Advanced Studies in Pure Mathematics 30, 2001
Class Field Theory – Its Centenary and Prospect
pp. 123–138

Galois Module Structure of p-Class Formations

Nguyen Quang Do Thong

0. Introduction

One of the main subjects in (classical) class field theory is to study the structure of the Galois groups $\mathcal{A}_L$ of abelian extensions of a local or global field L. One natural next step would be to take a Galois extension L/K with given group G and to investigate the structure of $\mathcal{A}_L$ as a G-module. This has been done by several authors (see e.g. [J$_2$], [N$_2$],..., and the references therein), mainly from the p-adic point of view: they single out a prime number p and focus their investigation on the $\mathbb{Z}_p[G]$-module structure of the p-Sylow subgroup A_L of $\mathcal{A}_L$. In the most interesting cases, it happens that (for a fixed base field K), the modules A_L constitute a so-called "p-class formation" (see §1); so the next natural step is to replace the A_L by the modules X_L belonging to any p-class formation. Adding noetherian conditions, we obtain (Thm. 3.2 (below)) that, up to projective summands, the $\mathbb{Z}_p[G]$-module X_L is determined by its $\mathbb{Z}_p$-torsion tX_L and a certain character χ_L of the group $H^2(G, tX_L)$. This generalizes a former result of U. Jannsen on the "homotopy type" of A_L ([J$_2$], Thm. 4.5) and could probably be proved by extending the methods of [J$_2$]. In order to throw some new light on the problem, we preferred instead to employ the technique of "envelopes" introduced by Gruenberg and Weiss ([GW], [W]) in their study of the Stark conjecture.

This paper (the first part of which is semi-expository) will be organized as follows: after recalling some known facts on p-class formations (§1) and the homotopy of modules (§2), we prove the main theorem in §3, essentially by giving a canonical description of the envelope of X_L by means of a relative Weil group, and of the character χ_L by means of a "trace form". As an illustration, we study in §4 the arithmetic of

Received August 17, 1998
Revised February 18, 1999

number fields which admit free pro-p-extensions of maximal rank (joint work with A. Lannuzel).

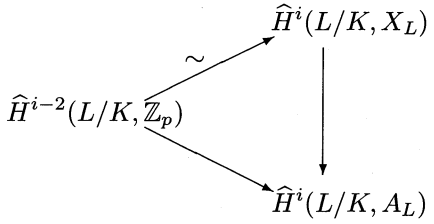
1. On p-class formations

Let $\mathcal{G}$ be a profinite group. For all generalities concerning class formations X attached to $\mathcal{G}$, we refer to [S], chap. XI. As a general convention, we will index the open subgroups of $\mathcal{G}$ by symbols K, L etc... as if they were Galois groups. The submodule of X fixed by such an open subgroup $\mathcal{G}_L$ will be denoted by X_L. For any pair of open subgroups $\mathcal{G}_L \subset \mathcal{G}_K$ such that $\mathcal{G}_L$ is normal in $\mathcal{G}_K$ (notation: $\mathcal{G}_L \lhd \mathcal{G}_K$), the quotient $G_{L/K} := \mathcal{G}_K/\mathcal{G}_L$ acts on X_L, and we will denote by $H^i(L/K, X_L)$ and by $\widehat{H}^i(L/K, X_L)$ respectively the ordinary and the modified cohomology groups.

1.1. Definition. Let p be a fixed prime number. A *p-class formation* $(\mathcal{G}, X)$ is a class formation with the additional property that all the modules X_L of the formation are $\mathbb{Z}_p$-modules. Then Tate's theorem implies that, for each pair of open subgroups $\mathcal{G}_L \lhd \mathcal{G}_K$, the cup-product with the fundamental class $\mathcal{E}_{L/K} \in H^2(L/K, X_L)$ induces an isomorphism $\widehat{H}^{i-2}(L/K, \mathbb{Z}_p) \xrightarrow{\sim} \widehat{H}^i(L/K, X_L)$ for every $i \in \mathbb{Z}$.

It is known that p-class formations "come essentially" from profinite groups $\mathcal{G}$ of strict p-cohomological dimension two (notation: $\mathrm{scd}_p \mathcal{G} = 2$). Let us make this more precise:

For a profinite group $\mathcal{G}$ and an open subgroup $\mathcal{G}_L$, write A_L for the p-Sylow subgroup of $\mathcal{G}_L^{\mathrm{ab}} := \mathcal{G}_L/\mathcal{G}'_L$ (the dash denotes the closed subgroup generated by commutators). If $(\mathcal{G}, X)$ is a p-class formation, the reciprocity map induces a homomorphism $\omega_L : X_L \to A_L$, and hence, for each pair of open subgroup $\mathcal{G}_L \lhd \mathcal{G}_K$ and for each $i \in \mathbb{Z}$, a homomorphism $\widehat{H}^i(L/K, X_L) \to \widehat{H}^i(L/K, A_L)$. Besides, the class $\xi_{L/K} \in H^2(L/K, \mathcal{G}_L^{\mathrm{ab}})$ associated with the extension $1 \to \mathcal{G}_L^{\mathrm{ab}} \to \mathcal{G}_K/\mathcal{G}'_L \to \mathcal{G}_K/\mathcal{G}_L \to 1$ induces by cup-product a homomorphism $\widehat{H}^{i-2}(L/K, \mathbb{Z}_p) \to \widehat{H}^i(L/K, A_L)$, and the theorem of Šafarevič-Weil gives a commutative triangle:



Kawada has defined $\mathcal{G}$ to be *p-malleable* if for each pair of open subgroups $\mathcal{G}_L \triangleleft \mathcal{G}_K$ and each $i \in \mathbb{Z}$, the above homomorphism $\widehat{H}^{i-2}(L/K, \mathbb{Z}_p) \to \widehat{H}^i(L/K, A_L)$ is an isomorphism. In this context, the main result is Brumer's theorem:

1.2 Theorem ([B], [K]). *The following properties are equivalent:*
i) $scd_p\mathcal{G} = 2$;
ii) $\mathcal{G}$ *is p-malleable;*
iii) *For every p-class formation* $(\mathcal{G}, X)$, *for each pair of open subgroups* $\mathcal{G}_L \triangleleft \mathcal{G}_K$ *and for each* $i \in \mathbb{Z}$, *the reciprocity map induces an isomorphism* $\widehat{H}^i(L/K, X_L) \xrightarrow{\sim} \widehat{H}^i(L/K, A_L)$;
iv) *For each pair of open subgroups* $\mathcal{G}_L \triangleleft \mathcal{G}_K$, *the transfer induces an isomorphism* $A_K \xrightarrow{\sim} H^0(L/K, A_L)$;
v) *For* $\mathcal{G}_L$ *running through the open subgroups of* $\mathcal{G}$, *the modules* A_L *constitute a p-class formation.*

Proof. The equivalence between i), ii) and iii) is the content of Thm. 6.1 of [B]. The equivalence between ii) and iv) is the content of §2.3, Propos. 10 of [Ha]. The remaining equivalence is obvious. □

We shall be mainly interested in the following examples:

1.3. Examples. 1) Let k be a p-adic local field (i.e. a finite extension of $\mathbb{Q}_p$) and $\mathcal{G} = \mathcal{G}_k$ be the absolute Galois group of k. Then $\mathrm{scd}_p\mathcal{G} = 2$.
2) Let k be a number field (supposed to be totally imaginary if $p = 2$), let S be a finite set of places containing the places above p and ∞, and $\mathcal{G} = \mathcal{G}_k(S)$ be the Galois group of the maximal S-ramified (i.e. unramified outside S) algebraic extension of k. Then $\mathrm{cd}_p\mathcal{G} \leq 2$, and $\mathrm{scd}_p\mathcal{G} = 2$ if and only if all finite S-ramified extensions of k verify Leopoldt's conjecture for p (here, cd_p and scd_p denote of course the p-cohomological dimensions).
3) If $\mathrm{cd}_p\mathcal{G} = 1$, then $\mathrm{scd}_p\mathcal{G} = 2$. This happens e.g. if $\mathcal{G}$ is some free profinite group $\mathcal{F}$.

Now take a finite group G and present it as a quotient $G \simeq \mathcal{F}_m/\mathcal{R}_m$, where $\mathcal{F}_m$ is free profinite on m generators. Let R_m^{ab} be the p-Sylow of $\mathcal{R}_m^{\mathrm{ab}}$. The *Lyndon resolution*

$$0 \to R_m^{\mathrm{ab}} \to \mathbb{Z}_p[G]^m \to \mathbb{Z}_p[G] \to \mathbb{Z}_p \to 0$$

is a 2-extension of $\mathbb{Z}_p$, the class of which is nothing but the fundamental class of $H^2(G, R_m^{\mathrm{ab}}) \simeq \mathrm{Ext}^2_{\mathbb{Z}_p[G]}(\mathbb{Z}_p, R_m^{\mathrm{ab}})$. Together with Schanuel's

lemma, it shows that, up to projective summands, the $\mathbb{Z}_p[G]$-module R_m^{ab} does not depend on m. By abuse of language, we will denote it by $R_m^{\mathrm{ab}}(G)$ or $R^{\mathrm{ab}}(G)$, and call it "the" *p-relation module of G*. Considered as a given data of G, it will intervene in the Galois module structure of all p-class formations (see 2.4).

2. Homotopy of modules and envelopes

Let G be a finite group and $\Lambda := \mathbb{Z}_p[G]$. In this section, we recall some basic facts concerning the homotopy theory of Λ-modules *of finite type*. The main references are [J$_2$] and [W].

2.1. Homotopy. Two Λ-modules M and N are *homotopic* (notation: $M \sim N$) if they differ by projective summands, i.e. if there exist two projective Λ-modules P and Q such that $M \oplus P \simeq N \oplus Q$. The homotopy class of M is denoted by $[M]$. Classifying Λ-modules up to homotopy is almost classifying them up to isomorphism, because $M \simeq N$ if and only if $M \sim N$ and $M \otimes \mathbb{Q}_p \simeq N \otimes \mathbb{Q}_p$ as $\mathbb{Q}_p[G]$-modules ([W], Chap. 6, Propos. 5).

A morphism of Λ-modules $f : M \to N$ is *homotopic to zero* (notation: $f \sim 0$) if f factors through a projective Λ-module. Two morphisms f and g are homotopic ($f \sim g$) if $f - g \sim 0$. The morphisms homotopic to zero form a subgroup of $\mathrm{Hom}_\Lambda(M, N)$, and the quotient is denoted $[M, N]$. We write $[f]$ for the class of f in $[M, N]$. One of our main tasks will be to determine $[M, N]$ for suitable Λ-modules M and N. If D is a Λ-*lattice* (i.e. D is a Λ-module without $\mathbb{Z}_p$-torsion), $[D, N] \simeq \widehat{H}^0(G, \mathrm{Hom}(D, N))$ canonically ([GW], 5.1). If D and D' are two Λ-lattices, we have an isomorphism $[D, D'] \simeq [D', D]^*$ (Pontryagin dual) induced by a pairing $[D, D'] \otimes [D', D] \xrightarrow{\cup} [D, D] \xrightarrow{\tau_D} \mathbb{Q}_p/\mathbb{Z}_p$, where τ_D is the so-called (*algebraic*) *trace form* $\tau_D : [D, D] \to \widehat{H}^0(G, \mathbb{Z}_p) \hookrightarrow \mathbb{Q}_p/\mathbb{Z}_p$ given by $\tau_D[g] \equiv \frac{1}{|G|}\mathrm{trace}(g) (\mathrm{mod} \mathbb{Z}_p)$ ([GW], 5.8).

2.2. Envelopes. A (*cohomologically trivial*) *envelope* of a Λ-module M is an exact sequence of Λ-modules:

$$0 \to M \to C \to D \to 0, \tag{1}$$

where C is a cohomologically trivial Λ-module and D is a Λ-lattice. It is not difficult to show that every Λ-module has an envelope, which is unique up to homotopy ([W], Chap. 6, Lemma 9). By abuse of language,

we will call C "the" envelope of M. Taking $\mathrm{Hom}(D, \cdot)$ and cohomology, we get a chain of isomorphisms

$$[D, D] \xrightarrow{\sim} \widehat{H}^0(G, \mathrm{Hom}(D, D)) \xrightarrow{\partial\sim} H^1(G, \mathrm{Hom}(D, M)) \xrightarrow{\sim} \mathrm{Ext}^1_\Lambda(D, M)$$

which sends $[\mathrm{id}_D]$ to the extension class of (1).

The shift to cohomologically trivial modules makes things easier because of *Jannsen's lemma*: two cohomologically trivial Λ-modules are homotopic if and only if their $\mathbb{Z}_p$-torsion submodules are Λ-isomorphic ([J$_1$], [W]). The problem is to recognize M starting from its envelope. There is a general "recognition theorem" due to Gruenberg and Weiss ([W], Chap. 6, Thm. 3), but we will be content with the following

2.3. Recognition lemma. *Let M be a Λ-module, T its $\mathbb{Z}_p$-torsion. Fix a Λ-lattice D and suppose there exists an exact sequence $0 \to M \to C \xrightarrow{f_M} D \to 0$, with C cohomologically trivial. Then the homotopy class $[M]$ is determined by the homotopy class $[f_M]$ and the isomorphism class of T.*

Proof. Suppose we have two exact sequences $0 \to M \to C \xrightarrow{f} D \to 0$ and $0 \to M' \to C' \xrightarrow{f'} D \to 0$ such that $f \sim f'$, C and C' are cohomologically trivial, and M and M' have the same $\mathbb{Z}_p$-torsion submodule T. Because D is a lattice, C and C' have the same torsion T; hence $C \sim C'$ by Jannsen's lemma. Write $C \oplus P \simeq C' \oplus P'$, with P and P' Λ-projective, and consider the surjective Λ-morphisms $C \oplus P \overset{f\oplus 0}{\twoheadrightarrow} D$ and $C' \oplus P' \overset{f'\oplus 0}{\twoheadrightarrow} D$. Since $f \sim f'$, we are in the situation of the *generalized Schanuel lemma* ([J$_2$], Lemma 1.3), which asserts that $\mathrm{Ker}(f \oplus 0) \sim \mathrm{Ker}(f' \oplus 0)$, i.e. $M \sim M'$. □

In the situation of Lemma 2.3, let us write $\widetilde{C} = C/T$. Then we have a commutative diagram

$$\begin{array}{ccc}
[D, \widetilde{C}] & \xrightarrow[\sim]{\delta} & H^1(G, \mathrm{Hom}(D, T)) \\
\downarrow & & \downarrow \\
[D, D] & \xrightarrow[\sim]{\partial} & H^1(G, \mathrm{Hom}(D, M)) \\
\downarrow{\scriptstyle \tau_D} & & \\
\mathbb{Q}_p/\mathbb{Z}_p & &
\end{array}$$

The lower horizontal isomorphism ∂ has already appeared in 2.2. The upper horizontal isomorphism δ is obtained analogously: from the exact sequence $0 \to T \to C \to \widetilde{C} \to 0$, we get an exact sequence $0 \to \mathrm{Hom}(D,T) \to \mathrm{Hom}(D,C) \to \mathrm{Hom}(D,\widetilde{C}) \to 0$ (because $\widetilde{C}$ is a lattice), and then by cohomology, an isomorphism $\widehat{H}^0(G,\mathrm{Hom}(D,\widetilde{C})) \xrightarrow{\sim} H^1(G,\mathrm{Hom}(D,T))$ (because $\mathrm{Hom}(D,C)$ is cohomologically trivial). The right vertical map is induced by the inclusion $T \hookrightarrow M$. The left vertical map $[D,\widetilde{C}] \to [D,D]$ is given by $[g] \mapsto [f_M \cdot g]$, by identifying $\mathrm{Hom}(C,D)$ and $\mathrm{Hom}(\widetilde{C},D)$ (because D is a lattice). The image of $[f_M]$ by the isomorphism $[C,D] = [\widetilde{C},D] \xrightarrow{\sim} [D,\widetilde{C}]^*$ is the composite map

$$[f_M]^* : [D,\widetilde{C}] \to [D,D] \to \mathbb{Q}_p/\mathbb{Z}_p, \quad [g] \mapsto \frac{1}{|G|}\mathrm{trace}(f_M \cdot g) (\mathrm{mod}\ \mathbb{Z}_p).$$

2.4. Special envelopes. In order to exploit Lemma 2.3, we must choose suitable lattices D. Let us say that a Λ-module is *special*, or admits a *special envelope*, if there exists an exact sequence:

$$0 \to M \to C \xrightarrow{f_M} I_G \to 0, \tag{2}$$

where C is cohomologically trivial and I_G is the augmentation ideal of Λ. The exact sequence (2) implies that $\widehat{H}^{i-2}(G,\mathbb{Z}_p) \xrightarrow{\sim} \widehat{H}^i(G,M)$ for all $i \in \mathbb{Z}$. Moreover, the exact sequence $0 \to \mathrm{Hom}(\mathbb{Z}_p,\cdot) \to \mathrm{Hom}(\Lambda,\cdot) \to \mathrm{Hom}(I_G,\cdot) \to 0$ gives canonical isomorphisms $H^1(G,\mathrm{Hom}(I_G,\cdot)) \simeq H^2(G,\cdot)$. We derive three consequences for a special Λ-module M:
1) The 2-extension $0 \to M \to C \to \Lambda \to \mathbb{Z}_p \to 0$ is described by the fundamental class (obvious definition) of $H^2(G,M) \simeq \mathrm{Ext}^2_\Lambda(\mathbb{Z}_p,M)$.
2) Comparing 1) with the Lyndon resolution (1.3), we get an alternative description of $[f_M]$ due to U. Jannsen ([J$_2$], 4.5b). More precisely, consider the chain of isomorphisms:

$$\begin{aligned}
[C,I_G] = [\widetilde{C},I_G] &\xrightarrow{\sim} \widehat{H}^0(G,\mathrm{Hom}(\widetilde{C},I_G)) \qquad \text{(by 2.1)} \\
&\simeq \widehat{H}^0(G,\mathrm{Hom}(C,I_G)) \\
&\xrightarrow{\sim} H^1(G,\mathrm{Hom}(C,R^{\mathrm{ab}})) \\
&\qquad \text{(by the left part of the Lyndon resolution in 1.3)} \\
&\simeq H^1(G,\mathrm{Hom}(\widetilde{C},R^{\mathrm{ab}})) \\
&\simeq \mathrm{Ext}^1_\Lambda(\widetilde{C},R^{\mathrm{ab}}) \hookrightarrow \mathrm{Ext}^1_\Lambda(C,R^{\mathrm{ab}}) \quad \text{(functorially)}
\end{aligned}$$

The image of $[f_M]$ in $\mathrm{Ext}^1_\Lambda(C, R^{\mathrm{ab}})$ is but the class of the pull-back extension:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & R_m^{\mathrm{ab}} & \longrightarrow & \Lambda^m & \longrightarrow & I_G & \longrightarrow & 0 \\ & & \| & & \uparrow & & \uparrow & & \\ 0 & \longrightarrow & R_m^{ab} & \longrightarrow & M' & \longrightarrow & C & \longrightarrow & 0 \\ & & & & \uparrow & & \uparrow & & \\ & & & & M & = & M & & \end{array}$$

3) The commutative diagram of 2.3 becomes

$$\begin{array}{ccc} [I_G, \widetilde{C}] & \xrightarrow[\delta]{\sim} & H^2(G,T) \\ \downarrow & & \downarrow \\ [I_G, I_G] & \xrightarrow[\partial]{\sim} & H^2(G,M) \\ \downarrow & & \\ \mathbb{Q}_p/\mathbb{Z}_p & & \end{array}$$

This defines a character

$$\chi_T := [f_M]^* \cdot \delta^{-1} : H^2(G,T) \to \mathbb{Q}_p/\mathbb{Z}_p.$$

Taking into account the generalized Schanuel lemma, we find that 2.3 becomes

2.5. Special recognition lemma. a) *Two special Λ-modules are homotopic if and only if their $\mathbb{Z}_p$-torsion submodules are Λ-isomorphic.* b) *Let M be a special Λ-module and T its $\mathbb{Z}_p$-torsion. Then the homotopy class $[M]$ is determined by the isomorphim class of T and the character χ_T. In particular, $\chi_T = 0 \iff M \sim R^{\mathrm{ab}}(G) \oplus C$, C being the special envelope of M.*

Remarks. a) Given T, there is a canonical construction of C due to U. Jannsen ([J$_1$], [J$_2$]). A free resolution $\Lambda^n \xrightarrow{\phi} \Lambda^m \to T^* \to 0$ exists if and only if there exists an exact sequence $0 \to (\Lambda^+)^m \xrightarrow{\phi^+} (\Lambda^+)^n \to C \to 0$ such that $\mathrm{tor}_{\mathbb{Z}_p} C \simeq T$. Here T^* is the Pontryagin dual of T and ϕ^+ is the *transpose map*, obtained by applying the functor $\mathrm{Hom}(\cdot, \Lambda)$. "The" module C is the *transposed module* of T^*, denoted by $D(T^*)$.

b) However, the recognition lemmas remain unsatisfactory because we don't know to what extent the invariants $[f_M]$ and χ_T (in spite of the notation) depend on M. Fortunately, this difficulty can be solved for p-class formations (see 3.4).

3. Galois module structure of p-class formations

A p-class formation $(\mathcal{G}, X)$ is called *of finite type* if all the $\mathbb{Z}_p$-modules X_L belonging to the formation are of finite type (note that similar conditions are required in Mazur's theory of Galois deformations; see [Ma]). All examples in 1.3 are of finite type.

In order to apply the special recognition lemma, we must show

3.1. Proposition. *Let $(\mathcal{G}, X)$ be a p-class formation of finite type. For each pair of open subgroups $\mathcal{G}_L \lhd \mathcal{G}_K$, the $\mathbb{Z}_p[\mathcal{G}_K/\mathcal{G}_L]$-module X_L admits a special envelope.*

Proof. We adapt the argument of [GW], 11.3. For simplicity, let us write $G = \mathcal{G}_K/\mathcal{G}_L$ and $\Lambda = \mathbb{Z}_p[G]$. The augmentation ideal is defined by the exact sequence $0 \to I_G \to \Lambda \to \mathbb{Z}_p \to 0$. Taking Hom $(\cdot, X_L)$ and cohomology, we get an isomorphism $H^1(G, \mathrm{Hom}(I_G, X_L)) \xrightarrow{\sim} H^2(G, \mathrm{Hom}(\mathbb{Z}_p, X_L)) = H^2(G, X_L)$. But $H^1(G, \mathrm{Hom}(I_G, X_L)) \simeq \mathrm{Ext}^1_\Lambda(I_G, X_L)$ because I_G is a lattice; hence we may consider the fundamental class $\mathcal{E}_{L/K}$ as a class of $\mathrm{Ext}^1_\Lambda(I_G, X_L)$, corresponding to a certain extension:

$$0 \to X_L \to Y_L \xrightarrow{f_L} I_G \to 0 \tag{3}$$

The cohomology of this exact sequence and of the augmentation sequence gives a chain of connecting maps:

$$\widehat{H}^{i-2}(G, \mathbb{Z}_p) \xrightarrow{\sim} \widehat{H}^{i-1}(G, I_G) \xrightarrow{\delta} \widehat{H}^i(G, X_L), \quad \forall i \in \mathbb{Z}.$$

Standard augument of homological algebra shows that the composite map is but the cup-product by $\mathcal{E}_{L/K}$, which is an isomorphism because we have a class formation. Hence the map δ is an isomorphism and $\widehat{H}^{i-1}(G, I_G) \xrightarrow{\sim} \widehat{H}^i(G, X_L)$, $\forall i \in \mathbb{Z}$. This shows that $\widehat{H}^i(G, Y_L) = 0$, $\forall i \in \mathbb{Z}$.

The same argument works for every subgroup of G, because of the functorial properties of the fundamental class with respect to restriction. Hence Y_L is cohomologically trivial. □

Remark. The extension of Λ-modules $0 \to X_L \to Y_L \to I_G \to 0$ just constructed and the extension of groups $0 \to X_L \to W_{L/K} \to G \to 0$ (the *relative Weil group*) defined by the fundamental class $\mathcal{E}_{L/K}$, are related by the so-called *translation functor* of Gruenberg and Weiss ([W], Chap. 3), which is an equivalence between two obvious categories.

Summarizing, we get

3.2. Theorem (*compare with* [J_2], 4.5). *Let $(\mathcal{G}, X)$ be a p-class formation of finite type. For each pair of open subgroups $\mathcal{G}_L \triangleleft \mathcal{G}_K$, the $\mathbb{Z}_p[\mathcal{G}_K/\mathcal{G}_L]$-module X_L is determined up to homotopy by:*
- the isomorphism class of its $\mathbb{Z}_p$-torsion tX_L, and
- the character χ_L of $H^2(L/K, tX_L)$ defined as the composite of the natural map $H^2(L/K, tX_L) \to H^2(L/K, X_L)$ and the invariant map of class formations $\mathrm{inv}_{L/K} : H^2(L/K, X_L) \xrightarrow{\sim} \widehat{H}^0(L/K, \mathbb{Z}_p) \hookrightarrow \mathbb{Q}_p/\mathbb{Z}_p$.

In particular the map $H^2(L/K, tX_L) \to H^2(L/K, X_L)$ is zero if and only if $X_L \sim R^{\mathrm{ab}}(\mathcal{G}_K/\mathcal{G}_L) \oplus D((tX_L)^*)$, where $R^{\mathrm{ab}}(\cdot)$ is the p-relation module and $D(\cdot)$ is the transposed module.

3.3. Special case. Let now $\mathcal{G}$ be a profinite group such that $\mathrm{scd}_p\mathcal{G} = 2$, and for an open subgroup $\mathcal{G}_L$, let A_L be the p-Sylow subgroup of $\mathcal{G}_L^{\mathrm{ab}}$. By the theorem of Brumer-Kawada (1.2), $(\mathcal{G}, (A_L))$ is a p-class formation, and we will assume from now on that it is of finite type. For $X_L = A_L$, Thm. 3.2 then gives Thm. 4.5 a) and b) of [J_2]. In this special case, the invariants which appear are of particular interest:
1) The special envelope of A_L can be taken as $B_L := H_0(\mathcal{G}_L, I_\mathcal{G})$, where $I_\mathcal{G}$ is the augmentation ideal of the completed group algebra $\mathbb{Z}_p[[\mathcal{G}]]$ ([J_2], [N_2]). If moreover $\mathcal{G}_K$ is a pro-p-group on d generators and r relations, we have a presentation $0 \to \Lambda^r \to \Lambda^d \to B_L \to 0$ (*where* $\Lambda = \mathbb{Z}_p[\mathcal{G}_L/\mathcal{G}_K]$) given by a matrix of *Fox derivatives*; in particular, B_L (and hence tA_L) is explicitly known if we know the relations of $\mathcal{G}_K$ (*see* [N_2]).
2) The module tA_L is an important arithmetical invariant when $\mathcal{G}$ is a Galois group. If the base field k is a p-adic local field, then $tA_L = \mu_L(p)$ (the group of p-primary roots of unity in L), and the Galois module structure is entirely determined up to homotopy ([J_1], [N_1]).

If the base field k is a number field and $\mathcal{G} = \mathcal{G}_k(S)$ (Ex. 1.3.2), tA_L is related by Iwasawa theory to p-adic L-functions (when they exist) and its structure has been studied intensively, e.g. in [N_3].
3) U. Jannsen ([J_2], 4.5 c)) has given an alternative description of the character χ_L of $H^2(L/K, tA_L)$ which shows that it does not depend on A_L, but only on $\mathcal{G}_L$ and tA_L.

Let us summarize Jannsen's result: Let

$$E_2^{(p)} = E_2^{(p)}(\mathcal{G}) := \varinjlim_m \varinjlim_L H^2(\mathcal{G}_L, \mathbb{Z}/p^m\mathbb{Z})^*$$

be the *p-dualizing module* of $\mathcal{G}$. It exists provided $\mathrm{cd}_p\mathcal{G} \leq 2$, and is characterized by the fact that $H^2(\mathcal{G}, M)^* \simeq \mathrm{Hom}_{\mathcal{G}}(M, E_2^{(p)})$ canonically for every p-torsion discrete $\mathcal{G}$-module. Note that the dualizing module is the same for $\mathcal{G}$ and for every open subgroup $\mathcal{G}_L$. If $\mathrm{scd}_p\mathcal{G} = 2$, then $tA_L \simeq H^2(\mathcal{G}_L, \mathbb{Z}_p)^*$ ([J1], [N1]) and $E_2^{(p)} \simeq \varinjlim_L tA_L$ with respect to the transfer. Thm. 4.5 c) of [J2] asserts that χ_L is the image of the identity of $E_2^{(p)}$ by the dual of the inflation map

$$\mathrm{Hom}_{\mathcal{G}_K}(E_2^{(p)}, E_2^{(p)}) \simeq H^2(\mathcal{G}_K, E_2^{(p)})^* \to H^2(L/K, tA_L)^*.$$

This can be seen quickly as follows:

The commutative diagram in 2.4.3 gives an isomorphism

$$H^2(L/K, tA_L)^* \xrightarrow{\sim} [B_L, I_G]$$

which sends χ_L to $[f_L]$ (= the homotopy class associated with the exact sequence (3) in the proof of 3.1). This isomorphism is functorial and, taking $\varinjlim_L$, we get $\mathrm{Hom}_{\mathcal{G}_K}(E_2^{(p)}, E_2^{(p)}) \simeq [I_{\mathcal{G}_K}, I_{\mathcal{G}_K}]$ by definition of $E_2^{(p)}$ and of the B_L. But $\varinjlim_L f_L = \mathrm{id}$ because $\varinjlim_L A_L = 0$.

We will now generalize this to get an analogous description of χ_L in the general case. Let us add a few notations: for a class formation $(\mathcal{G}, X)$, let tX_L be the $\mathbb{Z}_p$-torsion of X_L, $X = \varinjlim_L X_L$ and $tX = \varinjlim_L tX_L$; similar notations hold for the A_L. The reciprocity maps $X_L \to A_L$ induce maps $tX_L \to tA_L$ and $tX \to tA \simeq E_2^{(p)}$. Then:

3.4. Theorem. *The notations are the same as in* 3.2. *Suppose moreover that* $\mathrm{sdc}_p\mathcal{G} = 2$. *Then the character* χ_L *of* $H^2(L/K, tX_L)$ *is the image of the identity of* $E_2^{(p)}$ *by the composite of the natural map* $\mathrm{Hom}_{\mathcal{G}_K}(E_2^{(p)}, E_2^{(p)}) \to \mathrm{Hom}_{\mathcal{G}_K}(tX, E_2^{(p)})$ *and the dual of the inflation map* $\mathrm{Hom}_{\mathcal{G}_K}(tX, E_2^{(p)}) \simeq H^2(\mathcal{G}_K, tX)^* \to H^2(L/K, tX_L)^*$.

Proof. Because all our constructions are functorial, we have a commutative diagram

$$\begin{array}{ccc} H^2(L/K, tA_L)^* & \xrightarrow{\text{nat}} & H^2(L/K, tX_L)^* \\ \uparrow{\scriptstyle \inf^*} & & \uparrow{\scriptstyle \inf^*} \\ \mathrm{Hom}_{\mathcal{G}_K}(E_2^{(p)}, E_2^{(p)}) & \xrightarrow{\text{nat}} & \mathrm{Hom}_{\mathcal{G}_K}(tX, E_2^{(p)}), \end{array}$$

where the upper horizontal map sends the character χ_L corresponding to A_L to that corresponding to X_L. By Jannsen's theorem, the conclusion is obvious. □

Thm. 3.4 shows in particular that χ_L does not depend on X_L, but only on tX_L and $\mathcal{G}_L$.

4. On free pro-p-extensions

In this section, we fix a base field k, which is a p-adic local field or a number field, and we take $\mathcal{G} = \mathcal{G}_k$ or $\mathcal{G}_k(S)$ as in Examples 1.3.1 and 1.3.2. To simplify, we also suppose $p \neq 2$ and $\mathrm{scd}_p\mathcal{G} = 2$ (although a closer look at the proofs of Thm. 3.2 and 3.4 shows that weaker hypotheses could also work). Let G be a finite quotient of $\mathcal{G}$, corresponding to a Galois extension K/k. We stick to the notations of Thm. 3.2 and 3.4. Whereas the torsion module tA_K is related to Iwasawa theory and p-adic L-functions, the character χ_K is related to the *embedding problem* ([JW], [N$_1$]).

Because of the last statement of Thm. 3.2, we would like to study the arithmetical implications of the nullity of χ_K. The approach in 2.3 is sharp enough, in principle, to allow us to kill χ_K. It is known ([JW], [N$_1$]) that $\chi_K = 0$ if and only if every embedding problem with p-abelian kernel

$$\begin{array}{ccccccccc} & & & & & & \mathcal{G} & & \\ & & & & & \swarrow & \downarrow & & \\ 0 & \longrightarrow & A & \longrightarrow & E & \longrightarrow & G = \mathrm{Gal}(K/k) & \longrightarrow & 0 \end{array}$$

admits a solution (= the existence of the dotted arrow).

If we particularize further by supposing that G is a p-group and by replacing $\mathcal{G}$ by its maximal pro-p-quotient $\mathcal{G}(p)$, then it is clear that every embedding problem:

(4)
$$\begin{array}{ccccccccc} & & & & & & \mathcal{G}(p) & & \\ & & & & & \swarrow & \downarrow & & \\ 0 & \longrightarrow & A & \longrightarrow & E & \longrightarrow & G = \mathrm{Gal}(K/k) & \longrightarrow & 0 \end{array}$$

admits a solution if the given epimorphism $\mathcal{G}(p) \twoheadrightarrow G$ factors through a free pro-p-group. This leads us to

4.1. Definition (*see* [N$_1$]). A *free pro-p-extension*, or F_d*-extension*, is a Galois extension L/k such that $\mathrm{Gal}(L/k)$ is isomorphic to a free pro-p-group F_d on d generators.

Note that $F_1 \simeq \mathbb{Z}_p$ is the only abelian free pro-p-group. Define ρ_k to be *the maximal* d *such that* k *admits an* F_d*-extension.*

In the local case, the interplay between the value of ρ_k, the nullity of χ_K and the embedding problem is entirely known and can be summarized as follows:

4.2. Theorem ([JW], [N$_1$]). *Let* k *be a* p*-adic local field, and* $\mu_k(p)$ *the group of* p*-primary roots of unity in* k*. Suppose that* $G = \mathrm{Gal}(K/k)$ *is a* p*-group, and denote by* $d = d(G) := \dim H^1(G, \mathbb{Z}/p\mathbb{Z})$ *the minimal number of generators of* G*. Then:*
A. *If* $\mu_k(p) = 1$*, the Galois group* $\mathcal{G}_K(p)$ *is pro-p-free (Šafarevič),* $\rho_k = 1 + [k : \mathbb{Q}_p]$*, and* $A_K \simeq R_d^{\mathrm{ab}}(G) \oplus \mathbb{Z}_p[G]^{\rho_k - d}$.
B. *If* $\mu_k(p) \neq 1$*, the following four conditions are equivalent:*
i) $\chi_K = 0$;
ii) $A_K \sim R_d^{\mathrm{ab}}(G) \oplus D(\mu_K(p)^*)$;
iii) *Every embedding problem* (4) *admits a solution;*
iv) K/k *is embeddable in an* F_d*-extension;*
If moreover G *is abelian, the above conditions are equivalent to:*
v) *Let* p^s *be the minimum of the order of* $\mu_K(p)$ *and of the exponent of* G*. Then* $\mu_k(p) \subset N_{K/k}(K^*)$*, and for any* $h \leq s$*, the* $\mathbb{Z}/p^h\mathbb{Z}$*-module* $H^1(G, \mu_{p^h})$ *is orthogonal to itself with respect to the Hilbert symbol of order* p^h.

As a consequence of v), $\rho_k = 1 + \frac{1}{2}[k : \mathbb{Q}_p]$ (*J. Sonn*).

The situation in the global case is much more complicated. Let k be a number field, let $r_2 = r_2(k)$ be the number of complex places of k, S a finite set of primes of k containing the places above p and ∞, $\mathcal{G} = \mathcal{G}_k(S)$ as in Ex. 1.3.2, $A_k(S) = \mathcal{G}_k(S)^{\mathrm{ab}}(p)$, and $t(A_k(S)) = \mathrm{tor}_{\mathbb{Z}_p}(A_k(S))$. It is known that every F_d-extension is S_p-ramified. Because of our assumption $\mathrm{scd}_p \mathcal{G}_k(S) = 2$, k verifies Leopoldt's conjecture; hence $\rho_k \leq 1 + r_2$. Examples are known for which $\rho_k < 1 + r_2$ ([Y]). What would be a global analogue of Thm. 4.2?
A. Because of Leopoldt's conjecture, it is obvious that

$$t(A_k(S_p)) = 1 \Longleftrightarrow \mathcal{G}_k(S_p)(p) \text{ is pro-}p\text{-free} \Longrightarrow \rho_k = 1 + r_2.$$

Number fields k for which $\mathcal{G}_k(S_p)(p)$ is pro-p-free are called *p-rational* and have been extensively studied in [MN].

B. If $t(A_k(S_p)) \neq 1$, we still have i) $\Longleftrightarrow$ ii) $\Longleftrightarrow$ iii) $\Longleftarrow$ iv), but we don't know if iii) $\Longrightarrow$ iv) (except in particular cases). The main difficulty is that we don't have any global analogue of v) (there is no "global Hilbert symbol"). One easy special case is the totally real case ($r_2 = 0$):

4.3. Proposition. *Suppose that the number field k is totally real, and let K/k be an S-ramified Galois extension such that $G = \mathrm{Gal}(K/k)$ is a cyclic p-group. The following three conditions are equivalent:*
i) $\chi_K = 0$;
ii) $A_K(S) \simeq \mathbb{Z}_p \oplus (t(A_K(S))$, *and* $t(A_K(S))$ *is cohomologically trivial;*
iii) K/k *is embeddable in a* $\mathbb{Z}_p$*-extension.*

We omit the proof, which is obvious. The imaginary case ($r_2 \neq 0$) seems to be much deeper. To study the extreme situation, corresponding to $\rho_k = 1+r_2$, we must appeal to hard (as yet unsolved) conjectures. The following results have been obtained in collaboration with A. Lannuzel. The proofs will appear elsewhere.

We start by recalling some conjectures of Greenberg, a "classical" one and a "generalized" one:

4.4. Greenberg's conjecture (GC). *Let k be a totally real number field, $k_\infty = \bigcup_n k_n$ its cyclotomic $\mathbb{Z}_p$-extension, $\Gamma = \mathrm{Gal}(k_\infty/k_n)$, A'_n the modified p-class group of k_n (=the p-class group divided by the classes of ideals above p), $A'_\infty = \varinjlim A'_n$, $X'_\infty = \varprojlim A'_n$, and $\Lambda = \mathbb{Z}_p[[\Gamma]]$ the usual Iwasawa algebra. Then the following properties are equivalent:*
1) *The Γ-module A'_∞ is zero.*
2) *The Λ-module X'_∞ is finite.*

Greenberg's conjecture (GC) asserts that these equivalent properties hold for any totally real field (see [G$_1$]) and has been verified for many families of abelian fields, mainly quadratic fields (see e.g. [IS] and the references therein). Note that Greenberg's original formulation concerns p-class groups instead of modified p-class groups, but is known to be equivalent to the formulation above when Leopoldt's conjecture always holds along the cyclotomic tower - which is the case here.

In order to state a generalization of (GC) to any number field k, we must introduce: $\widetilde{K}_\infty$= the compositum of all $\mathbb{Z}_p$-extensions of k, $\widetilde{\Gamma} = \mathrm{Gal}(\widetilde{K}_\infty/k)$ ($\simeq \mathbb{Z}_p^{1+r_2}$ here), $\widetilde{\Lambda} = \mathbb{Z}_p[[\widetilde{\Gamma}]]$ = the multivariable Iwasawa algebra,

$$X_\infty = \varprojlim_L A_L, \quad X'_\infty = \varprojlim_L A'_L, \quad A'_\infty = \varinjlim_L A'_L$$

Here L runs through all finite subextensions of $\widetilde{K}_\infty/k$, A_L is defined as in 3.3 and A'_L is as in 4.4.

Let us recall the structure of X_∞:

4.5. Theorem (*see* [G_2]). *The $\widetilde{\Lambda}$-module X_∞ has $\widetilde{\Lambda}$-rank r_2. It has no non zero pseudo-null submodule.*

(Remember that "pseudo-null" means "killed by two co-prime elements of $\widetilde{\Lambda}$". If $\widetilde{\Lambda} = \Lambda$, "pseudo-null" is the same thing as "finite").

Thm. 4.5 is proved in [G_2] by using induction and class field theory. A simpler cohomological proof (by using the special envelopes B_L), more in the spirit of this talk, can be found in [N_2]. By means of Kummer's theory (after adding μ_p to k), Fitting's ideals, "Spiegelung" and decomposition properties of primes above p in $\widetilde{K}_\infty/k$, one can show the following (not so easy) lemma.

4.6. Lemma. *For an imaginary number field k ($r_2 \neq 0$), the following are equivalent:*

1) *The $\widetilde{\Gamma}$-module A'_∞ is zero.*
2) *The $\widetilde{\Lambda}$-module X'_∞ is pseudo-null.*
3) *The $\widetilde{\Lambda}$-torsion submodule of X_∞ is zero (if k contains μ_p).*

4.7. Greenberg's generalized conjecture (GGC). *The equivalent properties of* 4.6 *hold for every imaginary number field.*

Property 4.6.2 has been verified for many families of quadratic number fields by J. Minardi, and a few biquadratic fields by D. Hubbard (two students of R. Greenberg). Note that the local analogue of 4.6.3 holds true ([N_2], 4.3).

Remark. It is worth noting that, in spite of their common formulation in terms of class groups, the two conjectures (GC) and (GGC) are *not of the same nature*, because the property 4.6.3 definitely does not hold for totally real fields. Actually, for totally real fields, the torsion module $\mathrm{tor}_\Lambda X_\infty$ is related by the "main conjecture" of Iwasawa's theory to p-adic L-functions, hence is not trivial in general. The validity of 4.6.3 for imaginary fields, in this circle of ideas, would destroy any "naive" hope of constructing multivariable p-adic L-functions starting from $\mathrm{tor}_{\widetilde{\Lambda}} X_\infty$.

We can now state the main theorem concerning the extreme case $\rho_k = 1 + r_2$. R. Greenberg told us at the conference that his student Hubbard had obtained in his thesis [Hu] a similar, but somewhat weaker result (essentially because Lemma 4.6 is not available in [Hu]).

4.8. Theorem ([L], [Hu]). *Let k be an imaginary number field ($r_2 \neq 0$) verifying* (GGC). *The following two properties are equivalent:*
1) $\rho_k = 1 + r_2$.
2) *k is p-rational, i.e. $\mathcal{G}_k(S_p)(p)$ is pro-p-free.*

Note that, by the remark after 4.7, the extreme case $\rho_k = 1 + r_2$ is radically different, according as k is totally real (4.3) or is imaginary (4.8).

References

[B] A. Brumer, Pseudo-compact algebras, profinite groups and class-formations, J. of Algebra, **4** (1966), 33–40.

[G_1] R. Greenberg, On the Iwasawa invariants of totally real fields, Amer. J. Math., **98** (1976), 263–284.

[G_2] R. Greenberg, On the structure of certain Galois groups, Invent. Math., **47** (1978), 85–99.

[GW] K. W. Gruenberg and A. Weiss, Galois invariants for units, Proc. London Math. Soc., **70** 3 (1995), 264–284.

[Ha] K. Haberland, "Galois cohomology of algebraic number fields", VEB Deutscher Verlag der Wissenschaften, Berlin (1978).

[Hu] D. Hubbard, "The non-existence of certain free pro-p-extensions and capitulation in a family of dihedral extensions of $\mathbb{Q}$", Thesis, University of Washington (1996).

[IS] H. Ichimura and H. Sumida, On the Iwasawa invariants of certain real abelian fields II, Internat. Math. J., **7** 6 (1996), 721–744.

[J_1] U. Jannsen, On the structure of Galois groups as Galois modules, in "Number Theory, Noordwijkerhout 1983", Springer LNM, **1068** (1984), 109–125.

[J_2] U. Jannsen, Iwasawa Modules up to isomorphism, in "Algebraic Number Theory - in honor of K. Iwasawa", Advanced Studies in Pure Math., **17** (1989), 171–207.

[JW] U. Jannsen and K. Wingberg, Einbettungsprobleme und Galoisstruktur lokaler Körper, J. reine angew. Math., **319** (1980), 196–212.

[K] Y. Kawada, Cohomology of group extensions, J. Fac. Sci. Univ. Tokyo, **9** (1963), 417–431.

[L] A. Lannuzel, Sur les extensions pro-p-libres d'un corps de nombres, prépublication (1997).

[Ma] B. Mazur, Deforming Galois representations, in "Galois groups over $\mathbb{Q}$", MSRI Publ., **16** (1987), 385–437.

[Mi] J. Minardi, Iwasawa modules for $\mathbb{Z}_p^d$-extensions of number fields, Canadian Math. Soc. Conf. Proc., **7** (1987), 237–242.

[MN] A. Movahhedi and T. Nguyen Quang Do, Sur l'arithmétique des corps de nombres p-rationnels, Sém. Théorie des Nombres Paris 1987/88, Progr. Math. Birkhaüser, Boston, **81** (1990), 155–200.

[N_1] T. Nguyen Quang Do, Sur la structure galoisienne des corps locaux et la théorie d'Iwasawa, Compositio Math., **48** 1 (1982), 85–119.

[N_2] T. Nguyen Quang Do, Formations de classes et modules d'Iwasawa, in "Number Theory, Noordwijkerhout 1983", Springer LNM, **1068** (1984), 167–185.

[N_3] T. Nguyen Quang Do, Sur la $\mathbb{Z}_p$-torsion de certains modules galoisiens, Ann. Inst. Fourier, **36** (1986), 27–46.

[S] J.-P. Serre, "Corps locaux", Hermann, Paris (1962).

[W] A. Weiss, "Multiplicative Galois module structure", Fields Institute Monographs, **6** (1996).

[Y] M. Yamagishi, A note on free pro-p-extensions of algebraic number fields, J. Théor. Nombres Bordeaux, **5** (1993), 165–178.

UMR 6623 CNRS
Laboratoire de Mathématiques
Université de Franche-Comté
16 route de Gray F-25030 BESANÇON CEDEX FRANCE