Astérisque

JÜRGEN NEUKIRCH

The absolute Galois group of a p-adic number field

Astérisque, tome 94 (1982), p. 153-164

<http://www.numdam.org/item?id=AST_1982__94__153_0>

THE ABSOLUTE GALOIS GROUP OF A $\mathfrak{p}$-ADIC NUMBER FIELD

by

Jürgen NEUKIRCH

-:-:-:-

This is a report on the work of U. Jannsen and K. Wingberg on the explicit determination of the absolute galois group G_k of a $\mathfrak{p}$-adic number field k ([5], [6], [10]). This description depends upon four invariants q, n, p^s, α of k which are defined as follows.

Let $\bar{k}$ and k_{tr} be the algebraic closure and the maximal tamely ramified extension of k respectively. As is well known the galois group

$$\mathcal{G} = G(k_{tr}|k)$$

is generated by two elements σ, τ satisfying the relation $\sigma\tau\sigma^{-1} = \tau^q$. We put

$n = [k : \mathbb{Q}_p]$

q = cardinality of the residue class field of k,

$p^s = \# \mu_{p^s}$, μ_{p^s} being the group of p-power roots of unity in k_{tr}.

$\alpha : \mathcal{G} \to (\mathbb{Z}/p^s)^*$ the character given by $\rho\zeta = \zeta^{\alpha(\rho)}$, $\rho \in \mathcal{G}$, $\zeta \in \mu_{p^s}$.

α can also be replaced by two numbers $g, h \in \mathbb{Z}_p$ such that

$$g \equiv \alpha(\sigma), \quad h \equiv \alpha(\tau) \mod p^s .$$

With these invariants and under the assumption $p \neq 2$ the main result of Jannsen and Wingberg can be formulated as follows.

THEOREM. - The absolute galois group $G_k = G(\bar{k}|k)$ is isomorphic to the pro-finite group of $n+3$ generators $\sigma, \tau, x_o, \dots, x_n$ and the following defining relations

A. - The normal subgroup generated by $x_o, \dots, x_n$ is a pro-p-group.

B. - $\sigma\tau\sigma^{-1} = \tau^q$ (the "tame relation")

C. - There is only one additional relation, namely

$$\sigma x_o \sigma^{-1} = (x_o, \tau)^g x_1^{p^s} [x_1, x_2][x_3, x_4] \dots [x_{n-1}, x_n]$$

if n is even, and

$$\sigma x_o \sigma^{-1} = (x_o, \tau)^g x_1^{p^s} [x_1, y].[x_2, x_3] \dots [x_{n-1}, x_n]$$

if n is odd. Here we have put

$$(x_o, \tau) = (x_o^{h^{p-1}} \tau x_o^{h^{p-2}} \tau \dots x_o^h \tau)^{\frac{\pi}{p-1}} ,$$

where π is the element in $\hat{\mathbb{Z}}$ with $\pi\hat{\mathbb{Z}} = \mathbb{Z}_p$.

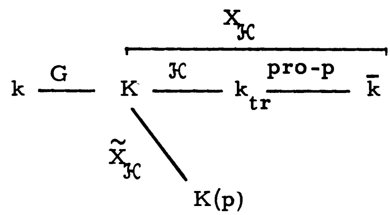
Remarks. - The condition A can easily be replaced by a collection of relations and expresses together with B the selfunder-standing relations in G_k .

For the exact definition of the element y occurring in the case of odd n we refer to the original paper [6]. It is of type $x_1^{f(\sigma, \tau)}$. If for example $\bar{k}|k$ is replaced by the maximal extension of $k(\mu_p)$ of odd ramification, then we can take $y = x_1^{\tau}$.

The proof of the theorem is based on the following method. For each finite normal subextension $K|k$ of $k_{tr}|k$ the galois group of the maximal p-extension $K(p)|K$ has the structure of a Demuškin group, given by class field theory. Moreover, a detailed study of the action of the group $G = G(K|k)$ on the group of units of K gives further information on the Demuškin structure under the G-action. These known properties of G_k are now taken as axioms for a new abstract concept, the concept of a "Demuškin formation", which goes already back to Koch [9], and which I therefore would like to call a Koch group over $\mathcal{G}$. Each such Koch group is endowed with invariants q, n, p^s, α .

In a first step it is proved that two Koch groups with the same invariants are isomorphic. Hereafter Jannsen and Wingberg show, that the abstract pro-finite group, defined by the generators and relations given in the theorem, is a Koch group with the same invariants as the Koch group $\mathcal{G}_k$ and is thus isomorphic to $\mathcal{G}_k$.

We now explain this procedure in more detail by looking at the following diagram of fields and galois groups.



Here $\mathcal{K}$ is an open normal subgroup of $\mathcal{G} = G(k_{tr}|k)$ contained in the kernel of α , so that μ_{p^s} is contained in the fixed field K of $\mathcal{K}$. $G = \mathcal{G}/\mathcal{K} = G(K|k)$, $X_{\mathcal{K}} = G(\bar{k}|K)$ and $\tilde{X}_{\mathcal{K}}$ is the galois group of the maximal p-extension $K(p)|K$. It is the maximal pro-p-factorgroup of $X_{\mathcal{K}}$ and is a Demuškin group. For these groups we have the following known properties.

I. - $\dim H^1(X_{\mathcal{K}}, \mathbb{F}_p) = n.\#G+2$, $\dim H^2(X_{\mathcal{K}}, \mathbb{F}_p) = 1$ and
$$H^1(X_{\mathcal{K}}, \mathbb{F}_p) \times H^1(X_{\mathcal{K}}, \mathbb{F}_p) \xrightarrow{\cup} H^2(X_{\mathcal{K}}, \mathbb{F}_p)$$
is a non degenerate anti-symmetric bilinear form.

II. - Viewing $H^1(\mathcal{K}, \mathbb{F}_p)$ as a 1-dimensional subspace of the symplectic space $H^1(X_{\mathcal{K}}, \mathbb{F}_p)$ we have an isomorphism of G-modules
$$H^1(\mathcal{K}, \mathbb{F}_p)^{\perp}/H^1(\mathcal{K}, \mathbb{F}_p) \cong \mathbb{F}_p[G]^n .$$
With respect to the induced non-degenerate bilinear form this G-module is hyperbolic, i.e., direct sum of two totally isotropic G-submodules.

III. - $(\tilde{X}^{ab}_{\mathcal{K}})_{tor} \cong \mu_{p^s}$ as a G-module.

<u>Explanation</u>. - Condition I expresses the well known fact that $\tilde{X}_{\mathcal{K}} = Gal(K(p)|K)$ is a Demuškin group. By class field theory
$$H^1(X_{\mathcal{K}}, \mathbb{F}_p) \text{ is dual to } K^*/K^{*p} = (\pi)/(\pi^p) \times U^1/(U^1)^p$$
where π is a prime element of k and U^1 the group of principal units of K . In this interpretation the cup product goes over into the Hilbert symbol on K^*/K^{*p} and $U^1/(U^1)^p$ contains $H^1(\mathcal{K}, \mathbb{F}_p)^{\perp}/H^1(\mathcal{K}, \mathbb{F}_p)$ as a subspace of co-

dimension 1 which is isomorphic to $\mathbb{F}_p[G]$.

The last isomorphism is a result of Iwasawa. The assertion on the hyperbolic property is due to Koch.

Taking the conditions I, II, III as axioms we come to the following abstract definition. Let $\mathcal{G}$ be any profinite group generated by two elements σ, τ such that $\sigma\tau\sigma^{-1} = \sigma^q$ and let $\alpha : \mathcal{G} \to (\mathbb{Z}/p^s)^*$ be a character.

DEFINITION. - A Koch group over $\mathcal{G}$ (Demuškin formation in Jannsen's and Wingberg's terminology) of degree n, of torsion p^s and character α, is a pro-finite group X together with a surjective homomorphism

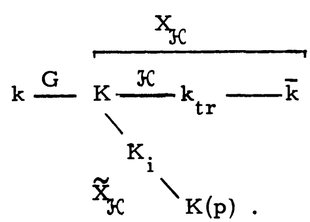
$$\Phi : X \to \mathcal{G}$$

such that for each open normal subgroup $\mathcal{K}$ of $\mathcal{G}$ in the kernel of α, the conditions I, II, III hold for $X_{\mathcal{K}} = \Phi^{-1}(\mathcal{K})$, where in III μ_{p^s} is replaced by the twisted $\mathcal{G}$-module $\mathbb{Z}/p^s(\alpha)$.

For these Koch groups we have now the following uniqueness theorem, which was announced by Koch [9] and was proved in full detail and even larger generality by Wingberg [10].

THEOREM I (Koch, Wingberg). - Two Koch groups X and Y over $\mathcal{G}$ with the same invariants n, p^s and α are isomorphic.

We indicate the concrete ideas of the proof, by sticking to the field theoretic situation and taking for X the Koch group G_k. The problem is roughly speaking, to reconstruct G_k purely by means of the axioms I, II, III. We look again at the diagram



The inserted field K_i is explained in a moment. Since $\mathrm{Gal}(\bar{k}|k_{tr})$ is a pro-p-group it is clear that $\bar{k} = \bigcup_{K \subseteq k_{tr}} K(p)$ and hence

$$G_k = \varprojlim_{\mathcal{K}} \mathrm{Gal}\,(K(p)|\,k).$$

This reduces us to the question, in which way the group $Gal(K(p)\,|\,k)$ is determined by the axioms. To attack this problem we look at the group extension

$$1 \longrightarrow Gal(K(p)\,|\,K) \longrightarrow Gal(K(p)\,|\,k) \longrightarrow G \longrightarrow 1$$

and we filter the Demuškin group $\tilde{X}_{\mathcal{K}} = Gal(K(p)\,|\,K)$ by its central series

$$\tilde{X}^{o}_{\mathcal{K}} = \tilde{X}_{\mathcal{K}} \quad , \quad \tilde{X}^{i}_{\mathcal{K}} = [\, \tilde{X}^{i-1}_{\mathcal{K}} \, , \, \tilde{X}_{\mathcal{K}}] \, . \, (\tilde{X}^{i-1}_{\mathcal{K}})^{p^s} \; .$$

The field K_i in the above diagram is the fixed field of $\tilde{X}^{i}_{\mathcal{K}}$, i.e. $K_i\,|\,K_{i-1}$ is the maximal abelian extension of exponent p^s . We now obtain the group extensions

$$1 \longrightarrow Gal(K_i\,|\,K) \longrightarrow Gal(K_i\,|\,k) \longrightarrow G \longrightarrow 1 \; .$$

Since $Gal(K(p)\,|\,k) = \varprojlim_i Gal(K_i\,|\,k)$ we are reduced to the question, how to obtain the group $Gal(K_i\,|\,k)$ by using only the axioms. This is achieved in successive steps $i = 1, 2, \ldots$. To mention one surprinsing fact in advance : It suffices to look only at the cases $i = 1, 2$. Once for these cases the group $Gal(K_i\,|\,k)$ is determined by the axioms it is automatically determined for all i .

In the case $i = 1$ we have to characterize the group $G(K_1\,|\,K)$ as a G-module by the axioms and to determine the cocycle of the group extension in $H^2(G, G(K_1\,|\,K))$. Now $G(K_1\,|\,K)$ is dual to $H^1(X_{\mathcal{K}} , \mathbb{Z}/p^s)$ and we have seen in the explanation following the axioms I, II, III that this group is very close to the G-module $H^1(\mathcal{K} , \mathbb{Z}/p^s)^{\perp} / H^1(\mathcal{K} , \mathbb{Z}/p^s) \cong \mathbb{Z}/p^s[G]$. With few additional investigations this gives the G-structure of $G(K_1\,|\,K)$. For the further developments however this is not enough. For example, one has to determine $H^1(X_{\mathcal{K}} , \mathbb{Z}/p^s)$ not only as a G-module but moreover as a symplectic G-module by means of axiom II. Furthermore one has to keep track of that part of $G(K_1\,|\,K)$ which comes from the torsion part of the abelian made group $\tilde{X}^{ab}_{\mathcal{K}} = Gal(K(p)\,|\,K)^{ab}$. This is achieved by means of the so-called Bockstein operator

$$H^1 (X_{\mathcal{K}} , \mathbb{Z}/p^s) \xrightarrow{\;B\;} H^2 (X_{\mathcal{K}} , \mathbb{Z}/p^s) \quad ,$$

the image of which is dual to this torsion part in $G(K_1\,|\,K)$.

Having determined the G-module $G(K_1\,|\,K)$ in sufficient detail by the axioms we have then to determine the cocycle in $H^2(G, G(K_1\,|\,K))$ associated to the group extension

$$1 \longrightarrow G(K_1\,|\,K) \longrightarrow G(K_1\,|\,k) \longrightarrow G \longrightarrow 1$$

in order to describe the group $G(K_1\,|\,k)$. This is done by going over to a p-Sylow group G_p of G, which is cyclic, so that

$$H^2(G_p, G(K_1|K)) = H^2(G_p, K^*/K^{*p^s}) = H^o(G_p, K^*/K^{*p^s}).$$

The cocycle is then represented by a prime element π of k. The selection of this prime element can be group theoretically interpreted by the selection of a section $\lambda : \mathcal{G}^{ab} \to G_k^{ab}$. In this way $G(K_1| k)$ is completely characterized by the axioms.

Much more complicated is the case $i = 2$, i.e., the study of the group extension

$$1 \longrightarrow G(K_2|K) \longrightarrow G(K_2|k) \longrightarrow G \longrightarrow 1$$

and we do not go any further into this, since already the case $i = 1$ has given some indication of the type of necessary investigations.

The cases $i = 1, 2$ have brought us to the following situation. We have the two Koch groups

$$X = G_k \xrightarrow{\Phi} \mathcal{G} , \quad Y \xrightarrow{\Psi} \mathcal{G}$$

and the normal sub groups

$$X_{\mathcal{K}} = \Phi^{-1}(\mathcal{K}) = \mathrm{Gal}(\bar{k}|K) , \quad Y_{\mathcal{K}} = \Psi^{-1}(\mathcal{K}) .$$

Let $X^i_{\mathcal{K}}$ and $Y^i_{\mathcal{K}}$ be the pre-image of $\tilde{X}^i_{\mathcal{K}}$ and $\tilde{Y}^i_{\mathcal{K}}$ under the canonical surjection

$$X_{\mathcal{K}} \to \tilde{X}_{\mathcal{K}} , \quad Y_{\mathcal{K}} \to \tilde{Y}_{\mathcal{K}}$$

where $\tilde{X}^i_{\mathcal{K}}$, $\tilde{Y}^i_{\mathcal{K}}$ is the i-th group in the central series of the Demuškin group $\tilde{X}_{\mathcal{K}}$, $\tilde{Y}_{\mathcal{K}}$. Then

$$X/X^i_{\mathcal{K}} = \mathrm{Gal}(K_i|k) .$$

Since for $i = 1, 2$ we have determined this group completely in terms of the axioms I, II, III, which are satisfied by X as well as by Y, we obtain an isomorphism

$$X/X^i_{\mathcal{K}} \cong Y/Y^i_{\mathcal{K}} \quad \text{for } i = 1, 2 .$$

We want such an isomorphism for all i and we have to show inductively that the surjective homomorphism $Y \to X/X^i_{\mathcal{K}}$ with kernel $Y^i_{\mathcal{K}}$ can be lifted to a surjective homomorphism $Y \to X/X^{i+1}_{\mathcal{K}}$. This leads us to the so-called "imbedding problem" for the group Y, i.e. to the diagram

(1)

$$\begin{array}{ccccccccc} & & & & & & Y & & \\ & & & & & & \downarrow & & \\ 1 & \longrightarrow & X_{\mathcal{K}}^{i}/X_{\mathcal{K}}^{i+1} & \longrightarrow & X/X_{\mathcal{K}}^{i+1} & \longrightarrow & X/X_{\mathcal{K}}^{i} & \longrightarrow & 1 . \end{array}$$

A "solution" of this imbedding problem is a surjection $Y \to X/X_{\mathcal{K}}^{i+1}$ which inserts into the diagram commutatively. We consider also the imbedding problem

(2)

$$\begin{array}{ccccccccc} & & & & & & Y & & \\ & & & & & & \downarrow & & \\ 1 & \longrightarrow & X_{\mathcal{K}}^{i}/X_{\mathcal{K}}^{i+2} & \longrightarrow & X/X_{\mathcal{K}}^{i+2} & \longrightarrow & X/X_{\mathcal{K}}^{i} & \longrightarrow & 1 . \end{array}$$

In turns out that the group $X_{\mathcal{K}}^{i}/X_{\mathcal{K}}^{i+2} = \mathrm{Gal}(K_{i+2} | K_i)$ is abelian for $i \geq 1$ and we have the following

LEMMA. - <u>If</u> $i \geq 1$ <u>then the imbedding problem</u> (2) <u>has a solution iff the imbedding problem</u> (1) <u>has a solution</u>.

If this lemma is shown, we have an isomorphism

$$X/X_{\mathcal{K}}^{i} \cong Y/Y_{\mathcal{K}}^{i}$$

for all i, and the theorem is proved. Namely (1) has a solution for $i = 1$, by what has been shown before. Therefore (2) has a solution for $i = 1$, and hence (1) has a solution for $i = 2$ etc.

For the proof of the lemma we have to consider the diagram

$$\begin{array}{ccc} H^2(X/X_{\mathcal{K}}^{i}, X_{\mathcal{K}}^{i}/X_{\mathcal{K}}^{i+2}) & \xrightarrow{\mathrm{Inf}} & H^2(Y, X_{\mathcal{K}}^{i}/X_{\mathcal{K}}^{i+2}) \\ \downarrow & & \downarrow \\ H^2(X/X_{\mathcal{K}}^{i}, X_{\mathcal{K}}^{i}/X_{\mathcal{K}}^{i+1}) & \xrightarrow{\mathrm{Inf}} & H^2(Y, X_{\mathcal{K}}^{i}/X_{\mathcal{K}}^{i+1}) . \end{array}$$

It is very well known and easy to show that the imbedding problem (1) or (2) has a solution, if the cohomology class associated to the group extension is mapped to zero under Inf . Therefore the lemma would follow immediately if

$$H^2(Y, X_{\mathcal{K}}^{i}/X_{\mathcal{K}}^{i+2}) \longrightarrow H^2(Y, X_{\mathcal{K}}^{i}/X_{\mathcal{K}}^{i+1})$$

were an isomorphism. A closer examination shows, that we can replace here Y by the group $\tilde{Y}_p$ which is the maximal pro-p-factor group of the pre-image Y_p under $Y \to Y/Y_{\mathcal{K}}$ of the p-Sylow group of $Y/Y_{\mathcal{K}}$. This group $\tilde{Y}_p$ is a

Demuškin group and because of the Poincaré duality the requested bijectivity runs up to the bijectivity of

$$H^o(\tilde{Y}_p, \mathrm{Hom}(X^i_{\mathcal{K}}/X^{i+2}_{\mathcal{K}}, \mu_{p^\infty})) \longrightarrow H^o(\tilde{Y}_p, \mathrm{Hom}(X^i_{\mathcal{K}}/X^{i+1}_{\mathcal{K}}, \mu_{p^\infty}))$$

which can be directly checked because of the known structure of $X^i_{\mathcal{K}}/X^{i+2}_{\mathcal{K}}$ and the $\tilde{Y}_p$-action on it. This finally proves the theorem.

Wingberg's actual proof of the uniqueness theorem is more abstract, but it is perfectly modelled after the field theoretical considerations which I have indicated above. The next step is now to construct an abstract Koch group X with the same invariants n, p^s, α as G_k. This is done in the following way.

Let F_{n+1} be the free pro-finite group of $n+1$ generators $z_o, \dots, z_n$ and let $F_{n+1} * \mathcal{G}$ be the free pro-finite product of F_{n+1} with $\mathcal{G} = G(k_{tr}|k)$. We then have an exact sequence

$$1 \to Z \to F_{n+1} * \mathcal{G} \to \mathcal{G} \to 1,$$

where Z is the normal subgroup generated by $z_o, \dots, z_n$. Let P be the maximal pro-p-factor group of Z. The kernel of $Z \to P$ is normal in $F_{n+1} * \mathcal{G}$ and we obtain a commutative diagram

$$\begin{array}{ccccccccc} 1 & \to & Z & \to & F_{n+1} * \mathcal{G} & \to & \mathcal{G} & \to & 1 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 1 & \to & P & \to & F(n+1,\mathcal{G}) & \to & \mathcal{G} & \to & 1 \end{array}$$

where P is the normal subgroup of $F(n+1,\mathcal{G})$ generated by the images $x_o, \dots, x_n$ of $z_o, \dots, z_n$. The group $F(n+1, \mathcal{G})$ is in a sense universal among the split group extensions of $\mathcal{G}$ by a pro-p-group. We now consider the element

$$r = x_o^{-\sigma} (x_o, \tau)^g x_1^{p^s} [x_1, x_2][x_3, x_4] \dots [x_{n-1}, x_n]$$

in $F(n+1, \mathcal{G})$ (for simplicity only in the case of even n). If can be shown that $r \in P$. Denoting by $<r>$ the normal subgroup of $F(n+1, \mathcal{G})$ generated by r and setting $V = P/<r>$, $X = F(n+1, \mathcal{G})/<r>$ we obtain a commutative diagram

$$\begin{array}{ccccccccc} 1 & \to & P & \to & F(n+1,\mathcal{G}) & \to & \mathcal{G} & \to & 1 \\ & & \downarrow & & \downarrow & & \| & & \\ 1 & \to & V & \longrightarrow & X & \longrightarrow & \mathcal{G} & \to & 1. \end{array}$$

THEOREM II. - X <u>is a Koch group over</u> $\mathcal{G}$ <u>of degree</u> n, <u>torsion</u> p^s <u>and character</u> α.

Clearly, theorem I and theorem II together yield an isomorphism

$$G_k \cong X$$

and hence the structure theorem for G_k, since X is constructed in exactly such a way as to satisfy the relations A, B, C in this theorem.

The starting point which finally led to the relation r, was the following basic result of Jannsen. In order to get the structure of G_k one has to study an arbitrary finite normal tamely ramified extension $K|k$ and the action of its galois group G on the galois group of the maximal abelian p-extension of K. Via class field theory this amounts to the determination of the group U^1 of principal units of K as a module over the group ring $\mathbb{Z}_p[G]$. Now U^1 is known to be a cohomologically trivial $\mathbb{Z}_p[G]$-module. Making a complete classification of cohomologically trivial $\mathbb{Z}_p[G]$-modules, Jannsen proved that there always exists an exact sequence

$$0 \longrightarrow \mathbb{Z}_p[G] \xrightarrow{\rho} \mathbb{Z}_p[G]^{n+1} \longrightarrow U^1 \longrightarrow 1 \quad ,$$

so that U^1 has only one defining relation as a $\mathbb{Z}_p[G]$ module, the image of 1 under ρ. Translating this back into the language of galois groups this made clear, that there should be only one essential defining relation for the group G_k. It was then the task to find this relation in such a way, that the axioms I, II, III of a Koch group were satisfied. This try enforced the specific shape of the relation r, and we give now some indications about how the special nature of r implies the properties I, II, III.

The relation r has a leading term $x_o^{-\sigma}(x_o, \tau)^g x_1^{p^s}$ and a commutator term $[x_1, x_2] \dots [x_{n-1}, x_n]$. The leading term is responsible for all assertions not involving the cupproduct and the commutator term for axiom I, which conerns the Demuškin structure. We consider again the diagram

$$\begin{array}{ccccccccc} 1 & \to & P & \to & F(n+1, \mathcal{G}) & \to & \mathcal{G} & \to & 1 \\ & & \downarrow & & \downarrow & & \| & & \\ 1 & \to & V & \longrightarrow & X & \longrightarrow & \mathcal{G} & \to & 1 \end{array} .$$

The abelian made group $V^{ab} = P^{ab}/\langle \mathrm{im}\ r \rangle$ is a module over the completed group ring $\mathbb{Z}_p[[\mathcal{G}]]$, and P^{ab} is a free $\mathbb{Z}_p[[\mathcal{G}]]$-module generated by the images $\bar{x}_i$ of $x_o, \dots, x_n$. Going over from $r \in P$ to the image of r in P^{ab} the commutators vanish and we obtain

$$r \equiv x_o^{-\sigma}(x_o^{h^{p-1}} \tau x_o^{h^{p-2}} \tau \dots x_o^h \tau)^{\frac{g\pi}{p-1}} x_1^{p^s} \equiv x_o^{-\sigma} x_o^{g\lambda} x_1^{p^s} \mod [P,P] ,$$

where λ is a certain element in $\mathbb{Z}_p[[\mathcal{G}]]$, and thus

$$V^{ab} \cong \bigoplus_{i=0}^{n} \mathbb{Z}_p[[\mathcal{G}]]\, \bar{x}_i / (\mathbb{Z}_p[[\mathcal{G}]]\,((\sigma - g\lambda)\, \bar{x}_o - p^s \bar{x}_1)) .$$

Taking everything mod p^s one finds that λ has the type of an idempotent $\sum_{i=0}^{\infty} h^{-i}\tau^i$, showing that (mod p^s) σ acts on $\bar{x}_o$ as multiplication by g and τ as multiplication by h. This gives the $\mathcal{G}$-isomorphism

$$V^{ab} \otimes \mathbb{Z}/p^s \cong \mu_{p^s} \oplus \bigoplus_{i=1}^{n} \mathbb{Z}/p^s[[\mathcal{G}]]\,\bar{x}_i .$$

Taking now an open subgroup $\mathcal{H} \subseteq \ker(\alpha)$ of $\mathcal{G}$ one proves the exactness of the sequence

$$H^1(X_{\mathcal{H}}, \mathbb{Q}_p/\mathbb{Z}_p) \xrightarrow{p^i} H^1(X_{\mathcal{H}}, \mathbb{Q}_p/\mathbb{Z}_p) \longrightarrow H^2(X_{\mathcal{H}}, \mathbb{Z}/p^i\mathbb{Z}) \longrightarrow 0$$

and taking Pontrjagin duals this yields the commutative exact diagram

$$\begin{array}{ccccccc} 0 & \to & H^2(X_{\mathcal{H}}, \mathbb{Z}/p^i\mathbb{Z})^* & \longrightarrow & \tilde{X}_{\mathcal{H}}^{ab} & \longrightarrow & \tilde{X}_{\mathcal{H}}^{ab} \\ & & \| \wr & & \uparrow & & \uparrow \\ 0 & \longrightarrow & \mu_{p^i} & \longrightarrow & V/[V, X_{\mathcal{H}}] & \to & V/[V, X_{\mathcal{H}}] \end{array}$$

for every $i \leq s$. This proves $\dim H^2(X_{\mathcal{H}}, \mathbb{F}_p) = 1$ and $(\tilde{X}_{\mathcal{H}})_{tor} \cong \mu_{p^s}$.

The space $H^1(X_{\mathcal{H}}, \mathbb{F}_p)$ is dual to $\tilde{X}_{\mathcal{H}}^{ab} \otimes \mathbb{Z}/p$ which as a G-module is generated by $\sigma, \bar{x}_o, \bar{x}_1, \dots, \bar{x}_n$ by the above consideration. If $\chi_\sigma, \chi_o, \dots, \chi_n$ is the dual $\mathbb{F}_p[G]$-basis of $H^1(X_{\mathcal{H}}, \mathbb{F}_p)$, then this space has the $\mathbb{F}_p$-basis $\chi_\sigma, \chi_o, \rho\chi_i, \rho \in G, i = 1, \dots, n$. This shows $\dim H^1(X_{\mathcal{H}}, \mathbb{F}_p) = n.\# G+2$.

The assertions concerning the cupproduct rely on the following general

LEMMA. - <u>Let</u> D <u>be a pro-p-group generated by</u> $y_1, \dots, y_m$, <u>such that</u> $H^2(D, \mathbb{F}_p) \cong \mathbb{F}_p$. <u>Let</u> $D^o = D$, $D^{i+1} = [D^i, D].(D^i)^p$ <u>be the central series and assume that there holds a relation</u>

$$\prod_i y_i^{a_i p} \cdot \prod_{i<y} [y_i, y_j]^{a_{ij}} \equiv 1 \mod D^2$$

<u>such that not all</u> a_i <u>and not all</u> a_{ij} <u>are</u> $\equiv 0 \mod p$.

If $\chi_1, \ldots, \chi_m$ is the dual basis of $H^1(D, \mathbb{F}_p)$ associated to $y_1, \ldots, y_m$ then

$$\chi_i \cup \chi_j = a_{ij}\, \xi \ , \quad i<j \ ,$$

where ξ is a generator of $H^2(D, \mathbb{F}_p)$.

Writing now the image of the relation r in the Demuškin group $\tilde{X}_{\mathcal{K}}$ mod $\tilde{X}_{\mathcal{K}}^2$ in the form ot the lemma, one gets an explicit description of the cup product

$$H^1(\tilde{X}_{\mathcal{K}}, \mathbb{F}_p) \times H^1(\tilde{X}_{\mathcal{K}}, \mathbb{F}_p) \longrightarrow H^2(\tilde{X}_{\mathcal{K}}, \mathbb{F}_p)$$

from which one draws all the required properties concerning the cupproduct. This concludes the proof of theorem II.

-:-:-:-

LITERATURE

[1] K. IWASAWA, On Galois groups of local fields, Trans. Am. Math. Soc. 80 (1955), 448-469.

[2] A. V. JAKOVLEV, The Galois group of the algebraic closure of a local field, Math. USSR-Izv. 2 (1968), 1231-1269.

[3] A. V. JAKOVLEV, Remarks on my paper "The Galois groups of the algebraic closure of a local field", Math. USSR-Izv. 12 (1978), 205-206.

[4] A. V. JAKOLEV, Structure of the multiplicative group of a simply ramified extension of a local field of odd degree, Math. USSR Sbornik 35 (1979), 581-591.

[5] U. JANNSEN, Über Galoisgruppen lokaler Körper, to appear.

[6] U. JANNSEN,and K. WINGBERG, Die Struktur der absoluten Galoisgruppen $\mathfrak{p}$-adischer Zahlkörper, to appear.

[7] H. KOCH, Über Galoissche Gruppen von $\mathfrak{p}$-adischen Zahlkörpern, Math. Nachr. 29 (1965), 77-111.

[8] H. KOCH, Galoissche Theorie der p-Erweiterungen, Berlin 1970.

[9] H. KOCH, The Galois group of a p-closed extension of a local field, Soviet Math. Dokl. 19 (1978), 10-13.

[10] K. WINGBERG, Der Eindeutigkeitssatz für Demuskinformationen. To appear.

-:-:-:-

Jürgen NEUKIRCH
Mathematisches Institut
der Universität
8400 REGENSBURG
(Allemagne de l'Ouest)