# ON THE STRUCTURE OF GALOIS GROUPS AS GALOIS MODULES

Uwe Jannsen

Fakultät für Mathematik
Universitätsstr. 31, 8400 Regensburg
Bundesrepublik Deutschland

Classical class field theory tells us about the structure of the Galois groups of the abelian extensions of a global or local field. One obvious next step is to take a Galois extension K/k with Galois group G (to be thought of as given and known) and then to investigate the structure of the Galois groups of abelian extensions of K as G-modules. This has been done by several authors, mainly for tame extensions or p-extensions of local fields (see [10],[12],[3] and [13] for example and further literature) and for some infinite extensions of global fields, where the group algebra has some nice structure (Iwasawa theory). The aim of these notes is to show that one can get some results for arbitrary Galois groups by using the purely algebraic concept of class formations introduced by Tate.

## 1. Relation modules.

Given a presentation

$$1 \to R_m \to F_m \to G \to 1$$

of a finite group G by a (discrete) free group $F_m$ on m free generators, the factor commutator group $R_m^{ab} = R_m/[R_m,R_m]$ becomes a finitely generated $\mathbb{Z}[G]$-module via the conjugation in $F_m$. By Lyndon [19] and Gruenberg [8]§2 we have

**1.1. PROPOSITION.** a) *There is an exact sequence of* $\mathbb{Z}[G]$*-modules*

$$(1) \qquad 0 \to R_m^{ab} \to \mathbb{Z}[G]^m \to I(G) \to 0 \quad ,$$

*where* I(G) *is the augmentation ideal, defined by the exact sequence*

$$(2) \qquad 0 \to I(G) \to \mathbb{Z}[G] \xrightarrow{aug} \mathbb{Z} \to 0, \qquad aug(\sum_{\sigma\in G} a_\sigma\sigma) = \sum_{\sigma\in G} a_\sigma.$$

b) $\mathbb{Q} \otimes_{\mathbb{Z}} R_m^{ab} \cong \mathbb{Q}[G]^{m-1} \oplus \mathbb{Q}$ *as* $\mathbb{Q}[G]$*-module.*

c) *For a second presentation* $1 \to R_n \to F_n \to G \to 1$ *one has*

$$R_n^{ab} \oplus \mathbb{Z}[G]^m \cong R_m^{ab} \oplus \mathbb{Z}[G]^n$$

*and therefore*

$$R_{n,p}^{ab} \cong R_{m,p}^{ab} \oplus \mathbb{Z}_p[G]^{n-m} \qquad (n \geq m), \tag{3}$$

*for every prime* p, *if we set* $R_{m,p}^{ab} = \mathbb{Z}_p \otimes_{\mathbb{Z}} R_m^{ab}$ ($\mathbb{Z}_p$ *the ring of integers in the field* $\mathbb{Q}_p$ *of* p*-adic numbers).*

In particular the G-structure of $R_{m,p}^{ab}$ only depends on m; for $R_m^{ab}$ itself and minimal m this is still an open problem, see [8]. One has $R_m^{ab} \cong I(G) \otimes_{\mathbb{Z}} I(G)$ for $m = (G:1)-1$, and $R_m^{ab} \cong \mathbb{Z}[G]^{m-1} \oplus \mathbb{Z}$ for cyclic G ($\mathbb{Z}, \mathbb{Q}, \mathbb{Z}_p$ and $\mathbb{Q}_p$ are always equipped with the trivial G-action). If G is a p-group, $R_{m,p}^{ab}$ is just the factor commutator group of $\hat{R}_m$ in any presentation $1 \to \hat{R}_m \to \hat{F}_m \to G \to 1$ of G by a free pro-p-group on m free generators. If the order of G is prime to p, one has $R_{m,p}^{ab} \cong \mathbb{Z}_p[G]^{m-1} \oplus \mathbb{Z}_p$.

Tate has shown (see [16]) that $R_m^{ab}$ is a class formation module for G, i.e.,

$$H^i(U, R_m^{ab}) \cong H^{i-2}(U, \mathbb{Z}) \tag{4}$$

for all subgroups U of G and all $i \in \mathbb{Z}$ (here and in the following we take the modified (Tate) cohomology groups), where the isomorphism is obtained by taking cupproduct with the restriction of a generating element of $H^2(G, R_m^{ab}) \cong \mathbb{Z}/(G:1)\mathbb{Z}$. It turns out that $R_m^{ab}$ has to be regarded as a standard object with this property - all other class formation modules only differing by "projective kernels":

<u>1.2. THEOREM</u>. *Let* G *be a finite group,* $G_p$ *a* p*-Sylow subgroup and* M *a finitely generated* $\mathbb{Z}_p[G]$*-module with the property*

$$(*) \qquad \begin{aligned} H^1(G_p, M) &= 0 \\ H^2(G_p, M) &\cong \mathbb{Z}_p/(G_p: 1)\mathbb{Z}_p \\ H^2(G, M) &\cong \mathbb{Z}_p/(G: 1)\mathbb{Z}_p. \end{aligned}$$

a) *There is an exact sequence*

$$0 \to X \to R_{m,p}^{ab} \to M \to 0 \tag{5}$$

*for some* $m \in \mathbb{N}$ *and some projective* $\mathbb{Z}_p[G]$*-module* X.

b) *If* $M$ *is torsion free (as* $\mathbb{Z}_p$*-module), the sequence (5) splits, so*

$$M \oplus X \cong R^{ab}_{m,p}$$

c) *There is an exact sequence*

$$(6) \qquad 0 \to M \to M' \to I_p(G) \to 0$$

*with a cohomologically trivial* $\mathbb{Z}_p[G]$*-module* $M'$ *and* $I_p(G) = \mathbb{Z}_p \otimes I(G)$.

<u>Proof</u>. The proof of a) is nearly as in [13]I: Let

$$0 \to M \to E \to G \to 1$$

be the group extension corresponding to a generating element of $H^2(G,M)$, and choose a homomorphism $\varphi: F_m \to E$ with dense image ($m$ suitable). This induces a surjection $\bar{\varphi}: R^{ab}_{m,p} \to M$, let $X = \ker \bar{\varphi}$. From the long exact sequence of cohomology under $G_p$ we get $H^2(G_p,X) = 0 = H^3(G_p,X)$, so $X$ is cohomologically trivial, i.e., projective, as $X$ is torsion free.

b) is clear (compare [13] 1.5), and $M'$ is defined by the exact commutative diagram

$$\begin{tikzcd}
 & & I_p(G) \arrow[r, equal] & I_p(G) & \\
0 \arrow[r] & X \arrow[r] & \mathbb{Z}_p[G]^m \arrow[r] \arrow[u, two heads] & M' \arrow[r] \arrow[u, two heads] & 0 \\
0 \arrow[r] & X \arrow[r] \arrow[u, equal] & R^{ab}_{m,p} \arrow[r] \arrow[u] & M \arrow[r] \arrow[u] & 0,
\end{tikzcd}$$

where the middle column is given by 1.1.a).

## 2. Cohomologically trivial $\mathbb{Z}_p[G]$-modules.

We fix the following notations. For a finitely generated $\mathbb{Z}_p[G]$-module $M$, $\mathrm{Tor}(M)$ will denote the $\mathbb{Z}_p$-torsion submodule of $M$, $M^* = \mathrm{Hom}(M,\mathbb{Q}_p/\mathbb{Z}_p)$ is the Pontrjagin dual of $M$ (with the operation $(\sigma f)(m) = f(\sigma^{-1}m))$, and $d_G(M)$ is the minimal number of $\mathbb{Z}_p[G]$-generators for $M$. Tensor products now are taken over $\mathbb{Z}_p$, if not denoted otherwise. For a pro-finite group $A$ (abelian or not) $A(p)$ is the maximal pro-$p$-quotient.

A $\mathbb{Z}_p[G]$-module $P$ is projective iff it is torsion free and cohomologically trivial, and then determined by the structure of $\mathbb{Q}_p \otimes P$ as $\mathbb{Q}_p[G]$-module by a theorem of Swan [23] 6.4. This generalizes to

2.1. THEOREM ([12] 1.2.). *For cohomologically trivial, finitely generated* $\mathbb{Z}_p[G]$*-modules* $M$ *and* $M'$ *the following statements are equivalent:*

i) $M \cong M'$.

ii) $\mathrm{Tor}(M) \cong \mathrm{Tor}(M')$ *and* $\mathbb{Q}_p \otimes M \cong \mathbb{Q}_p \otimes M'$.

Furthermore we have the following construction, which follows from [12] 1.8-1.10.

2.2. LEMMA. *Let* $N$ *be a finite* $\mathbb{Z}_p[G]$*-module.*

*a) There is a presentation (exact sequence)*

$$\mathbb{Z}_p[G]^{\ell} \xrightarrow{f} \mathbb{Z}_p[G]^m \longrightarrow N^* \longrightarrow 0$$

*if and only if there is an exact sequence*

$$0 \to \mathbb{Z}_p[G]^m \xrightarrow{f^+} \mathbb{Z}_p[G]^{\ell} \to M \to 0$$

*for the cohomologically trivial* $\mathbb{Z}_p[G]$*-module* $M$ *with* $\mathrm{Tor}(M) \cong N$ *and* $\mathbb{Q}_p \otimes M \cong \mathbb{Q}_p[G]^{\ell-m}$.

b) *In the above statement,* $f^+$ *can be chosen to be the transpose of* $f$ *in the following sense: If* $f$ *is given by the matrix* $(\alpha_{ij})$ *with* $\alpha_{ij} \in \mathbb{Z}_p[G]$, $f^+$ *is then given by the matrix* $(\alpha_{ji}^+)$, *where* $^+$ *is the anti-involution of* $\mathbb{Z}_p[G]$ *given by*

$$\Big(\sum_{\sigma\in G} a_\sigma \sigma\Big)^+ = \sum_{\sigma\in G} a_\sigma \sigma^{-1} .$$

## 3. Applications to number fields.

Let $K/k$ be a finite Galois extension of local or global number fields with Galois group $G$ (function fields can be treated similarly). Fix a prime $p$ and let $\overline{K}$ be

i) the maximal p-extension of $K$, if $k$ is local,

ii) the maximal p-extension of $K$ unramified outside $S$, if $k$ is global; here $S$ is a finite set of non-archimedean primes of $K$ closed under the action of $G$ and containing all primes above $p$ and all primes ramified in $K/k$.

For every field $k \subseteq L \subseteq K$ we set $G_L = \mathrm{Gal}(\overline{K}/L)$, and we want to consider the finitely generated $\mathbb{Z}_p[G]$-module $G_K^{ab}$.

Notations: for any field $L$, $\mu_L$ is the group of roots of unity in $L$, and $\mu_n = \{\zeta \in \mu_\Omega | \zeta^n = 1\}$ for an algebraic closure $\Omega$ of $L$.

i) For local fields the only interesting case is where p equals the residue characteristic. The following theorem generalizes the results for p-groups due to Borevič, K. Wingberg and the author (see [2],[3], [13] and [25]):

<u>3.1. THEOREM</u>. *Let* $k$ *be of degree* $n$ *over* $\mathbb{Q}_p$.

a) $G$ *is generated by* $n+2$ *elements, and there is an exact sequence*

$$(7) \qquad 0 \to \mathbb{Z}_p[G] \to R^{ab}_{n+2,p} \to G^{ab}_K \to 0 .$$

b) *If* $K$ *is regular* (i.e., $\mu_p \not\subseteq K$), $G$ *is generated by* $n+1$ *elements, and there is an isomorphism*

$$(8) \qquad G^{ab}_K \cong R^{ab}_{n+1,p} .$$

<u>Proof</u>. We only show a), because b) is similar, using the splitting of (7). As the reciprocity map induces an isomorphism between $G^{ab}_K$ and the projective limit over the groups $K^x/K^{xp^n}$ for all n, $G^{ab}_K$ has the property (*), and using the p-adic logarithm we get an isomorphism

$$(9) \qquad \mathbb{Q}_p \otimes G^{ab}_K \cong \mathbb{Q}_p[G]^n \oplus \mathbb{Q}_p .$$

Let $R$ be defined by the exact commutative diagram

$$\begin{tikzcd}
 & & I_p(G) \arrow[r, equal] & I_p(G) & \\
0 \arrow[r] & \mathbb{Z}_p[G] \arrow[r] & \mathbb{Z}_p[G]^{n+2} \arrow[r] \arrow[u] & M' \arrow[r] \arrow[u] & 0 \\
0 \arrow[r] & \mathbb{Z}_p[G] \arrow[r] \arrow[u, equal] & R \arrow[r] \arrow[u] & G^{ab}_K \arrow[r] \arrow[u] & 0
\end{tikzcd} ,$$

where the right column is given by 1.2.c) and the middle row exists by 2.2., because $M'$ is cohomologically trivial, $\mathrm{Tor}(M') \cong \mu_K(p)$ is cyclic and $\mathbb{Q}_p \otimes M' \cong \mathbb{Q}_p[G]^{n+1}$ by (9). If we can show that $G$ is generated by n+2 elements, we are done, because then $R \cong R^{ab}_{n+2,p}$ by applying Schanuel's lemma to the middle column and 1.1.a).

For this we may assume that the ramification group of G is abelian, by Burnside's theorem on p-groups. If L is the fixed field of the ramification group, G is then a quotient of the middle group in the extension

$$(10) \qquad 1 \to G^{ab}_L \to G_k/[G_L,G_L] \to \overline{G} \to 1,$$

where $\overline{G} = Gal(L/k)$ is generated by 2 elements. Applying the above to L instead of K we get a surjection

$$\overline{\varphi}:\ R^{ab}_{n+2,p}(\overline{G}) \to G^{ab}_{L} ,$$

which induces an isomorphism in cohomology. As $H^2(\overline{G},G^{ab}_L)$ is generated by the element $x_1$ belonging to (10) (proposition of Weil-Safarevic) and $H^2(\overline{G},R^{ab}_{n+2})$ by $x_0$ belonging to

$$(11) \qquad 1 \to R^{ab}_{n+2} \to F_{n+2}/[R_{n+2},R_{n+2}] \to \overline{G} \to 1$$

(Tate, see [16]13.), after possibly multiplying $\overline{\varphi}$ by a unit in $\mathbb{Z}_p$, we may assume that the image of $x_0$ in $H^2(\overline{G},R^{ab}_{n+2,p})$ is mapped to $x_1$ under the map induced by $\overline{\varphi}$. This means ([1]p. 179) there exists a lifting

$$\varphi:\ F_{n+2}/[R_{n+2}/R_{n+2}] \to G_k/[G_L,G_L]$$

that induces $\overline{\varphi}$ and therefore has dense image. So $G_k/[G_L,G_L]$ is (topologically) generated by n+2 elements.

<u>3.2. COROLLARY</u>. *The absolute Galois group of a* $\mathfrak{p}$*-adic number field* k *is generated by* n+2 *elements,* $n = [k:\mathbb{Q}_p]$, *and this number is minimal.*

Indeed, if $K = k(\mu_p)$ and $G_k$ was generated by n+1 elements, $G^{ab}_K$ would be generated by [K:k]+1 elements as $\mathbb{Z}_p$-module (using (7) and the rank of $R^{ab}_{n+1}$), which is not true. 3.2. was shown in [15]1.4.d) for $\mu_p \subseteq k$.

ii) In the case of a global number field we assume that k is totally imaginary for p = 2 and fix the following notations.

$r_1$ and $r_2$ are the numbers of the real and complex places of k, respectively, and $r_1' \leq r_1$ is the cardinality of the set $S_\infty'$ of the real places of k which ramify in K/k. $S_p$ is the set of primes above p in k, and for any set T of primes in k and any extension L/k we let T(L) be the set of primes in L lying above primes in T. Finally, $L_\mathfrak{p}$ denotes the completion of L with respect to the prime $\mathfrak{p}$ of L, and d(H) is the minimal number of generators for a finitely generated profinite group H.

If $S_\infty' = \phi$ and hence $r_1' = 0$ (e.g., for K/k a p-extension), all statements are remarkably simplified, and we have a complete analogy with the local case.

3.3. THEOREM. *Let* k *be a finite extension of* $\mathbb{Q}$. *If Leopoldt's conjecture with respect to* p *is true for* K ([6] p. 274), $G_K^{ab}$ *has the property (*), and the following holds.*

*a) If* $d(G_k) \leq d$, *there is an exact sequence*

$$0 \to X \to R_{d,p}^{ab} \to G_K^{ab} \to 0 \tag{12}$$

*with a projective* $\mathbb{Z}_p[G]$*-module* X, *whose structure is defined by the isomorphism*

$$X \oplus \mathbb{Z}_p[G]^{r_1'} \cong Y_{S_\infty'} \oplus \mathbb{Z}_p[G]^{d-r_1-1} , \tag{13}$$

*where* $Y_{S_\infty'}$ *is the free* $\mathbb{Z}_p$*-module with basis* $S_\infty'(K)$ *and the natural (left) action of* G.

*b) One has* $d_G(\mathrm{Tor}(G_K^{ab})^*) \leq d(G_k)-r_2-1-r_1'+d_G(Y_{S_\infty'})$ *and conversely* $d(G_k) \leq \max(d(G),d_G(\mathrm{Tor}(G_K^{ab})^*)+r_2+1+r_1'-r_1'')$, *if* $Y_{S_\infty'}$ *has* $r_1''$ *free* $\mathbb{Z}_p[G]$*-summands.*

*c) If* $G_K^{ab}$ *is torsion free, the sequence (12) is splitting, and there is an isomorphism*

$$G_K^{ab} \oplus \mathbb{Z}_p[G]^{d-r_2-1} \cong Z_{S_\infty'} \oplus R_{d,p}^{ab} , \tag{14}$$

*where* $Z_{S_\infty'}$ *is defined by the property*

$$Y_{S_\infty'} \oplus Z_{S_\infty'} \cong \mathbb{Z}_p[G]^{r_1'} . \tag{15}$$

*d) If* $G_K^{ab}$ *is torsion free and* $\mu_p \subseteq K$, G *is generated by* $r_2+1+r_1'-r_1''$ *elements (and so is* $G_k$ *by c)). So for* $S_\infty' = \phi$ *we then get an isomorphism*

$$G_K^{ab} \cong R_{r_2+1,p}^{ab} . \tag{16}$$

3.4. Remarks. a) By the existence of $r_2+1$ linear independent $\mathbb{Z}_p$-extensions over k one has always $d \geq r_2+1$ in (13). X is well defined by the Krull-Schmidt theorem for $\mathbb{Z}_p[G]$-modules, in particular

$$X \cong Y_{S_\infty'} \oplus \mathbb{Z}_p[G]^{d-r_2-1-r_1'} \tag{17}$$

for $d - r_2 - 1 - r_1' \geq 0$ and

$$X \cong \mathbb{Z}_p[G]^{d-r_2-1}$$

for $S'_\infty = \phi$.

b) Choosing one decomposition group $G_{\mathfrak{p}} \subseteq G$ for every prime $\mathfrak{p} \in S'_\infty$, the module $Y_{S'_\infty}$ can be described as

(18) $$Y_{S'_\infty} = \bigoplus_{\mathfrak{p}\in S'_\infty} \operatorname{Ind}_{G_{\mathfrak{p}}}^{G}(\mathbb{Z}_p),$$

where $\operatorname{Ind}_{G_{\mathfrak{p}}}^{G}$ means induction from $G_{\mathfrak{p}}$ to G. As well

(19) $$Z_{S'_\infty} = \bigoplus_{\mathfrak{p}\in S'_\infty} \operatorname{Ind}_{G_{\mathfrak{p}}}^{G}(\mathbb{Z}_p(-1)),$$

where $\mathbb{Z}_p(-1)$ is the module $\mathbb{Z}_p$, on which the non-trivial element of $G_{\mathfrak{p}}$ acts by multiplication with -1. For $p \neq 2$ one has $\mathbb{Z}_p[G_{\mathfrak{p}}] = \mathbb{Z}_p \oplus \mathbb{Z}_p(-1)$, which shows (15) (recall that $S'_\infty = \phi$ for $p = 2$ by assumption).

<u>Proof of 3.3</u>. As $S$ contains $S_p$ and k is totally imaginary for $p = 2$, we have $cd_p(G_k) \leq 2$ (see [4] 2.11), and

(20) $$H^2(G_K, \mathbb{Q}_p/\mathbb{Z}_p) = 0,$$

if and only if the Leopoldt conjecture is true for K and p (using the same arguments as in [9]4.4). In this case, $cd_p(G_k) \leq 2$ implies

(21) $$H^i(G_L, \mathbb{Q}_p/\mathbb{Z}_p) = 0 \qquad \text{for all} \quad k \subseteq L \subseteq K$$

not only for $i \geq 3$ but also for $i = 2$, using (20) and the surjectivity of the corestriction, see [22]I 3.3. Using the spectral sequence

(22) $$H^i(G(K/L), H^j(G_K, \mathbb{Q}_p/\mathbb{Z}_p)) \Longrightarrow H^{i+j}(G_L, \mathbb{Q}_p/\mathbb{Z}_p)$$

one shows as in [16], App., or [9] 2.3, that $G_K^{ab}$ has the property (*) and $H^2(G, G_K^{ab})$ is generated by the element belonging to

$$0 \to G_K^{ab} \to G_k/[G_K, G_K] \to G \to 0 .$$

Proceeding as in the proof of 1.2.a), we get an exact sequence

(23) $$0 \to X \to R_{d,p}^{ab} \to G_K^{ab} \to 0$$

with projective X, if $G_k/[G_K,G_K]$ is generated by d elements.

On the other hand, class field theory gives us an exact sequence

$$(24) \qquad U_K\otimes_{\mathbb{Z}}\mathbb{Z}_p \to \prod_{\mathfrak{p}\in S(K)} U_{K_\mathfrak{p}}(p) \to G_K^{ab} \to Cl_K(p) \to 0,$$

where $U_K$ (resp. $U_{K_\mathfrak{p}}$) denotes the group of units in K (resp. $K_\mathfrak{p}$) and $Cl_K$ is the class group of K.

If the Leopoldt conjecture is true for K and p, the first map in (24) is injective and we may compute $\mathbb{Q}_p \otimes G_K^{ab}$. By Dirichlet's theorem $\mathbb{Q} \oplus \mathbb{Q}\otimes U_K$ is isomorphic to the $\mathbb{Q}$-vector space with all archimedean places of K as a basis and the natural permutation action of G on this basis. Therefore

$$(25) \qquad \mathbb{Q}_p \oplus \mathbb{Q}_p\otimes_{\mathbb{Z}} U_K \cong \mathbb{Q}_p\otimes Y_{S'_\infty} \oplus \mathbb{Q}_p[G]^{r_2+r_1-r'_1} .$$

On the other hand, by the local theory one gets

$$(26) \qquad \mathbb{Q}_p \otimes \Big( \prod_{\mathfrak{p}\in S(K)} U_{K_\mathfrak{p}}(p)\Big) \cong \mathbb{Q}_p[G]^n = \mathbb{Q}_p[G]^{r_1+2r_2} ,$$

with $n = [k:\mathbb{Q}] = \sum_{\mathfrak{p}\in S_p} [k_\mathfrak{p}: \mathbb{Q}_p]$. By (24) we calculate

$$(27) \qquad \mathbb{Q}_p\otimes G_K^{ab} \oplus \mathbb{Q}_p\otimes Y_{S'_\infty} \oplus \mathbb{Q}_p[G]^{r_2+r_1-r'_1} \cong \mathbb{Q}_p[G]^{r_1+2r_2} \oplus \mathbb{Q}_p,$$

while (23) and 1.1.b) imply

$$(28) \qquad \mathbb{Q}_p\otimes G_K^{ab} \oplus \mathbb{Q}_p\otimes X \cong \mathbb{Q}_p\otimes R_{d,p}^{ab} \cong \mathbb{Q}_p[G]^{d-1} \oplus \mathbb{Q}_p.$$

Combining (27) and (28) we get

$$\mathbb{Q}_p \otimes (X \oplus \mathbb{Z}_p[G]^{r'_1}) \cong \mathbb{Q}_p \otimes (Y_{S'_\infty} \oplus \mathbb{Z}_p[G]^{d-r_2-1}),$$

which implies (13) by Swan's theorem.

To show the first part of b), we apply the functor $M \rightsquigarrow M^+ = \mathrm{Hom}(M,\mathbb{Z}_p)$ to (12) and get the exact sequence

$$0 \to (G_K^{ab})^+ \to (R_{d,p}^{ab})^+ \to X^+ \to \mathrm{Tor}(G_K^{ab})^* \to 0,$$

because of the canonical isomorphism $\mathrm{Ext}^1_{\mathbb{Z}_p}(M,\mathbb{Z}_p) \cong \mathrm{Tor}(M)^*$. As $d_G(M\oplus\mathbb{Z}_p[G]) = d_G(M)+1$ for a finitely generated $\mathbb{Z}_p[G]$-module, see [8] 5.8, we get

$$d_G(\mathrm{Tor}(G_K^{ab})^*) \le d_G(X^+) = d_G(Y_{S'_\infty}{}^+) + d - r_2 - 1 - r_1$$

by (13) and the isomorphism $\mathbb{Z}_p[G]^+ \cong \mathbb{Z}_p[G]$, which also implies $d_G(P^+) = d_G(P)$ for projective P.

For the second part of b) one proceeds as in the proof of 3.1. (where we had $d_G(\mathrm{Tor}(G_K^{ab})^*) = 1$ and $d(G) \le n+2$), by considering $G_K^{ab} \oplus \tilde{Y}_{S'_\infty}$ for $Y_{S'_\infty} \cong \tilde{Y}_{S'_\infty} \oplus \mathbb{Z}_p[G]^{r_1''}$, and c) is clear.

For d) we use the fact that $H^2(G_K,\mathbb{Z}/p\mathbb{Z}) = 0$ for torsion free $G_K^{ab}$ (which follows from (20) and the cohomology sequence for $0 \to \mathbb{Z}/p\mathbb{Z} \to \mathbb{Q}_p/\mathbb{Z}_p \overset{p}{\to} \mathbb{Q}_p/\mathbb{Z}_p \to 0$). If K contains a primitive p-th root of unity, this is only possible, if K has only one prime $\mathfrak{p}_0$ above p, see [4] 3.3. In particular, G is equal to the decomposition group for $\mathfrak{p}_0$, and we may use the same arguments as in the local case (considering again $G_K^{ab} \oplus \tilde{Y}_{S'_\infty}$).

<u>3.5. COROLLARY</u>. *If K/k is a p-extension (and Leopoldt's conjecture is true for K and p), let* $d = \dim H^1(G_k)$ *and* $r = \dim H^2(G_k)$ *be the numbers of generators and relations of the pro-p-group* $G_k$*, respectively. Then* $r = d-r_2-1 = d_G(\mathrm{Tor}(G_K^{ab})^*) =$ *p-rank of* $\mathrm{Tor}(G_k^{ab})$*, and there is an exact sequence*

$$(29) \qquad 0 \to \mathbb{Z}_p[G]^r \to R_{d,p}^{ab} \to G_K^{ab} \to 0\ .$$

<u>Proof</u>. The equality $1-d+r = \chi(G_k) = -r_2$ was shown by Tate [24], $H^2(G_k,\mathbb{Q}_p/\mathbb{Z}_p) = 0$ implies $H^2(G_k)^* \cong \{x \in G_k^{ab} | px = 0\}$, see [5] 5.6., and $H^2(G_K,\mathbb{Q}_p/\mathbb{Z}_p) = 0$ implies $(G_K^{ab})^G \cong G_k^{ab}$, see [9] 2.3. Finally, for M a finite $\mathbb{Z}_p[G]$-module and G a p-group, one has $d_G(M^*) =$ p-rank of $M^*/I_p(G)M^* \cong (M^G)^*$.

<u>3.6. Examples and remarks</u>. a) The numbers d and r in 3.5. have been studied extensively by Koch in [17]. If s, resp. s', denotes the cardinality of S, resp. the subset $S' = \{\mathfrak{p} \in S | \mu_p \subseteq k\}$, one has

$$(30) \qquad \begin{array}{ll} s' \le r \le s' + c_p + r_1 + r_2 - 1 & \text{for } \mu_p \not\subseteq k, \\ r = s + c_p - 1 & \text{for } \mu_p \subseteq k, \end{array}$$

where $c_p$ is the p-rank of the S-class group of k (quotient of $Cl_k$ by the classes of the primes in S), and in both cases $r = s'-1$ for large S.

b) If K is a p-extension of $k = \mathbb{Q}$ $(p \ne 2)$ and Leopoldt's conjecture is true for K and p (e.g., K abelian), there is an exact sequence

$$(31) \qquad 0 \to \mathbb{Z}_p[G]^{s'} \to R_{s'+1,p} \to G_K^{ab} \to 0,$$

with s' as in a) (use (30)).

c) If $k = \mathbb{Q}(\sqrt{-D})$ is imaginary quadratic and $p \geq 5$ does not divide the class number of k, then for $S = S_p$ the group $G_k = G_{k,S_p}$ is free on two generators by (30). So for any p-extension K of k which is unramified outside p the Leopoldt conjecture is true for K and p (by (20)) and there is an isomorphism

$$G_K^{ab} \cong R_{2,p}^{ab} .$$

The same is true for p = 3 if the localizations above $\mathbb{Q}_3$ do not contain $\mu_3$.

## 4. The special case of $\mathbb{Z}_p$-extensions.

Let K/k, G = Gal(K/k), S, $\bar{K}$, $G_L = \mathrm{Gal}(\bar{K}/L)$ and the other notations be as in the beginning of §3. If k is a global field, assume that Leopoldt's conjecture is true for K and p, and that k is totally imaginary for p = 2.

4.1. THEOREM. *Let* $G_p$ *be a p-Sylow group of* G *and* $K_p$ *be the fixed field of* $G_p$. *If* $G_p$ *is cyclic, the following assertions are equivalent:*

*i)* $G^{ab} \cong M' \oplus R$ *with* M' *cohomologically trivial and* R *torsion free.*

*ii) The extension* $K/K_p$ *is embeddable in a* $\mathbb{Z}_p$*-extension.*

Proof. In a decomposition i), the $\mathbb{Z}_p[G]$-module R has the property (*), so as $G_p$-module $R \cong \mathbb{Z}_p \oplus P$ with P projective, as follows from 1.2.b) and (3). The projection $G_K^{ab} \twoheadrightarrow \mathbb{Z}_p$ induces an isomorphism in the cohomology under $G_p$, so there is a commutative diagram

$$(32) \qquad \begin{tikzcd} 1 \arrow[r] & G_K^{ab} \arrow[r] \arrow[d] & G_{K_p}/[G_K,G_K] \arrow[r] \arrow[d] & G_p \arrow[r] \arrow[d, equal] & 1 \\ 1 \arrow[r] & \mathbb{Z}_p \arrow[r] & \mathbb{Z}_p \arrow[r] & G_p \arrow[r] & 1 \end{tikzcd} ,$$

which shows ii).

On the other hand, if there is a diagram (32), we can solve the embedding problem

$$(33)\qquad \begin{tikzcd} & & & G_k \arrow[dl, dashed] \arrow[d] & \\ 1 \arrow[r] & R^{ab}_{m,p} \arrow[r] & E \arrow[r] & G \arrow[r] & 1 \end{tikzcd}$$

(i.e., the dotted arrow making the diagram commutative exists), where $E$ corresponds to an element of $H^2(G,R^{ab}_{m,p})$ which under the restriction map goes to that element of $H^2(G_p,R^{ab}_{m,p})$, which corresponds to the lower sequence in (32) via some $G_p$-isomorphism $R^{ab}_{m,p} \cong \mathbb{Z}_p \oplus \mathbb{Z}_p[G_p]^{m-1}$ ($G$ generated by $m$ elements). Indeed, the solvability may be checked on $G_p$ by a theorem of Hoechsmann, and there it is solvable by assumption. (In fact one has to look at the induced problems with kernel $R^{ab}_{m,p}/p^r\, R^{ab}_{m,p}$ for all $r$ to have finite modules and then use the fact that $G_k$ is finitely generated).

We get a map $G^{ab}_K \to R^{ab}_{m,p}$, which induces an isomorphism in cohomology (because it does in dimensions $i = 1,2,3$). Adding a suitable map $\mathbb{Z}_p[G]^r \to R^{ab}_{m,p}$, we get a surjective map

$$G^{ab}_K \oplus \mathbb{Z}_p[G]^r \twoheadrightarrow R^{ab}_{m,p} \quad ,$$

whose kernel $Q$ must be cohomologically trivial. Therefore the corresponding exact sequence splits, as $R^{ab}_{m,p}$ is torsion free, so

$$R^{ab}_{m,p} \oplus Q \cong G^{ab}_K \oplus \mathbb{Z}_p[G]^r \quad ,$$

which shows i) by the Krull-Schmidt theorem.

4.2. Remark. If $G_p$ has $d$ generators, $d > 1$, consider the statements

ii)' $K/K_p$ can be embedded in a $\hat{F}_d$-extension, $\hat{F}_d$ the free pro-p-group on $d$ generators.

iii) The embedding problem

$$(34)\qquad \begin{tikzcd} & & & G_{K_p} \arrow[d] & \\ 1 \arrow[r] & \hat{R}^{ab}_d \arrow[r] & \hat{F}_d/[\hat{R}_d,\hat{R}_d] \arrow[r] & G_p \arrow[r] & 1 \end{tikzcd}$$

is solvable.

Then i) $\Longleftrightarrow$ iii) $\Longleftarrow$ ii)', and iii) $\Longrightarrow$ ii)' for local fields by a result of Lur'e [18], compare [14] for the case of p-groups.

By 1.2.b) and 2.1. the modules $M'$ and $R$ in i) are determined by $\mathrm{Tor}(M') = \mathrm{Tor}(G^{ab}_K)$, $\mathbb{Q}_p \otimes M'$ and $\mathbb{Q}_p \otimes R$. But $\mathbb{Q}_p \otimes G^{ab}_K$ is known, and $M'$ and $R$ are uniquely defined up to projectives, so for (p-Sylow groups embeddable in) $\mathbb{Z}_p$-extensions the $\mathbb{Z}_p[G]$-structure of $G_K^{ab}$ is completely determined by $\mathrm{Tor}(G_K^{ab})$. We illustrate this first by completely determining the structure in the local case.

For this we also allow $K/k$ to be infinite, in which case $G_k^{ab}$ is a module over the completed group ring $\mathbb{Z}_p[[G]] = \varprojlim \mathbb{Z}_p[G/U]$, where $U$ runs over all open normal subgroups of $G$. The relation module for $G$ may then be described by $R^{ab}_{m,p} = R^{ab}_{m,p}(G) = \varprojlim R^{ab}_{m,p}(G/U)$, starting from a homomorphism $F_m \to G$ with dense image, which induces exact sequences $1 \to R_m(U) \to F_m \to G/U \to 1$ for all $U$. Another description is $R^{ab}_{m,p}(G) = \hat{R}^{ab}_m \otimes_{\hat{\mathbb{Z}}} \mathbb{Z}_p$, where $1 \to \hat{R}_m \to \hat{F}_m \to G \to 1$ is a presentation by a free profinite group $\hat{F}_m$ on $m$ generators.

<u>4.3. THEOREM</u>. *Let* $k$ *be of degree* $n$ *over* $\mathbb{Q}_p$ *and* $K/k$ *be a Galois extension such that* $K/K_p$ *is a* $\mathbb{Z}_p$*-extension or embeddable in a* $\mathbb{Z}_p$*-extension, where* $K_p$ *is the fixed field of a* $p$*-Sylow group of* $G$.

*a)* $G$ *has two generators.*

*b) If* $K/K_p$ *is cyclotomic and of finite degree,*

$$G_K^{ab} \cong \mu_K(p) \oplus \mathbb{Z}_p[\![G]\!]^n \oplus \mathbb{Z}_p. \tag{35}$$

*c) If* $K/K_p$ *is cyclotomic and of infinite degree,*

$$G_K^{ab} \cong \mathbb{Z}_p(1)^\delta \oplus \mathbb{Z}_p[\![G]\!]^n \ , \tag{36}$$

*where* $\mathbb{Z}_p(1)^\delta$ *is the Tate module of* $\mu_K(p)$ $(\mathbb{Z}_p(1)^\delta = \varprojlim \mu_{p^r}$ *for* $\mu_p \subseteq K$, $= 0$ *for* $\mu_p \not\subseteq K)$.

*d) If* $K/K_p$ *is not cyclotomic,*

$$G_K^{ab} \oplus \mathbb{Z}_p[\![G]\!] \cong M' \oplus R^{ab}_{2,p} \oplus \mathbb{Z}_p[\![G]\!]^{n-1} \ , \tag{37}$$

*with* $M'$ *given by the exact sequence*

$$\begin{aligned} 0 \to \mathbb{Z}_p[\![G]\!] &\to \mathbb{Z}_p[\![G]\!]^2 \to M' \to 0 \\ 1 &\to (x-g,\ 1+(q-1)\lambda), \end{aligned} \tag{38}$$

*where:* $x$ *generates the* $p$*-Sylow group,* $q$ *is the order of* $\mu_K(p)$, $g \in \mathbb{Z}_p$ *with* $\zeta^x = \zeta^g$ *for all* $\zeta \in \mu_K(p)$, *and* $\lambda$ *is the idempotent of* $\mathbb{Z}_p[\![G_o]\!]$ *which belongs to the action on* $\mu_K(p)$; *here* $G_o$ *is a maximal* $p'$*-subgroup (i.e., with order prime to* $p$*).*

<u>Proof</u>. Let $L_0$ (resp. $L_1$) be the fixed field of the inertia (resp. ramification) group and $\alpha\colon \mathrm{Gal}(L_1/k) \to (\mathbb{Z}_p/p^s\mathbb{Z}_p)^\times$, $0 \le s \le \infty$, be the

character of the operation on $\mathrm{Gal}(K/L_1)$. Then $\mathrm{Gal}(L_1/k)$ has two generators $\sigma,\tau$, where $\tau$ generates $\mathrm{Gal}(L_1/L_0)$ and $\sigma$ can be chosen such that $\alpha(\sigma)$ generates the image of $\alpha$. If $\tau^r$ generates $\mathrm{Ker}\,\alpha \cap <\tau>$ , $G$ is generated by $x\tau^r$ and $\sigma$ (where $\sigma$ and $\tau$ are suitable liftings in $G$), because the order of $\tau$ is prime to $p$ and $x\tau^r = \tau^r x$.

If $L_o^p$ is the maximal $p$-extension of $k$ in $L_o$, the order of $\mathrm{Gal}(L_1/L_o^p)$ is prime to $p$, and $G_o$ can be chosen as the image of a section of $\mathrm{Gal}(K/L_o^p) \twoheadrightarrow \mathrm{Gal}(L_1/L_o^p)$.

By taking limits, c) follows from b), and in b) we may assume $G$ to be finite (by a compactness argument we may take compatible isomorphisms (35), for which the transition maps on $\mathbb{Z}_p$ are just multiplication with the group index). Now $\mu_K(p)$ is cohomologically trivial for cyclotomic $K/K_p$, and $\mathbb{Z}_p$ is a module with the property (*) for $G$, because the $p$-Sylow group maps isomorphically onto the maximal $p$-quotient. Therefore $G_K^{ab} \cong \mu_K(p) \oplus \mathbb{Z}_p \oplus P$ with projective $P$, which must be free by Swan's theorem.

For d) we may again restrict to finite groups and then only have to check that $M'$ is the cohomologically trivial module with $\mathrm{Tor}(M') = \mu_K(p) = \mathrm{Tor}\,G_K^{ab}$ and $\mathbb{Q}_p \otimes M' = \mathbb{Q}_p[G]$. By 2.2. we only need to show that

$$\begin{array}{l} \mathbb{Z}_p[G]^2 \to \mathbb{Z}_p[G] \to \mu_K(p)^* \to 0 \\ \left.\begin{array}{l}(1,0) \mapsto x^{-1}-g, \\ (0,1) \mapsto 1+(q-1)\lambda^+\end{array}\right. , \ 1 \mapsto \text{generating element,} \end{array}$$

is exact. This is easy, using the fact that $x$ and $G_o$ generate $G$.

<u>4.4. Remarks</u>. a) If $g_o = (G_o:1)$ is finite and $\beta\colon G_o \to (\mathbb{Z}/p\mathbb{Z})^\times \subseteq \mathbb{Z}_p^\times$ is the character describing the operation on $\mu_K(p)$, one has $\lambda = n_o^{-1}\,\Sigma\,\beta(\rho)^{-1}\rho$, where the sum runs over all $\rho \in G_o$. For infinite $G_o$ one takes the limit of these elements for finite quotients.

b) The case $G_o = 1$ has been studied by Iwasawa in [11] and the split case (i.e., $G$ is the product of $\mathbb{Z}_p$ and $G_o$) by Dummit in [7]. They also get b) and c) but instead of d) an exact sequence $0 \to G_K^{ab} \to \mathbb{Z}_p[\![G]\!]^n \to \mu_K(p) \to 0$ which cannot exist in the non-split case, because then $\mathbb{Q}_p \otimes G_K^{ab}$ is not free.

c) For $n \geq 2$ one may cancel one $\mathbb{Z}_p[\![G]\!]$ in (37) and so get an explicit formula for $G_K^{ab}$. If the group $G$ is given, it is easy to determine $R_{2,p}^{ab}$ and a free summand of $M' \oplus R_{2,p}^{ab}$ for $n = 1$. For example, in the split case $R_{2,p}^{ab} \cong \mathbb{Z}_p[\![G]\!] \oplus \mathbb{Z}_p$ for $[K:K_p] < \infty$ and $R_{2,p}^{ab} \cong \mathbb{Z}_p[\![G]\!]$ for $[K:K_p] = \infty$.

For global fields 4.1. immediately implies

<u>4.5. PROPOSITION</u>. *If the* p-*Sylow subextension of* K/k *is embeddable in a* $\mathbb{Z}_p$-*extension and* K *is a totally real number field,*

(39) $$G_K^{ab} \cong \mathrm{Tor}(G_K^{ab}) \oplus \mathbb{Z}_p,$$

*and* $\mathrm{Tor}(G_K^{ab})$ *is cohomologically trivial.*

Now let k be an arbitrary finite extension of $\mathbb{Q}$ and $K = \bigcup_n K_n$ be the cyclotomic $\Gamma$-extension, $K_n = k(\mu_{p^{n+1}})$ and $\Gamma = \mathrm{Gal}(K/k)$. Let $\Gamma_n = \mathrm{Gal}(K/K_n)$ and assume that Leopoldt's conjecture with respect to p is true for all $K_n$ (e.g. k abelian). We want to relate the $\mathbb{Z}_p[[\Gamma]]$-module $X_1 = G_K^{ab}$ (usually considered for $S = S_p$, i.e., $X_1 = \mathrm{Gal}(M/k)$, where M is the maximal abelian p-extension of K unramified outside p) and $X_3 = \mathrm{Gal}(L'/K)$, where L' is the maximal abelian p-extension of K, which is unramified and in which every prime splits completely.

By Tate's duality theorem we get an exact sequence

(40) $$0 \to \mu_{K_n}(p) \to \prod_{\mathfrak{p}\in S(K_n)} \mu_{K_{n,\mathfrak{p}}}(p) \overset{\psi}{\to} \mathrm{Tor}(G_{K_n}^{ab}) \to R_1(K_n) \to 0$$

where $R_1(K_n)$ is the kernel of the map

(41) $$H^1(G_{K_n}, \mu_K(p) \to \prod_{\mathfrak{p}\in S(K_n)} H^1(G_{K_{n,\mathfrak{p}}}, \mu_{K_{n,\mathfrak{p}}}(p))$$

induced by the restriction maps (compare [21]2.5.ii), $H^2(G_K,\mathbb{Q}_p/\mathbb{Z}_p) = 0$ implies $H^2(G_K,\mathbb{Z}_p) \cong \mathrm{Tor}(G_K^{ab})^*$, $\psi$ is then given by the reciprocity map). By taking limits we get an exact sequence

(42) $$0 \to \mu_K(p) \to \bigoplus_{\mathfrak{p}\in S(K)} \mu_{K_\mathfrak{p}}(p) \to \varinjlim_n \mathrm{Tor}(G_{K_n}^{ab}) \to \mathrm{Hom}(X_3,\mu_K(p)) \to 0,$$

and, by dualizing and setting $X_4 = (\varinjlim_n \mathrm{Tor}(G_{K_n}^{ab}))^*$ (the limit being taken via the transfer maps), the exact sequence

(43) $$0 \to X_3(-1) \to X_4 \to \prod_{\mathfrak{p}\in S(K)} \mathbb{Z}_p(1) \to \mathbb{Z}_p(1) \to 0,$$

where M(n) denotes the n-th Tate twist of a $\mathbb{Z}_p[[\Gamma]]$-module M (as in [6]). Let $\Delta = \mathrm{Gal}(K_o/k)$, $d = (\Delta:1)$, and $e_i$ be the idempotent in $\mathbb{Z}_p[\Delta]$ belonging to the i-th power of the cyclotomic character, $0 \leq i \leq d-1$.

We then may split $X_1 (X_3, \ldots)$ into the direct sum of the $e_i X_1$ $(e_i X_3, \cdots)$ and consider these as modules under $\Lambda = \mathbb{Z}_p[\![\Gamma_o]\!]$.

Suppose now that $e_{1-i}X_3$ is known (and so also $(e_{1-i}X_3)(-1) = e_{-i}(X_3(-1)))$ and suppose further that we can calculate $e_{-i}X_4$ from (43) (e.g., if S(K) contains just one prime). Then we can get $e_i X_1$ as follows: Choose a minimal presentation

$$(44) \qquad \Lambda^{\ell_i} \xrightarrow{(\alpha_{rs})} \Lambda^{m_i} \to e_{-i}X_4 \to 0,$$

and take the transpose as in 2.2. to get an exact sequence

$$(45) \qquad 0 \to \Lambda^{m_i} \xrightarrow{(\alpha_{sr}^{+})} \Lambda^{\ell_i} \to M_i \to 0,$$

($M_i$ defined by exactness). Then there is an isomorphism

$$(46) \qquad e_i X_1 \cong M_i \oplus \Lambda^{d_i},$$

where

$$(47) \qquad d_i = m_i - \ell_i + \begin{cases} r_1 + r_2 & \text{for d even and i odd,} \\ r_2 & \text{else.} \end{cases}$$

Indeed, we have $(e_{-i}X_4)_{\Gamma_m} = (e_i \varinjlim_{n} \operatorname{Tor}(G_{K_n}^{ab})^{\Gamma_m})^* = (e_i \operatorname{Tor}(G_{K_m}^{ab}))^*$ for the module of coinvariants under $\Gamma_m$, using the fact that the transfer induces an isomorphism $\operatorname{Tor}(G_{K_n}^{ab}) \xrightarrow{\sim} \operatorname{Tor}(G_{K_{n+1}}^{ab})^{\Gamma_n}$ if $H^2(G_{K_{n+1}}, \mathbb{Q}_p/\mathbb{Z}_p) = 0$. So by 2.2. $(M_i)_{\Gamma_m}$ is cohomologically trivial with torsion module isomorphic to $e_i \operatorname{Tor}(G_{K_m}^{ab})$. The same is true for $(e_i X_1)_{\Gamma_m}$, as follows from the spectral sequence

$$(48) \qquad H^i(\Gamma_m, H^j(G_K, \mathbb{Q}_p/\mathbb{Z}_p)) \Longrightarrow H^{i+j}(G_{K_m}, \mathbb{Q}_p/\mathbb{Z}_p).$$

Therefore by 2.1. these modules only differ by projective $\mathbb{Z}_p[\Gamma_o/\Gamma_n]$-modules, whose structure is easily calculated knowing the structure of $e_i \mathbb{Q}_p \otimes G_{K_m}^{ab}$. Passing to the limit we obtain (46).

Bibliography.

1. Artin, E. and Tate, J., Class field theory, Harvard 1961.

2. Borevič, Z.I. On the group of principal units of a normal p-extension of a regular local field, Proc. Math. Inst. Steklov 80 (1965), 31-47.

3. Borevič, Z.I. and El Musa, A.J., Completion of the multiplicative group of p-extensions of an irregular local field, J. Soviet Math. 6, 3 (1976), 6-23.

4. Brumer, A., Galois groups of extensions of number fields with given ramification, Michigan Math. J. 13 (1966), 33-40.

5. Brumer, A., Pseudocompact algebras, profinite groups and class formations, J. Algebra 4 (1966), 442-470.

6. Coates, J., p-adic L-functions and Iwasawa's theory, in Algebraic Number Fields (Durham Symp. 1975, ed. A. Fröhlich), 269-353. Academic Press, London 1977.

7. Dummit, D., An extension of Iwasawa's Theorem on Finitely Generated Modules over Power Series Rings, Manuscripta Math. 43(1983), 229-259.

8. Gruenberg, K.W. Relation modules of finite groups, conf. board of math. sciences 25, AMS, Providence 1976.

9. Haberland, K., Galois Cohomology of Algebraic Number Fields, VEB Deutscher Verlag der Wissenschaften, Berlin 1978.

10. Iwasawa, K., On Galois groups of local fields, Trans. Amer. Math. Soc. 80 (1955), 448-469.

11. Iwasawa, K., On $\mathbb{Z}_\ell$-extensions of algebraic number fields, Ann. of Math. (2) 98(1973), 246-326.

12. Jannsen, U., Über Galoisgruppen lokaler Körper, Invent. Math. 70 (1982), 53-69.

13. Jannsen, U. and Wingberg, K., Die p-Vervollständigung der multiplikativen Gruppe einer p-Erweiterung eines irregulären $\mathfrak{p}$-adischen Zahlkörpers, J. reine angew. Math. 307/308 (1979), 399-410.

14. Jannsen, U. and Wingberg, K., Einbettungsprobleme und Galoisstruktur lokaler Körper, J. reine angew. Math. 319 (1980), 196-212.

15. Jannsen, U. and Wingberg, K., Die Struktur der absoluten Galoisgruppe $\mathfrak{p}$-adischer Zahlkörper, Invent. Math. 70 (1982), 71-98.

16. Kawada, Y., Class formations, Proc. Symp. Pure Math. 20 (1971), 96-114.

17. Koch, H., Galoissche Theorie der p-Erweiterungen, VEB Deutscher Verlag der Wissenschaften / Springer Berlin-Heidelberg-New York 1970.

18. Lur'e, B.B., Problem of immersion of local fields with a non abelian kernel, J.Soviet Math. 6, no. 3 (1976), 298-306.

19. Lyndon, R.C., Cohomology theory of groups with a single defining relation, Ann. of Math. (2) 53 (1950), 650-665.

20. Nguyen-Quang-Do, T., Sur la structure galoisienne des corps locaux et la théorie d'Iwasawa II, J. reine angew. Math. 333 (1982), 133-143.

21. Schneider, P., Über gewisse Galoiscohomologiegruppen, Math. Z. 168 (1979), 181-205.

22. Serre, J-P., Cohomologie galoisienne, Lecture Notes in Math. 5, Springer Verlag, Berlin-Heidelberg-New York 1964.

23. Swan, R., Induced representations and projective modules, Ann. of Math. (2) 71(1960), 522-578.

24. Tate, J., Duality theorems in Galois cohomology over number fields, Proc. Intern. Congress Math. 1962, Stockholm 1963, p. 288-295.

25. Wingberg, K. Die Einseinheitengruppe von p-Erweiterungen regulärer $\mathfrak{p}$-adischer Zahlkörper als Galoismodul, J. reine angew. Math. 305 (1979), 206-214.