JÜRGEN NEUKIRCH

The absolute Galois group of a $p$-adic number field


<http://www.numdam.org/item?id=AST_1982__94__153_0>
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 $p$-adic number field $k$ ([5], [6], [10]). This description depends upon four invariants $q$, $n$, $p^s$, $a$ of $k$ which are defined as follows.

Let $\overline{k}$ and $k_{tr}$ be the algebraic closure and the maximal tamely ramified extension of $k$ respectively. As is well known the galois group $\mathbb{Q} = G(k_{tr}|k)$ is generated by two elements $\sigma, \tau$ satisfying the relation $\sigma \tau \sigma^{-1} = \tau^q$. We put

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

$$q = \text{cardinality of the residue class field of } k,$$

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

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

$\alpha$ 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 $G_k = G(k|k)$ is isomorphic to the pro-finite group of $n+3$ generators $\sigma, \tau, x_0, \ldots, x_n$ and the following defining relations.

A. - The normal subgroup generated by $x_0, \ldots, x_n$ is a pro-$p$-group.

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

C. - There is only one additional relation, namely

$$\sigma x_0 \sigma^{-1} = (x_0, \tau)^{g} x_1^p [x_1, x_2] [x_3, x_4] \ldots [x_{n-1}, x_n]$$

if $n$ is even, and

$$\sigma x_0 \sigma^{-1} = (x_0, \tau)^{g} x_1^p [x_1, y] [x_2, x_3] \ldots [x_{n-1}, x_n]$$

if $n$ is odd. Here we have put

$$(x_0, \tau) = (x_0^p, \tau x_0^p \tau \ldots x_0^p \tau)^{p-1},$$

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

Remarks. - The condition A can easily be replaced by a collection of relations and expresses together with B the self-understanding 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 $k|k$ is replaced by the maximal extension of $k(\mu_p)$ of odd ramification, then we can take $y = x_1^r$.

The proof of the theorem is based on the following method. For each finite normal subextension $K|k$ of $k_{tr}$ 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 $\mathbb{Q}$.

Each such Koch group is endowed with invariants $q, n, p^s, \alpha$.

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...
THE ABSOLUTE GALOIS GROUP OF A p-ADIC NUMBER FIELD

group, defined by the generators and relations given in the theorem, is a Koch group with the same invariants as the Koch group $G_k$ and is thus isomorphic to $G_k$.

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

Here $K$ is an open normal subgroup of $G = G(ktr|k)$ contained in the kernel of $\alpha$, so that $\mu_p$ is contained in the fixed field $K$ of $K$. $G = G/K = G(K/k)$, $X^*_k = G(k|K)$ and $X^*_k$ is the galois group of the maximal $p$-extension $K(p)|K$.

It is the maximal pro-$p$-factor group of $X^*_k$ and is a Demuškin group. For these groups we have the following known properties.

I. - $\dim H^1(X^*_k, \mathbb{F}_p) = n \neq G + 2$, $\dim H^2(X^*_k, \mathbb{F}_p) = 1$ and $H^1(X^*_k, \mathbb{F}_p) \otimes H^1(X^*_k, \mathbb{F}_p) \cong \mathbb{F}_p[G]^n$ is a non degenerate anti-symmetric bilinear form.

II. - Viewing $H^1(K, \mathbb{F}_p)$ as a 1-dimensional subspace of the symplectic space $H^1(X^*_k, \mathbb{F}_p)$ we have an isomorphism of $G$-modules $H^1(K, \mathbb{F}_p) \cong \mathbb{F}_p[G]^n$.

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. - $(X^*_{k})^{ab}_{tor} \cong \mu_p$ as a $G$-module.

Explanation. - Condition I expresses the well known fact that $\tilde{X}^*_k = \text{Gal}(K(p)|K)$ is a Demuškin group. By class field theory $H^1(X^*_k, \mathbb{F}_p)$ is dual to $K^*/K^*_p = (\pi)/(\pi^p) \times U^1/(U^1)^p$ where $\pi$ 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 $H^1(K, \mathbb{F}_p) \cong \mathbb{F}_p[G]^n$ 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 $\mathbb{Q}$ be any profinite group generated by two elements $\sigma, \tau$ such that $\sigma \tau \sigma^{-1} = \sigma^q$ and let $\alpha : \mathbb{Q} \to (\mathbb{Z}/p^s)^*$ be a character.

**DEFINITION.** - A Koch group over $\mathbb{Q}$ (Demuškin formation in Jannsen's and Wingberg's terminology) of degree $n$, of torsion $p^s$ and character $\alpha$, is a profinite group $X$ together with a surjective homomorphism

$$\phi : X \to \mathbb{Q}$$

such that for each open normal subgroup $\mathcal{K}$ of $\mathbb{Q}$ in the kernel of $\alpha$, the conditions I, II, III hold for $X_{\mathcal{K}} = \phi^{-1}(\mathcal{K})$, where in III $\mathbb{Z}/p^s$ is replaced by the twisted $\mathbb{Q}$-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 $\mathbb{Q}$ with the same invariants $n, p^s$ and $\alpha$ 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

$$
\begin{array}{c}
X_{\mathcal{K}} \\
\downarrow \\
G_k \\
\downarrow \\
K_{tr} \\
\downarrow \\
K(p) \\
\end{array}
$$

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

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

\[
1 \to \text{Gal}(K(p) \mid K) \to \text{Gal}(K(p) \mid k) \to G \to 1
\]

and we filter the Demuškin group \( \widetilde{X}_K = \text{Gal}(K(p) \mid K) \) by its central series

\[
\tilde{X}_K^0 = \tilde{X}_K, \quad \tilde{X}_K^i = [\tilde{X}_K^{i-1}, \tilde{X}_K], (\tilde{X}_K^{i-1})^{p^i}.
\]

The field \( K_i \) in the above diagram is the fixed field of \( \tilde{X}_K^i \), i.e. \( K_i \mid K_{i-1} \) is the maximal abelian extension of exponent \( p^i \). We now obtain the group extensions

\[
1 \to \text{Gal}(K_i \mid K) \to \text{Gal}(K_i \mid k) \to G \to 1.
\]

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

In the case \( i = 1 \) we have to characterize the group \( \text{Gal}(K_1 \mid K) \) as a \( G \)-module by the axioms and to determine the cocycle of the group extension in

\[
H^2(G, \text{Gal}(K_1 \mid K)).
\]

Now \( \text{Gal}(K_1 \mid K) \) is dual to \( H^1(X_K, \mathbb{Z}/p^s) \) and we have seen in the explanation following the axioms I, II, III that this group is very close to the \( G \)-module \( H^1(K, \mathbb{Z}/p^s) \). With few additional investigations this gives the \( G \)-structure of \( \text{Gal}(K_1 \mid K) \). For the further developments however this is not enough. For example, one has to determine \( H^1(X_K, \mathbb{Z}/p^s) \) 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 \( \text{Gal}(K_1 \mid K) \) which comes from the torsion part of the abelian made group \( \tilde{X}_K^{ab} = \text{Gal}(K(p)\mid K)^{ab} \). This is achieved by means of the so-called Bockstein operator

\[
H^1(X_K, \mathbb{Z}/p^s) \xrightarrow{B} H^2(X_K, \mathbb{Z}/p^s),
\]

the image of which is dual to this torsion part in \( \text{Gal}(K_1 \mid K) \).

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

\[
1 \to \text{Gal}(K_1 \mid K) \to \text{Gal}(K_1 \mid k) \to G \to 1
\]

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

$$H^2(G_p, G(K_1|K)) = H^2(G_p, K^*/K^{*p}) = H^0(G_p, K^*/K^{*p}).$$

The cocycle is then represented by a prime element $\pi$ of $k$. The selection of this prime element can be group theoretically interpreted by the selection of a section $\lambda : Q^{ab} \to G^{ab}_k$. 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

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

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

$$X = G_k, \quad Y = G_k$$

and the normal subgroups

$$X^i_{\mathcal{X}} = G_k = \text{Gal}(k|K), \quad Y^i_{\mathcal{Y}} = G_k.$$  

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

$$X^i_{\mathcal{X}} \to \tilde{X}^i_{\mathcal{X}}, \quad Y^i_{\mathcal{Y}} \to \tilde{Y}^i_{\mathcal{Y}}$$

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

$$X/X^i_{\mathcal{X}} = \text{Gal}(K_1|k).$$

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

$$X/X^i_{\mathcal{X}} \cong Y/Y^i_{\mathcal{Y}}$$

for $i=1,2$.

We want such an isomorphism for all $i$ and we have to show inductively that the surjective homomorphism $Y \to X/X^i_{\mathcal{X}}$ with kernel $Y^i_{\mathcal{Y}}$ can be lifted to a surjective homomorphism $Y \to X/X^{i+1}_{\mathcal{X}}$. This leads us to the so-called "imbedding problem" for the group $Y$, i.e. to the diagram
A "solution" of this imbedding problem is a surjection $Y \to X/X_{\mathcal{C}}^{i+1}$ which inserts into the diagram commutatively. We consider also the imbedding problem

$$1 \to X_{\mathcal{C}}^{i}/X_{\mathcal{C}}^{i+1} \to X/X_{\mathcal{C}}^{i+1} \to X/X_{\mathcal{C}}^{i} \to 1.$$ 

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

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

If this lemma is shown, we have an isomorphism

$$X/X_{\mathcal{C}}^{i} \simeq Y/Y_{\mathcal{C}}^{i},$$

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

$$H^{2}(X/X_{\mathcal{C}}^{i}, X_{\mathcal{C}}^{i}/X_{\mathcal{C}}^{i+2}) \to H^{2}(Y, X_{\mathcal{C}}^{i}/X_{\mathcal{C}}^{i+2}) \to H^{2}(Y, X_{\mathcal{C}}^{i+1}/X_{\mathcal{C}}^{i+1}).$$

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 $\text{Inf}$. Therefore the lemma would follow immediately if

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

were an isomorphism. A closer examination shows, that we can replace here $Y$ by the group $\widetilde{Y}_{p}$ which is the maximal pro-$p$-factor group of the pre-image $Y_{p}$ under $Y \to Y/Y_{\mathcal{C}}$ of the p-Sylow group of $Y/Y_{\mathcal{C}}$. This group $\widetilde{Y}_{p}$ is a
Demushkin group and because of the Poincaré duality the requested bijectivity runs up to the bijectivity of

\[ H^0(\tilde{Y}_p, \text{Hom}(X_n^i / X_{n+2}^i, \mu)) \rightarrow H^0(\tilde{Y}_p, \text{Hom}(X_n^i / X_{n+2}^i, \mu)) \]

which can be directly checked because of the known structure of \( X_n^i / X_{n+2}^i \) 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 \( n, p, \alpha \) as \( G_k \). This is done in the following way.

Let \( F_{n+1} \) be the free pro-finite group of \( n+1 \) generators \( z_0, \ldots, z_n \) and let \( F_{n+1} \ast Q \) be the free pro-finite product of \( F_{n+1} \) with \( Q = G(k_{tr}|k) \). We then have an exact sequence

\[ 1 \rightarrow Z \rightarrow F_{n+1} \ast Q \rightarrow Q \rightarrow 1, \]

where \( Z \) is the normal subgroup generated by \( z_0, \ldots, z_n \). Let \( P \) be the maximal pro-p-factor group of \( Z \). The kernel of \( Z \rightarrow P \) is normal in \( F_{n+1} \ast Q \) and we obtain a commutative diagram

\[
\begin{array}{c}
1 \rightarrow Z \rightarrow F_{n+1} \ast Q \rightarrow Q \rightarrow 1 \\
\downarrow \quad \downarrow \quad \downarrow \\
1 \rightarrow P \rightarrow F(n+1, Q) \rightarrow Q \rightarrow 1
\end{array}
\]

where \( P \) is the normal subgroup of \( F(n+1, Q) \) generated by the images \( x_0, \ldots, x_n \) of \( z_0, \ldots, z_n \). The group \( F(n+1, Q) \) is in a sense universal among the split group extensions of \( Q \) by a pro-p-group. We now consider the element

\[ r = x_0^{-\sigma} (x_0, \tau)^p x_1^p [x_1, x_2] [x_3, x_4] \ldots [x_{n-1}, x_n] \]

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

\[
\begin{array}{c}
1 \rightarrow P \rightarrow F(n+1, Q) \rightarrow Q \rightarrow 1 \\
\downarrow \quad \downarrow \quad \downarrow \\
1 \rightarrow V \rightarrow X \rightarrow Q \rightarrow 1
\end{array}
\]

THEOREM II. - \( X \) is a Koch group over \( Q \) of degree \( n \), torsion \( p \) and character \( \alpha \).
Clearly, theorem I and theorem II together yield an isomorphism

\[ G_k \cong \mathbb{X} \]

and hence the structure theorem for \( G_k \), since \( \mathbb{X} \) 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

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

so that \( U^1 \) has only one defining relation as a \( \mathbb{Z}_p[G] \) module, the image of \( 1 \) under \( \rho \). 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 \( x_o^{-c}(x_o, \tau)^g x_1^p \) and a commutator term \( [x_1, x_2] \ldots [x_{n-1}, x_n] \). The leading term is responsible for all assertions not involving the cupproduct and the commutator term for axiom I, which concerns the Demuškin structure. We consider again the diagram

\[ 1 \rightarrow P \rightarrow F(n+1, \mathbb{Q}) \rightarrow Q \rightarrow 1 \]

\[ 1 \rightarrow V \rightarrow X \rightarrow Q \rightarrow 1. \]

The abelian made group \( V^{ab} = P^{ab}/\text{im } r \) is a module over the completed group ring \( \mathbb{Z}_p[[Q]] \), and \( P^{ab} \) is a free \( \mathbb{Z}_p[[Q]] \)-module generated by the images \( \overline{x_i} \) of \( x_o, \ldots, x_n \). Going over from \( r \in P \) to the image of \( r \) in \( P^{ab} \) the commutators vanish and we obtain
\[ r = x^{-\sigma} (x_o h_p^{-1} x_o h_p^{-2} \cdots x_o h_p^{-s} x\lambda x_1^s \mod [P, P]), \]

where \( \lambda \) is a certain element in \( \mathbb{Z}_p[[Q]] \), and thus

\[ \mathbb{V}^{ab} \cong \bigoplus_{i=0}^{n} \mathbb{Z}_p[[Q]] x_i / (\mathbb{Z}_p[[Q]] ((x - g \lambda x_o - p s x_1^s)) \).

Taking everything mod \( p^s \) one finds that \( \lambda \) has the type of an idempotent \( \sum h^i x_i \), showing that \( (\mod p^s) \sigma \) acts on \( x_i \) as multiplication by \( g \) and \( v \) as multiplication by \( h \). This gives the \( \mathbb{Q} \)-isomorphism

\[ \mathbb{V}^{ab} \otimes \mathbb{Z}/p^s \cong \bigoplus_{i=1}^{n} \mathbb{Z}/p[[Q]] x_i. \]

Taking now an open subgroup \( K \subseteq \ker(\alpha) \) of \( \mathbb{Q} \) one proves the exactness of the sequence

\[ H^1(X_\mathbb{Q}, \mathbb{Q}_p/\mathbb{Z}) \xrightarrow{\mu} H^1(X_\mathbb{Q}, \mathbb{Q}_p/\mathbb{Z}_p) \to H^2(X_\mathbb{Q}, \mathbb{Z}/p^i \mathbb{Z}) \to 0 \]

and taking Pontrjagin duals this yields the commutative exact diagram

\[ 0 \to H^2(X_\mathbb{Q}, \mathbb{Z}/p^i \mathbb{Z})^* \xrightarrow{\mu} \mathbb{X}^{ab}_\mathbb{Q} \xrightarrow{\iota} \mathbb{X}^{ab}_\mathbb{Q} \to \mathbb{V}/[\mathbb{V}, X_\mathbb{Q}] \to V/[V, X_\mathbb{Q}] \]

for every \( i \leq s \). This proves \( \dim H^2(X_\mathbb{Q}, \mathbb{F}_p) = 1 \) and \( (X_\mathbb{Q})^{tor} \cong \mu_p^s \).

The space \( H^1(X_\mathbb{Q}, \mathbb{F}_p) \) is dual to \( \mathbb{X}^{ab}_\mathbb{Q} \otimes \mathbb{Z}/p \) which as a \( \mathbb{G} \)-module is generated by \( \sigma, x_o, x_1, \ldots, x_n \) by the above consideration. If \( \chi_0, \chi_1, \ldots, \chi_n \) is the dual \( \mathbb{F}_p[G] \)-basis of \( H^1(X_\mathbb{Q}, \mathbb{F}_p) \), then this space has the \( \mathbb{F}_p \)-basis \( \chi_\sigma \cdot x_o, \rho \chi_i, \rho \in \mathbb{G}, i = 1, \ldots, n \). This shows \( \dim H^1(X_\mathbb{Q}, \mathbb{F}_p) = n \neq G + 2 \).

The assertions concerning the cupproduct rely on the following general

**Lemma. -** Let \( D \) be a pro-p-group generated by \( y_1, \ldots, y_m \), such that \( H^2(D, \mathbb{F}_p) \cong \mathbb{F}_p \). Let \( D^0 = D, D^{i+1} = [D^i, D], (D^i)^p \) be the central series and assume that there holds a relation

\[ \prod_{i} a_{i}^{p} y_i \cdot \prod_{i < j} [y_i, y_j]^{a_{ij}} = 1 \mod D^2 \]

such that not all \( a_i \) and not all \( a_{ij} \) are \( 0 \mod p \).
THE ABSOLUTE GALOIS GROUP OF A p-ADIC NUMBER FIELD

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

Writing now the image of the relation \( r \) in the Demuškin group \( \tilde{X}_\chi \mod \tilde{X}_\chi^2 \) in the form ot the lemma, one gets an explicit description of the cup product
\[
H^1(\tilde{X}_\chi, \mathbb{F}_p) \times H^1(\tilde{X}_\chi, \mathbb{F}_p) \rightarrow H^2(\tilde{X}_\chi, \mathbb{F}_p)
\]
from which one draws all the required properties concerning the cup product.
This concludes the proof of theorem II.

LITERATURE


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