assumptions of 1.3 and 1.4 hold and let $\zeta := \zeta_p$ be a p-th root of unity. Remark, that $v_k(\zeta^i - 1) = \frac{p^m e}{p-1} > h$. So for any element x of the ring $\mathscr{O}_K$ which has the relatively prime to p order in the field K we've got

$$v_k((\sigma - 1)x) = v_k((\zeta^i\sigma - 1)(x)),$$

because $\zeta^i\sigma - 1 = \zeta^i(\sigma - 1) + (\zeta^i - 1)$. That's why in 1.3 and 1.4 we can replace the operator $(\sigma - 1)$ by $(\zeta^i\sigma - 1)$ and repeating the proof of Prop. 1.3, 1.4, Lemma 1.4.1 and Lemma 2.3 we get the following result.

LEMMA 2.4. — *Let the ideal $\mathscr{M}^\kappa$ be decomposable as $o[G]$-module, that means*

$$\mathscr{M}^\kappa = \mathfrak{A} \oplus \mathscr{L}$$

and

$$0 < \bar{\kappa} \leq \bar{h} = e_* .$$

Then one of the decomposition component contains an element x_i for which the element

$$y_i = \left(1 + \zeta^i\sigma + \zeta^{2i}\sigma^2 + \cdots + (\zeta^i\sigma)^{p-1}\right)(x_i)/p$$

satisfies the condition

$$v_k(y_i) = p\left[\frac{\kappa}{p}\right] .$$

2.5. — Here there will be proved the main theorem B (see Introduction). If the conditions of the theorem B hold then the corresponding ideals are decomposable (see Prop. 2.2.1).

Prove the converse statement. So, let the ideal $\mathscr{M}^\kappa$ of the extension K/k in which the ramification index p^m divides the different of this extension is decomposable. We use the induction in the degree of the extension. Remark that the extension K/k can be considered according to Prop. 1.6 as totally ramified, so $p^m = [K : k]$.

Let $m = 1$. If the ramification jump h can be divided by p then all the ideals in K/k are decomposable (see Corollary 2.2.2). If $(h, p) = 1$ and $\mathscr{M}^\kappa$ is an ideal in K/k then decomposability of the ideal induces, according to Lemma 1.4 that $p \mid \kappa$ or $\bar{\kappa} > \bar{h}$. In both cases the decomposability is proved in Prop. 2.2.1.

2.6. — Furthermore, let

$$\mathscr{M}^\kappa = \mathfrak{A} \oplus \mathscr{L} \tag{6}$$

be a nontrivial $o[G]$-decomposition.

Consider three cases

A) The field K_{m-1} (see 2.1) is included in one of the linear envelopes $k\mathfrak{A}$ or $k\,\mathscr{L}$.

B) The field K_{m-1} is not included in these linear envelopes and $k' = k(\xi_p)$ (the field k' can coincide with k) does not contain all the p^m-th root of unity.

C)The field k' contains all the p^m-th roots of unity.

In case **A)** according to Lemma 1.5.2, decomposition of the linear envelope

$$k = k\,\mathcal{M}^{\kappa} = k\mathfrak{A} \oplus k\,\mathscr{L}$$

will be a $K_{m-1}[G_{K_{m-1}}]$-module decomposition where $G_{K_{m-1}} = \mathrm{Gal}(K/K_{m-1})$, hence decomposition (6) of the ideal $\mathcal{M}^{\kappa}$ will be a $\mathcal{O}_{K_{m-1}}[G_{K_{m-1}}]$-module decomposition and we can apply to it the induction assumption.

2.7. — In the case **B)** any intermediate field is not included in the linear envelopes $k\mathfrak{A}$ and $k\,\mathscr{L}$. That's why the non trivial decomposition (6) induces the nontrivial decomposition of the following ideals

$$\mathcal{M}_i^{a_i} = \frac{\mathrm{tr}_{K/K_i}}{p^i}(\mathcal{M}^{\kappa}) = \frac{\mathrm{tr}_{K/K_i}}{p^i}\mathfrak{A} \oplus \frac{\mathrm{tr}_{K/K_i}}{p^i}\,\mathscr{L}$$

in the extensions K_i/k, $1 \le i \le m-1$

$$\mathcal{M}_i^{b_i} = K_i \cap \mathcal{M}^{\kappa} = (K_i \cap \mathfrak{A}) \oplus (K_i \cap \mathscr{L})\,.$$

Let $\kappa \equiv \kappa_0 + \kappa_1 p + \cdots \bmod p^m$ where $0 \le \kappa_i \le p-1$. If $\kappa_0 = 0$ or $\kappa_0 > \bar{h}$ then the conditions of Theorem B hold and the proof is finished.

If $0 < \kappa_0 \le \bar{h}$ then the degree a_1 is equal to

$$a_1 \equiv \kappa_1 + p\kappa_2 + \cdots \bmod p^{m-1}$$

(see (5) from Prop. 2.2.1).

For the ideal $\mathcal{M}_1^{a_1}$ the induction assumption holds, hence $\kappa_1 = 0$ or there exists $\kappa_i > \bar{h}$, $1 \le i \le m-1$. In the second case for the ideal $\mathcal{M}^c$ the condition of the Theorem B holds. In the first case we can pass to the next extension K_2/k and the same arguments give the holding of the conditions of the Theorem B for the ideal $\mathcal{M}^{\kappa}$, or $\kappa_1 = \kappa_2 = 0$.

So we've got two possibilities: the conditions of the Theorem B hold for the ideal $\mathcal{M}^{\kappa}$ or $\kappa \equiv \kappa_0 \bmod p^m$, where $0 < \kappa_0 \le \bar{h}$.

In the second case consider for our ideal $\mathcal{M}^{\kappa} = \mathcal{M}^{\kappa_0}$ the ideal $\mathcal{M}_1^{b_1} = K_1 \cap \mathcal{M}^{\kappa}$ for which on the one hand

$$b_1 \equiv 1 \bmod p^m - 1 \tag{7}$$

and on the other hand it has a nontrivial decomposition in K_1/k, hence according to the induction assumption the conditions of Theorem B hold, that is $\bar{b}_1 = 0$ or $\bar{b}_1 > \bar{h} \ge 1$ which is contradiction to (7).

2.8. — For the case **C)** we need the following lemma. Let K/k be a totally ramified cyclic extension of degree p^m with the maximal jump

$$h := h_m = \frac{p^m e}{p-1} - 1$$

and suppose $\zeta_{p^m} \in k$. Then

$$K = k(\theta)$$

where $\theta^{p^m} \in k$.

LEMMA 2.8. — *Suppose that in any subextension F/k, $F \neq K$, the ideal $\mathcal{M}_F^{\kappa}$ with $p \nmid \kappa$ is decomposable as $o[\mathrm{Gal}(F/k)]$-module. Let for the ideal $\mathcal{M}^{\kappa}$, $p \mid \kappa$, of the field K we have $o[G]$-extension*

$$\mathcal{M}^{\kappa} = \mathfrak{A} \oplus \mathscr{L} \cdots \tag{8}$$

If one of the summand (for example, $\mathfrak{A}$) of this decomposition contains an element κ such that

$$v_k(\kappa) \equiv \kappa - 1 \bmod p^m$$

then another summand is trivial.

Proof. — If $\kappa \equiv 0 \bmod p^m$ then the element x from the lemma will satisfy the following condition

$$v_k(x) \equiv \kappa - 1 \equiv h \bmod p^m$$

so it generates according to Lemma 1.7 a normal basis of the extension K/k, then the linear envelope $k\mathfrak{A}$ will coincide with K so $\mathscr{L} = (0)$.

If $\kappa = p^r \kappa_r$, $(\kappa_r, p) = 1$ and $1 \leq r \leq m-1$ then consider the subextension K/K_r of degree p^r and show that the decomposition (8) is $\mathcal{O}_r$-decomposition, where $\mathcal{O}_r$ is the ring of integers of the field K_r.

If it is so then the element x in the extension K/K_r will satisfy Lemma 1.8 that means it will generate a normal basis in this extension. So again $k\mathfrak{A} = K$ and $\mathscr{L} = (0)$. So we have to check that decomposition (8) is defined over $\mathcal{O}_r$.

Consider the intersections $\mathcal{M}^{\kappa} \cap K_r\theta^i$ and $\mathcal{M}^{\kappa} \cap K_r$, where $(i,p) = 1$. According to Lemma 1.7 we have

$$\mathcal{M}^{\kappa} \cap K_r\theta^i = \mathcal{M}_r^{c_i}\theta^i = \mathfrak{A}_i\theta^i \oplus \mathscr{L}_i\theta^i\,,$$

where $\mathfrak{A}_i\theta^i = \mathfrak{A} \cap K_r\theta^i$, $\mathscr{L}_i\theta^i = \mathscr{L} \cap K_r\theta^i$ and there is such a $o[H_r]$-decomposition

$$\mathcal{M}_i^{c_i} = \mathfrak{A}_i \oplus \mathscr{L}_i\,,$$

where $H_r = \mathrm{Gal}(K_r/k)$ since $p^r \mid \kappa$, $c_i = \left[\frac{\kappa}{p^r}\right] = \kappa_r \not\equiv 0 \bmod p$.

Therefore, according to the condition of our lemma the ideal $\mathcal{M}_r^{c_i}$ is decomposable, so the linear envelope $k\,\mathcal{M}_r^{c_i}\theta^i = K_r\theta^i$ lies or in the linear envelope $k\mathfrak{A}$ or $k\,\mathscr{L}$. That's why according to Lemma 1.5.2 decomposition (8) is a $[H_r]$-decomposition. The lemma is proved.

2.9. — Check the case **C)** (see 2.5). Consider the intersections of the ideal $\mathcal{M}^\kappa$ and the kernels of the operators $s-\zeta^i$, $i=0,1,\dots,p-1$, where s is a generator of the Galois group of the extension K/K_1, $\zeta := \zeta_p$.

Then we have, according to Lemma 1.7

$$\mathcal{M}^\kappa \cap K_i\theta^i = \mathcal{M}_i^{c_i}\theta^i = \mathfrak{A}_i\theta^i \oplus \mathscr{L}_i\theta^i$$

where

$$\mathfrak{A}_i\theta^i = \mathfrak{A}\cap \operatorname{Ker}(s-\zeta^i) = \mathfrak{A}\cap K_1\theta^i,$$
$$\mathscr{L}_i\theta^i = \mathscr{L}\cap \operatorname{Ker}(s-\zeta^i) = \mathscr{L}\cap K_1\theta^i.$$

And there is a $\mathcal{O}[H_1]$-decomposition

$$\mathcal{M}_r^{c_i} = \mathfrak{A}_i \oplus \mathscr{L}_i\,,$$

where

$$H_1 = \operatorname{Gal}(K/K_1) = \langle s\rangle\,.$$

Compute the orders c_i:

$$c_i = \begin{cases} \dfrac{\kappa}{p} - \dfrac{i\nu_k(\theta)}{p}, & \text{if } p\,|\kappa \\ \left[\dfrac{\kappa}{p}\right] + 1 - \dfrac{i\nu_k(\theta)}{p}, & \text{if } p\not|\kappa. \end{cases} \tag{9}$$

If c_i is relatively prime to p then the ideal $\mathcal{M}_1^{c_i}$ is decomposable in the extension K_1/k according to the induction assumption, so the linear envelope $k\,\mathcal{M}_i^{c_i}\theta^i = K_1\theta^i$ lies or the linear envelope $k\mathfrak{A}$, or in $k\,\mathscr{L}$.

Suppose now that $p\,|c_i$, the ideal $\mathcal{M}^\kappa$ is decomposable in the extension K/j and the condition of Theorem B for it doesn't hold, that is $0<\bar\kappa\le\bar h = e_*$. Then we can apply Lemma 2.3.1 for the intersection $\mathcal{M}^\kappa\cap K_1$ and Lemma 2.4 for the intersections $\mathcal{M}^\kappa\cap K_1\theta^i$, $1\le i\le p-1$. According to these lemmas one of the component of the decomposition $\mathcal{M}^\kappa = \mathfrak{A}\oplus\mathscr{L}$, say $\mathfrak{A}$, contains an element x_i, $0\le i\le p-1$, for which $y_i = (1+\zeta^i s+\dots+(\zeta^i s)^{p-1})(x_i)/p$ satisfies the condition $\nu_k(y_i) = p\left[\frac{\kappa}{p}\right]$. So, on one hand y_i is contained in the $o[G]$-module $\mathfrak{A}$ and on the other hand $y_i\in\operatorname{Ker}(\zeta^i s-1) = \operatorname{Ker}(\zeta^i(s-\zeta^{-i})) = K_1\theta^{-i}$, that means $y_i\in\mathfrak{A}_{-i}\theta^{-i}$. The element $z_i = y_i\theta^i\in\mathfrak{A}_{-i}$and has the order $\nu_k(z^i) = \left[\frac{\kappa}{p}\right] + \frac{i\nu_k(\theta)}{p}$.

But the corresponding ideal $\mathcal{M}_1^{c_i} = \mathfrak{A}_{-i} \oplus \mathscr{L}_{-i}$ has the order

$$c_{-i} = \left[\frac{\kappa}{p}\right] + 1 + \frac{i\nu_k(\theta)}{p}$$

because $p \not| \kappa$ (see (9)). Hence,

$$\nu_{K_1}(z_i) = c_i - 1$$

and the conditions of Lemma 2.8 hold. Therefore, $\mathscr{L}_{-i} = (0)$ and $k\,\mathcal{M}_1^{c_{-i}} = K_1\theta^{-i}$ lies in $k\mathfrak{A}$.

So we've shown that for every $i : 0 \leq i \leq p-1$ the linear envelope $K_1\theta^i$ lies or in $k\mathfrak{A}$, or in $k\,\mathscr{L}$ and that means that the decomposition $K = k\mathfrak{A} \oplus k\,\mathscr{L}$ is defined over K_1, so $\mathcal{M}^\kappa = \mathfrak{A} \oplus \mathscr{L}$ is a $o_1[H_1]$-decomposition and the theorem is proved.

2.10. — It's left the case, when the field k has not all the p-th rooth of unity but the extension K'/k is radical. In this case consider so called composit-modules defined in the paper [ББЖ].

Definition. — *An $\mathcal{O}_K[G']$-submodule in K' is called a composit if it is also a $\mathbb{Z}_p[\zeta_p]$-module.*

Remark 1. — If $k' = k$ then composit-modules are the ideals of K'.

Remark 2. — If I is an ideal in K then $o'I$ is a composit-module in K'.

Applying Prop. 2.3 of [ББЖ] and repeating the preceding arguments we get our statement in this case.

Bibliography

[B] N. Byott. — *On Galois isomorphisms between ideals in extensions of local fields*, Manuscripta Math. **73** (1991), 282–311.

[BF] Z.I. Borevich and D.K. Faddeev. — *Theory of homologies in groups, II. On projective resolvents of finite groups*, Vestn. Leningr. Univ. **7** (1959), 72–81.

[BV] Z.I. Borevich and S.V. Vostokov. — *The ring of integral elements of an extension of prime degree of a local field as a Galois module*, Inst. Steklov (lOMI) **31** (1973), 24–37; English trans. in J. Soviet Math., **6** (1) (1976), 227–238.

[E] G.G. Elder. — *Galois module structure of ideals in wildly ramified cyclic extensions of degree p^2*, Ann. Inst. Fourier (Grenoble) **45,** (3) (1995), 625–647.

[EM] G.G. Elder and M.L. Madan. — *Galois module structure of the integers in weakly ramified extensions*, Arch. Math. **64** (1995), 117–120.

[FV] I. Fesenko and S. Vostokov. — *Local field and their extensions: a constructive approach*, AMS, Providence, RI, 1993.

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

[Le] G. Lettl. — *Note on the Galois module structure of quadratic extensions*, Col. Math., vol. LXVII.

[M1] Y. Migata. — *On the module structure of the ring of all integers of a $\mathfrak{p}$-adic number field*, Nagoya Math. J. **54** (1974), 53–59.

[M2] Y. Migata. — *On the module a cyclic extension over a $\mathfrak{p}$-adic number field*, Nagoya Math. J. **74** (1979), 61–68.

[M3] Y. Migata. — *On the module structure of a $\mathfrak{p}$-adic number field*, Nagoya Math. J. **77** (1980), 13–23.

[M4] Y. Migata. — *On the Galois Module Structure of Ideals and Rings of all Integers of $\mathfrak{p}$-adic number field*, J. of Algebra **177** (1995), 627–642.

[N] E. Nœther. — *Normalbasis bei Körpern ohne höher Verzweigung*, J. Reine und Angew. Math. **167** (1932), 147–152.

[Se] J.-P. Serre. — *Local fields*, Graduate Textes in Mathematics, **67**, Springer-Verlag, Berlin-Heidelberg-New-York, 1979.

[U] S. Ullom. — *Integral normal bases in Galois extensions of local fields*, Nagoya Math. J. **39** (1970), 141–148.

[V1] S.V. Vostokov. — *Ideals of the abelian p-extension of an irregular local field as Galois modules*, Zap. Nauchn. Sem. Leningrad. Otdel. Math. Inst. Steklov (LOMI) **46** (1974), 14–35; English trans. in J. Soviet Math., **9** (3) (1978), 299–317.

[V2] S.V. Vostokov. — *Ideals of the abelian p-extension of a local field as Galois modules*, Zap. Nauchn. Sem. Leningrad. Otdel. Math. Inst. Steklov (LOMI) **57** (1976), 64–84; English trans. in J. Soviet Math., **11** (4) (1979), 567–584.

[V3] S.V. Vostokov. — *A normal base of an ideal of a local field*, Zap. Nauchn. Sem. Leningrad. Otdel. Math. Inst. Steklov (LOMI) **64** (1976), 64–68; English trans. in J. Soviet Math., **17** (2) (1981), 1755–1759.

[БВЖ] М.В. Бондарко, С.В. Востоков, И. Б. Жуков. — Аддитивные модули Галуа в полных дискретно нормированных полях , Алгебра и анализ, 1997.

Mikhail V. BONDARKO & **Serguei V. VOSTOKOV** & **Oleg V. DEMCHENKO**
email : m@vbond.usr.pu.ru email : sergei@vostokov.usr.pu.ru email : vas@usr.pu.ru