

COMPOSITIO MATHEMATICA

THONG NGUYEN-QUANG-DO

**Sur la structure galoisienne des corps locaux
et la théorie d'Iwasawa**

Compositio Mathematica, tome 46, n° 1 (1982), p. 85-119

http://www.numdam.org/item?id=CM_1982__46_1_85_0

© Foundation Compositio Mathematica, 1982, tous droits réservés.

L'accès aux archives de la revue « Compositio Mathematica » (<http://http://www.compositio.nl/>) implique l'accord avec les conditions générales d'utilisation (<http://www.numdam.org/conditions>). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques

<http://www.numdam.org/>

SUR LA STRUCTURE GALOISIENNE DES CORPS LOCAUX ET LA THEORIE D'IWASAWA

Thong Nguyen-Quang-Do

§0 Introduction

Soit k un corps local p -adique, c'est-à-dire une extension finie du corps \mathbb{Q}_p des nombres p -adiques. Etant donnée une extension galoisienne finie K/k , de groupe de Galois G , on sait que l'étude du G -module K^\times peut se ramener à l'étude du $\mathbb{Z}_p G$ -module E_K , où E_K est le groupe des unités principales de K^\times ([2b], §2).

Dans le cas modérément ramifié (e.g. si p ne divise pas l'ordre de G), ce problème a été étudié et résolu par de nombreux auteurs (pour un compte-rendu et une description détaillés, voir par exemple [12], [22]). Pour étudier le cas sauvagement ramifié, on se ramène à l'hypothèse où G est un p -groupe. Il est alors plus commode, et aussi plus naturel, de remplacer E_K par le $\mathbb{Z}_p G$ -module $A(K) = \varprojlim K^\times / K^{\times p^n}$. Par le corps de classes, $A(K)$ est isomorphe au groupe de Galois de la pro- p -extension abélienne maximale de K . On ne connaît encore que des résultats partiels sur $A(K)$ (voir notamment [2], [3], [14], [32]), qu'on peut résumer comme suit:

– si le corps k est régulier, i.e. ne contient pas de racine primitive $p^{\text{ième}}$ de l'unité, il résulte d'un théorème de Šafarevič que le $\mathbb{Z}_p G$ -module $A(K)$ est projectivement équivalent à R_d^{ab} , le module des pro-relations minimal de G (voir définitions au §1).

– si k est irrégulier, i.e. contient les racines $p^{\text{ièmes}}$ de l'unité, la situation est beaucoup plus compliquée. D'après un résultat de Jannsen et Wingberg ([14]), deux cas, et deux seulement, peuvent se présenter:

(a) le cas *totalemtent irrégulier*, où $A(K)$ est projectivement équivalent à un $\mathbb{Z}_p G$ -module indécomposable.

(b) le cas *quasi-régulier*, où $A(K)$ est projectivement équivalent à la somme directe de R_d^{ab} et d'un $\mathbb{Z}_p G$ -module indécomposable.

L'objet de ce travail est d'étudier d'une façon extensive le cas quasi-régulier. De façon assez surprenante (théorème principal, §2), ce cas est relié à un problème de plongement, plus précisément au problème de la factorisation d'un groupe de Demuškin à travers un pro- p -groupe libre, dont l'étude a été initiée par J. Sonn ([27]) dans le cas où G est abélien. Il en résulte une extension de la théorie d'Iwasawa pour les corps locaux (§8), où les \mathbb{Z}_p -extensions sont remplacées par les F_d -extensions (F_d est un pro- p -groupe libre à d générateurs) et l'algèbre d'Iwasawa à une variable est remplacée par l'algèbre de Magnus à d variables. Une tentative de globalisation est faite au §9, en liaison avec la conjecture de Leopoldt. Enfin, F. Laubie ([17]) donnera une application à l'étude de la ramification dans les groupes de Lie p -adiques.

§1 Préliminaires algébriques

Dans toute la suite, on adoptera les notations et les conventions suivantes: p est un nombre premier, \mathbb{Z}_p est l'anneau des entiers p -adiques, F_p est le corps \mathbb{Z}/p . Un p -groupe est un groupe fini dont l'ordre est une puissance de p . Un pro- p -groupe est une limite projective de p -groupes. Pour tout pro- p -groupe H , le rang $d(H)$ de H est le nombre minimal de générateurs; il est égal à $\dim H^1(H, F_p)$. Sauf mention expresse du contraire, tous les pro- p -groupes considérés seront supposés de rang fini.

1.1 Module des pro-relations

Nous reprenons d'abord quelques définitions de [20]. Soit G un p -groupe fixé, de rang d . Une *présentation libre* de G est une suite exacte $1 \rightarrow R_n \rightarrow F_n \rightarrow G \rightarrow 1$, où F_n est un pro- p -groupe libre de rang n ($n \geq d$) et R_n un sous-groupe normal de F_n . L'entier n est le rang de la présentation libre. Si nous ne voulons pas préciser ce rang, nous écrirons simplement F et R au lieu de F_n et R_n . Une présentation libre de G est dite *minimale* si son rang est égal au rang de G . Le $\mathbb{Z}_p G$ -module $R^{ab} = R/[R, R]$ est appelé module des *pro-relations* de G .

Si la présentation est minimale, le module est appelé *minimal*, et noté R_d^{ab} . La classe de cohomologie $\chi \in H^2(G, R^{ab})$ associée à l'extension $1 \rightarrow R^{ab} \rightarrow F/[R, R] \rightarrow G \rightarrow 1$ est appelée *classe caractéris-*

tique. A équivalence projective près, les notions précédentes ne dépendent pas de la présentation libre choisie de G . Plus précisément:

THÉORÈME 1: *Soit G un p -groupe de rang d . Pour tout entier $n \geq d$, on a un isomorphisme de $\mathbb{Z}_p G$ -modules $R_n^{ab} \simeq R_d^{ab} \times (\mathbb{Z}_p G)^{n-d}$. Le $\mathbb{Z}_p G$ -module R_d^{ab} est indécomposable.*

PREUVE: voir [20]. Les modules de pro-relations de G peuvent être caractérisés de façon purement cohomologique. D'abord, rappelons un résultat de formation de classes:

PROPOSITION 1: (Kawada) *Soit H un pro- p -groupe. Pour tout sous-groupe ouvert U de H , posons $A(U) = U/[U, U]$. Les conditions suivantes sont équivalentes:*

(i) *la dimension cohomologique stricte de H est 2 (H est "malléable" dans la terminologie de [9]).*

(ii) *pour tout couple de sous-groupes ouverts $V \triangleleft U$, on a: $H^1(U/V, A(V)) = 0$, $H^2(U/V, A(V)) \simeq \mathbb{Z}/(U:V)$ et est engendré par la classe de cohomologie de l'extension $1 \rightarrow A(V) \rightarrow U/[V, V] \rightarrow U/V \rightarrow 1$.*

(iii) *pour tout couple de sous-groupes ouverts $V \triangleleft U$, le transfert induit un isomorphisme $A(U) \simeq (A(V))^{U/V}$.*

(iv) *pour tout couple de sous-groupes ouverts $V \triangleleft U$, pour tout $n \in \mathbb{Z}$, on a un isomorphisme $\hat{H}^{n-2}(U/V, \mathbb{Z}) \simeq \hat{H}^n(U/V, A(V))$ obtenu par cup-produit avec la classe de $H^2(U/V, A(V))$ associée à l'extension $1 \rightarrow A(V) \rightarrow U/[V, V] \rightarrow U/V \rightarrow 1$.*

PREUVE: pour les équivalences (i) \Leftrightarrow (ii) \Leftrightarrow (iii), voir [9], 2-3. L'équivalence (ii) \Leftrightarrow (iv) est un résultat bien connu de Tate ([29]). Q.E.D.

Un pro- p -groupe libre, ou un groupe de Demuškin, vérifient les conditions précédentes.

PROPOSITION 2: *Soit G un p -groupe fixé.*

Pour tout $\mathbb{Z}_p G$ -module A de type fini, les conditions suivantes sont équivalentes:

(i) *A est isomorphe à un module de pro-relations de G .*

(ii) *A est \mathbb{Z}_p -libre, et pour tout sous-groupe H de G , on a: $H^1(H, A) = 0$, $H^2(H, A) \simeq \mathbb{Z}/(H:1)$ et la restriction $H^2(G, A) \rightarrow H^2(H, A)$ est surjective.*

PREUVE: Un module de pro-relations est évidemment sans \mathbb{Z}_p -torsion. De plus, un pro- p -groupe libre est de dimension cohomolo-

gique stricte égale à 2, et (i) \Rightarrow (ii) d'après la proposition 1. Pour (ii) \Rightarrow (i), voir [14], Korollar 1–8. Q.E.D.

On peut aussi décrire complètement les modules de pro-relations de G par générateurs et relations: voir [2], pour G abélien, et [32] pour le cas général.

1.2 Catégorie d'extensions

Nous allons adapter à la situation qui nous occupe la théorie générale des catégories d'extensions ([8], §9). Soit toujours G un p -groupe. Soit Mod_G la catégorie des $\mathbb{Z}_p G$ -modules de type fini. Introduisons deux autres catégories associées à la catégorie Mod_G .

1.2.1 La catégorie \mathcal{G}

Par définition, c'est la catégorie des objets de Mod_G qui sont $H^2(G, \cdot)$ pointés. Plus précisément, les objets de \mathcal{G} sont les couples (A, ϵ) , où $A \in \text{Mod}_G$ et $\epsilon \in H^2(G, A)$. Un morphisme $\tilde{\alpha} : (A, \epsilon) \rightarrow (B, \eta)$ est un morphisme de $\mathbb{Z}_p G$ -modules $\alpha : A \rightarrow B$ tel que $\alpha^*(\epsilon) = \eta$, où $\alpha^* = H^2(G, \alpha)$. On vérifie sans difficulté que $\tilde{\alpha}$ est un épimorphisme (resp. un monomorphisme) si et seulement si α est un homomorphisme surjectif (resp. injectif). La somme de deux objets est définie par:

$$(A, \epsilon) \oplus (B, \eta) = (A \times B, (\epsilon, \eta)),$$

où

$$(\epsilon, \eta) \in H^2(G, A \times B) \simeq H^2(G, A) \times H^2(G, B).$$

Chacun des objets intervenant dans la somme sera appelé *facteur direct* de la somme.

La proposition suivante est essentielle pour la suite:

PROPOSITION 3: Soient $1 \rightarrow R \rightarrow F \rightarrow G \rightarrow 1$ une présentation libre de G , et χ la classe caractéristique associée à l'extension $1 \rightarrow R^{ab} \rightarrow F/[R, R] \rightarrow G \rightarrow 1$. L'objet (R^{ab}, χ) est un objet projectif de la catégorie \mathcal{G} .

PREUVE: Rappelons que dans une catégorie, un objet P est dit projectif si tout diagramme

$$\begin{array}{ccc} & & P \\ & \beta \text{ (pointillé)} & \downarrow \\ A_1 & \xrightarrow{\alpha} & A_2 \end{array}, \text{ où } \alpha \text{ est un épimor-}$$

phisme, peut être complété par un morphisme $\beta : P \rightarrow A_1$ (en pointillé).

En fait, il résulte immédiatement de la propriété universelle du pro- p -groupe libre que (R^{ab}, χ) est un objet libre de \mathcal{G} , en en sens évident ([8], 9-5). La projectivité en résulte. Q.E.D.

COROLLAIRE: *Soit un épimorphisme $(A, \epsilon) \rightarrow (R^{ab}, \chi)$. Alors (A, ϵ) est isomorphe à une somme $(R^{ab} \oplus B, (\chi, 0))$.*

PREUVE: Soit α l'homomorphisme surjectif $A \rightarrow R^{ab}$ sous-jacent, et soit $B = \text{Ker } \alpha$. Par la projectivité de (R^{ab}, χ) , il existe une suite exacte $0 \rightarrow R^{ab} \xrightarrow{\beta} A \xrightarrow{\gamma} B \rightarrow 0$ telle que $\beta^*(\chi) = \epsilon$, où $\beta^* = H^2(G, \beta)$. On en déduit la suite exacte de cohomologie: $\dots \rightarrow H^2(G, R^{ab}) \xrightarrow{\beta^*} H^2(G, A) \xrightarrow{\gamma^*} H^2(G, B) \rightarrow \dots$, d'où $\gamma^*(\epsilon) = \gamma^*\beta^*(\chi) = 0$. Q.E.D.

1.2.2. La catégorie \mathcal{F}

C'est la sous-catégorie pleine de \mathcal{G} dont les objets sont les couples (A, ϵ) tels que l'extension $1 \rightarrow A \rightarrow E \rightarrow G \rightarrow 1$ associée à ϵ vérifie $d(E) = d(G)$. Autrement dit, A est contenu dans le sous-groupe de Frattini (topologique) de E .

PROPOSITION 4: *Soit toujours G un p -groupe de rang d .*

Soit (A, ϵ) un objet de \mathcal{G} . Les conditions suivantes sont équivalentes:

- (i) (A, ϵ) est un objet de \mathcal{F} .
- (ii) (A, ϵ) est une image épimorphique de (R_d^{ad}, χ) .
- (iii) tout morphisme $(B, \eta) \rightarrow (A, \epsilon)$ est un épimorphisme.
- (iv) si $(A, \epsilon) \rightarrow (B, 0)$ est un épimorphisme, alors $B = 0$.

PREUVE: L'équivalence (i) \Leftrightarrow (ii) est évidente.

(i) \Rightarrow (iv): soit $(A, \epsilon) \rightarrow (B, 0)$ un épimorphisme. Sur les extensions de groupes associées cela veut dire qu'on a un diagramme commutatif:

$$\begin{array}{ccccccc}
 1 & \longrightarrow & A & \longrightarrow & E & \longrightarrow & G \longrightarrow 1 \\
 & & \sigma \downarrow & & \tau \downarrow & & \downarrow \\
 1 & \longrightarrow & B & \longrightarrow & H & \longrightarrow & G \longrightarrow 1
 \end{array}$$

où σ et τ sont des homomorphismes surjectifs. Comme H est une extension scindée (produit semi-direct), on a $d(H) > d(G)$ si $B \neq 0$: contradiction avec la surjectivité de τ .

(iv) \Rightarrow (iii): soit $\tilde{\alpha}: (A_1, \epsilon_1) \rightarrow (A, \epsilon)$ un morphisme. Soit $C = \text{Im } \alpha$, où α est l'homomorphisme sous-jacent. La suite exacte de $\mathbb{Z}_p G$ -modules $0 \rightarrow C \xrightarrow{\beta} A \xrightarrow{\gamma} A/C \rightarrow 0$ donne la suite exacte de cohomologie $\dots \rightarrow$

$H^2(G, C) \xrightarrow{\beta^*} H^2(G, A) \xrightarrow{\gamma^*} H^2(G, A/C) \rightarrow \dots$. Comme $\epsilon \in \text{Im } \beta^*$ par hypothèse, on a $\gamma^*(\epsilon) = 0$. Donc γ induit un morphisme $\tilde{\gamma}: (A, \epsilon) \rightarrow (A/C, 0)$. D'après (iv), on a alors $A/C = 0$ et $A = C$, ce qui montre que $\tilde{\alpha}$ est un épimorphisme.

(iii) \Rightarrow (ii): d'après la propriété universelle du pro- p -groupe libre (voir démonstration de la proposition 3), (A, ϵ) est une image épimorphique d'un objet de la forme (R^{ab}, χ) . Mais d'après le théorème 1, (R_d^{ab}, χ) est facteur direct de (R^{ab}, χ) . Donc il existe un morphisme $(R_d^{ab}, \chi) \rightarrow (A, \epsilon)$, qui est un épimorphisme d'après (iii). Q.E.D.

En langage des catégories, la proposition 4, (ii) signifie simplement que (R_d^{ab}, χ) est un recouvrement projectif de \mathcal{F} .

REMARQUE 1: Soit q une puissance de p . Tous les résultats de ce paragraphe restent valables en remplaçant \mathbb{Z}_p par \mathbb{Z}/q . Les nouveaux objets seront notés avec un indice (q): par exemple, $R_d^{ab}(q) = R_d^{ab} \otimes \mathbb{Z}/q$, $\chi(q)$ est la classe caractéristique associée, etc. . .

§2 Structure de $A(K)$, énoncé du théorème principal

Revenons à l'arithmétique. Soit k une extension de degré fini n de \mathbb{Q}_p . Nous ferons les conventions suivantes: une p -extension (resp. une pro- p -extension) de k est une extension galoisienne dont le groupe de Galois est un p -groupe (resp. un pro- p -groupe); le groupe de Galois de la pro- p -extension maximale $k(p)$ de k sera noté $G_k(p)$. Pour tout entier $n \geq 1$, soit μ_{p^n} le groupe des racines p^n -ièmes de l'unité. Posons $\mu_{p^\infty} = \bigcup \mu_{p^n}$, et $\mu_k = \mu_{p^\infty} \cap k^\times$. L'ordre de μ_k est appelé *indice d'irrégularité de k* . Le corps k est dit *régulier* si $\mu_k = (1)$, *irrégulier* sinon.

Soit K/k une p -extension, de groupe de Galois G , fixée une fois pour toutes. On pose $d = d(G)$. On se propose d'étudier le $\mathbb{Z}_p G$ -module $A(K) = \varprojlim K^\times / K^{xp^m}$.

2.1. Le cas régulier

Dans ce cas, d'après un résultat de Šafarevič ([24]), le groupe $G_k(p)$ est un pro- p -groupe libre F_{n+1} de rang $(n+1)$.

THÉORÈME 2: Si k est régulier, on a un isomorphisme de $\mathbb{Z}_p G$ -modules.

$$A(K) \xrightarrow{\sim} R_d^{ab} \times (\mathbb{Z}_p G)^{n+1-d}$$

PREUVE: Par le corps de classes, $A(K)$ est isomorphe au groupe de Galois de la pro- p -extension abélienne maximale de K , et ce dernier groupe, d'après le résultat de Šafarevič ([24]) est isomorphe à R_{n+1}^{ab} . Il n'y a plus qu'à appliquer le théorème 1. Q.E.D.

Comme on sait décrire explicitement R_d^{ab} par générateurs et relations ([32]), le problème est donc résolu dans le cas régulier.

2.2. Le cas irrégulier

Dans ce cas, $G_k(p)$ est un groupe de Demuškin ([5]) et la structure de $A(K)$ est beaucoup plus compliquée. Rappelons le théorème de Janssen-Wingberg ([14]).

THÉORÈME 3: *Supposons k irrégulier. Soit $\delta = 1$ si $\mu_K \subset N_{K/k}(K^\times)$ $K^{\times p}$, 0 sinon. Soit t la dimension du radical de $H^1(G, F_p)$ pour le symbole de Hilbert d'ordre p . Alors:*

(i) *soit $A(K) \simeq N \times (\mathbb{Z}_p G)^{n+2-(d+t)-\delta}$, où N est un $\mathbb{Z}_p G$ -module indécomposable, isomorphe à $(R_d^{ab} \times (\mathbb{Z}_p G)^{t+\delta})/\mathbb{Z}_p G$.*

(ii) *soit $A(K) \simeq R_d^{ab} \times M \times (\mathbb{Z}_p G)^{n+2-2d-\delta}$, où M est un $\mathbb{Z}_p G$ -module indécomposable, isomorphe à $(\mathbb{Z}_p G)^{d+\delta}/\mathbb{Z}_p G$.*

Dans le cas (i), on dira que l'extension K/k est de type totalement irrégulier; dans le cas (ii), de type quasi-régulier (voir justification plus loin).

REMARQUE 2: Les $\mathbb{Z}_p G$ -modules R_d^{ab} et $A(K)$ ont même cohomologie (d'après la proposition 1 par exemple). Il en résulte que si l'extension K/k est de type quasi-régulier, le $\mathbb{Z}_p G$ -module M est cohomologiquement trivial. Par ailleurs, M contient la \mathbb{Z}_p -torsion de $A(K)$ i.e. μ_K .

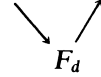
2.3. Le cas quasi-régulier

Le résultat principal de cet article est le théorème suivant, qui caractérise en termes de problème de plongement une extension de type quasi-régulier.

THÉORÈME 4: *Rappelons que $n = [k : \mathbb{Q}_p]$, $G = \text{Gal}(K/k)$, $d = d(G)$. Supposons k irrégulier. Soit q l'indice d'irrégularité de K . Les conditions suivantes sont équivalentes.*

(1) *l'extension K/k est de type quasi-régulier.*

(2) le problème de plongement $D_{n+2} \longrightarrow G = \text{Gal}(K/k)$, où D_{n+2} est le



groupe de Demuškin de rang $(n+2)$ et F_d le pro- p -groupe libre de rang d , possède une solution.

(3) tout problème de plongement $1 \rightarrow N \rightarrow E \rightarrow G = \text{Gal}(K/k) \rightarrow 1$, où N est un p -groupe tel que $d(E) = d(G)$, possède une solution.

(4) tout problème de plongement $1 \rightarrow A \rightarrow E \rightarrow G = \text{Gal}(K/k) \rightarrow 1$, où A est un p -groupe abélien tel que $d(E) = d(G)$, possède une solution.

(5) l'inclusion $\mu_K \rightarrow K^\times$ induit un homomorphisme $H^2(G, \mu_K) \rightarrow H^2(G, K^\times)$ qui est nul.

(6) μ_K est contenu dans un sous-module cohomologiquement trivial de $A(K)$.

(7) (R_d^{ab}, χ) est facteur direct de $(A(k), u)$, où χ est la classe caractéristique, et u la classe fondamentale de la théorie du corps de classes local.

(8) $(R_d^{ab}(q), \chi(q))$ est facteur direct de $(K^\times/K^{\times q}, u(q))$, où $u(q)$ est l'image par $H^2(G, K^\times) \rightarrow H^2(G, K^\times/K^{\times q})$ de la classe fondamentale.

Des cas particuliers seront examinés plus loin. La démonstration (qui n'est pas courte) se fera par étapes dans les paragraphes suivants. Mais tirons d'abord quelques conséquences immédiates.

Nous convenons d'appeler F_d -extension de k une extension galoisienne de k dont le groupe de Galois est isomorphe au pro- p -groupe libre à d générateurs. Pour $d = 1$, on retrouve la notion de Z_p -extension au sens d'Iwasawa ([11]).

COROLLAIRE 1: (on rappelle que $d = d(\text{Gal}(K/k))$).

Pour que l'extension K/k soit de type quasi-régulier, il faut et il suffit qu'elle se plonge dans une F_d -extension.

PREUVE: ce n'est qu'une autre formulation de la propriété 2).

REMARQUE 3: Il n'est pas vrai que pour un corps k quelconque, les propriétés (2) et (3) sont équivalentes. Supposons par exemple que k est un corps de nombres algébriques. On sait (en liaison avec la conjecture de Leopoldt) qu'il existe des extensions K/k cycliques de degré p t.q. K/k se plonge, pour tout entier m , dans une surextension cyclique de degré p^m , mais K/k ne se plonge pas dans une Z_p -extension. Par exemple, $k = Q(\mu_p)$, p irrégulier, où $k = Q(\sqrt{-3}, \sqrt{83})$, $p = 3$ (voir ([16])).

COROLLAIRE 2: (Comparer à [21], p. 83).

Soit K/k une p -extension cyclique de corps locaux p -adiques irréguliers. Pour que K/k se plonge dans une \mathbb{Z}_p -extension, il faut et il suffit que $\mu_k \subset N_{K/k}(K^\times)$.

PREUVE: Si G est cyclique, $H^2(G, \mu_K) = \mu_k/N_{K/k}(\mu_K)$ et $H^2(G, K^\times) = k^\times/N_{K/k}(K^\times)$. Il suffit alors d'appliquer l'équivalence (2) \Leftrightarrow (5). Q.E.D.

Pour d'autres relations avec la théorie d'Iwasawa, voir le §8.

COROLLAIRE 3: Soit K/k une p -extension de type quasi-régulier. Soit M/k une sous-extension galoisienne, contenue dans K . Alors les extensions M/k et K/M sont de type quasi-régulier.

PREUVE: On a $d_1 = d(\text{Gal}(M/k)) \leq d = d(\text{Gal}(K/k))$. Comme K/k se plonge dans une F_d -extension, il est clair que M/k se plonge dans une F_{d_1} -extension.

Soit $d_2 = d(\text{Gal}(K/M))$. On a une suite exacte $1 \rightarrow R_d \rightarrow F_d \rightarrow G \rightarrow 1$ et, en désignant par F_e l'image réciproque de $\text{Gal}(K/M)$ dans F_d , une suite exacte $1 \rightarrow R_d \rightarrow F_e \rightarrow \text{Gal}(K/M) \rightarrow 1$. Un sous-groupe fermé d'un pro- p -groupe libre étant libre, il est alors clair que K/M se plonge dans une F_{d_2} -extension. Q.E.D.

COROLLAIRE 4: Supposons que l'extension K/k est la translatée d'une extension K_0/k_0 de corps locaux réguliers (par exemple, $k = k_0(\mu_q)$ et $K = K_0(\mu_q)$). Alors K/k est de type quasi-régulier.

PREUVE: Comme k_0 est régulier, le groupe $G_{k_0}(p)$ est un pro- p -groupe libre. Il en résulte immédiatement que K_0/k_0 se plonge dans une F_d -extension. Par translation, il en est de même de K/k . Q.E.D.

Ce résultat justifie l'appellation de "quasi-régulier".

COROLLAIRE 5: Supposons l'extension K/k totalement ramifiée. Alors il existe une extension translatée K_1/k_1 que est de type quasi-régulier.

PREUVE: Soit k_1 une extension non ramifiée de k et soit $K_1 = k_1 \cdot K$. Comme toute extension non ramifiée s'obtient en ajoutant des racines de l'unité d'ordre premier à p , on a $\mu_{K_1} = \mu_K$. D'autre part, on a un diagramme commutatif,

$$\begin{array}{ccccc}
 H^2(G, \mu_K) & \xrightarrow{f} & H^2(G, K^\times) & \xrightarrow{\text{inv}} & \mathbb{Q}/\mathbb{Z} \\
 \parallel & & \downarrow & & \downarrow g \\
 H^2(G, \mu_{K_1}) & \xrightarrow{f_1} & H^2(G, K_1^\times) & \xrightarrow{\text{inv}} & \mathbb{Q}/\mathbb{Z}
 \end{array}$$

où inv est l'invariant (injectif) du corps de classes local et la flèche verticale g est la multiplication par le degré $[k_1:k]$. Comme $H^2(G, \mu_K)$ est d'exposant q , on peut choisir k_1 de façon que $[k_1:k] \equiv 0 \pmod{q}$ et annuler ainsi la flèche f_1 . Q.E.D.

Ce résultat sera utilisé dans [17].

§3 Équivalence des conditions (2) à (5), problème de plongement

Dans toute cette section, K/k est une p -extension de corps locaux p -adiques, et $G = \text{Gal}(K/k)$. Faisons quelques rappels sur le problème de plongement, mais uniquement dans le cadre qui nous occupe, c'est-à-dire essentiellement les pro- p -extensions.

3.1. Problème de plongement dont le noyau est un pro- p -groupe

Soit une extension de groupes $1 \rightarrow N \rightarrow E \rightarrow G \rightarrow 1$ dont le noyau N est un pro- p -groupe. On appelle problème de plongement $1 \rightarrow N \rightarrow E \rightarrow G = \text{Gal}(K/k) \rightarrow 1$ le problème de trouver une surextension galoisienne de corps L/k , contenant K , telle que le diagramme suivant soit commutatif:

$$\begin{array}{ccccccc}
 1 & \longrightarrow & N & \longrightarrow & E & \longrightarrow & G & \longrightarrow & 1 \\
 & & \downarrow \wr & & \downarrow \wr & & \downarrow \wr & & \\
 1 & \longrightarrow & \text{Gal}(L/K) & \longrightarrow & \text{Gal}(L/k) & \longrightarrow & \text{Gal}(K/k) & \longrightarrow & 1
 \end{array}$$

Si le noyau N est abélien, l'extension de groupes $1 \rightarrow N \rightarrow E \rightarrow G \rightarrow 1$ est décrite par une classes de cocycles $\epsilon \in H^2(G, N)$. Dans ce cas, on notera $(K/k, N, \epsilon)$ le problème de plongement précédent.

Une autre façon commode de présenter le problème est de considérer le triangle suivant:

$$\begin{array}{ccc}
 & G_k(p) & \\
 \tau \swarrow & \downarrow \sigma & \\
 E & \longrightarrow & G = \text{Gal}(K/k)
 \end{array}$$

où σ est la surjection canonique. Résoudre le problème de plongement, c'est trouver un homomorphisme *surjectif* τ qui rende le triangle commutatif.

Suivant la commodité, on emploiera l'une ou l'autre des trois formulations précédentes.

REMARQUE 4: Il est d'usage, dans l'étude du problème de plongement, de considérer les *solutions faibles* et les *solutions fortes*.

Une solution faible (resp. forte) est une solution qui est une algèbre galoisienne (resp. un corps qui est une extension galoisienne). Dans le triangle commutatif précédent, une solution faible (resp. forte) correspond à un homomorphisme τ non forcément surjectif (resp. surjectif). *Nous ne considérerons que des solutions fortes*. De toute façon, dans l'hypothèse $d(E) = d(G)$, il n'y a pas d'ambiguïté possible, car l'existence d'une solution faible entraîne alors l'existence d'une solution forte d'après la proposition 4, (iii).

3.2. Cas d'un noyau fini

Le problème se ramène à des noyaux cycliques d'après le résultat suivant:

THÉORÈME 5: (Demuškin-Šafarevič-Lur'e).

Soit K/k une p -extension de corps locaux p -adiques, de groupe de Galois G . Soit $1 \rightarrow N \rightarrow E \rightarrow G \rightarrow 1$ une extension de groupes où le noyau N est un p -groupe tel que $d(E) = d(G)$. Soit $\epsilon \in H^2(G, N^{ab})$ la classe de cohomologie associée à l'extension $1 \rightarrow N^{ab} \rightarrow E/[N, N] \rightarrow G \rightarrow 1$.

Les conditions suivantes sont équivalents:

(i) le problème de plongement $1 \rightarrow N \rightarrow E \rightarrow G = \text{Gal}(K/k) \rightarrow 1$ possède une solution.

(ii) le problème de plongement $(K/k, N^{ab}, \epsilon)$ possède une solution.

(iii) pour tout caractère $\varphi \in \text{Hom}_G(N^{ab}, K^\times)$, on a $\varphi^*(\epsilon) = 0$, où $\varphi^* = H^2(G, \varphi)$.

Dans le cas d'un noyau abélien, ce théorème a été démontré par Demuškin et Šafarevič ([6]; pour une démonstration cohomologique utilisant la dualité locale, voir [24]). Il a été étendu au cas d'un noyau non abélien par B.B. Lur'e ([18]).

3.3. Passage à un noyau infini

On pourrait dire qu'on "passe à la limite" sur les noyaux finis, mais il faut prendre quelques précautions (voir remarque 3).

PROPOSITION 5: Soit $N = \varprojlim N_i$, où les N_i sont des p -groupes. Soit $(P) 1 \rightarrow N \rightarrow E \rightarrow G = \text{Gal}(K/k) \rightarrow 1$ un problème de plongement qui est limite projective (en un sens évident) d'une suite de problèmes de plongement $(P_i) 1 \rightarrow N_i \rightarrow E_i \rightarrow G = \text{Gal}(K/k) \rightarrow 1$.

Si chaque problème (P_i) possède une solution, alors le problème (P) possède une solution.

PREUVE: (suggérée par J.P. Serre).

Par hypothèse, il existe, pour tout i , une surextension galoisienne L_i/k , contenant K , telle que le diagramme suivant soit commutatif:

$$\begin{array}{ccccccc}
 1 & \xrightarrow{\quad} & \text{Gal}(L_i/K) & \xrightarrow{\quad} & \text{Gal}(L_i/k) & \xrightarrow{\quad} & \text{Gal}(K/k) & \xrightarrow{\quad} & 1 \\
 & & \downarrow \wr & & \downarrow \wr & & \downarrow \wr & & \\
 1 & \xrightarrow{\quad} & N_i & \xrightarrow{\quad} & E_i & \xrightarrow{\quad} & G & \xrightarrow{\quad} & 1
 \end{array}$$

Soit S_i l'ensemble des solutions du problème (P_i) . Alors $S_i \neq \emptyset$, et S_i est fini d'après le lemme de Krasner. De plus, par l'hypothèse sur les (P_i) , chaque solution L_{i+1} de S_{i+1} contient une solution L_i de S_i . Les ensembles S_i forment donc un système projectif, les morphismes de liaison $f_i : S_{i+1} \rightarrow S_i$ étant définis de la façon suivante:

Pour tout $L_{i+1} \in S_{i+1}$, on pose $f_i(L_{i+1}) = L_i$, où L_i est un élément quelconque de S_i contenu dans L_{i+1} . Soit $S = \varprojlim S_i$. Alors $S \neq \emptyset$ d'après le lemme bien connu (Bourbaki, Topol. Gén., chap. I, Appendice, th. 1):

LEMME 1: Une limite projective d'ensembles finis non vides est non vide.

Tout élément L de S est alors solution du problème de plongement (P) . Q.E.D.

Pour le cas d'un noyau infini abélien, voir plus loin propo. 6.

3.4. Preuve des équivalences (2) à (5)

(2) \Rightarrow (3): d'après la propriété universelle du pro- p -groupe libre.

(3) \Rightarrow (2): soit F le pro- p -groupe libre de rang d . Soit F^i une suite descendante de sous-groupes ouverts tels que $d(F/F^i) = d$ et $F = \varprojlim F/F^i$ (par exemple, la suite des sous-groupes de Frattini successifs). On applique alors la proposition 5 en prenant $N_i = F/F^i$.

(3) \Leftrightarrow (4) \Leftrightarrow (5) d'après le théorème 4: en effet, pour tout G -caractère d'un groupe abélien fini à valeurs dans K^\times , $\text{Im } \varphi$ est un groupe de

racines de l'unité. De plus, si $\mu_r \subset \mu_q$ la nullité de $H^2(G, \mu_q) \rightarrow H^2(G, K^\times)$ entraîne évidemment celle de $H^2(G, \mu_r) \rightarrow H^2(G, K^\times)$. Q.E.D.

§4 Équivalence des propriétés restantes, le pro- p -groupe de Weil

K/k désigne toujours une p -extension de groupe de Galois G . Soit u la classe fondamentale de $H^2(G, K^\times) = H^2(G, A(K))$. On appellera *pro- p -groupe de Weil* (sous-entendu relativement à K/k) l'objet $(A(K), u)$ de la catégorie \mathcal{G} .

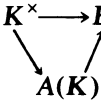
4.1. Un autre point de vue sur le problème de plongement

On se limite ici aux noyaux *abéliens*. On considèrera donc les problèmes de plongement de la forme $(K/k, B, \epsilon)$ où $(B, \epsilon) \in \mathcal{G}$.

PROPOSITION 6: *Pour tout $(B, \epsilon) \in \mathcal{G}$, le problème de plongement $(K/k, B, \epsilon)$ possède une solution si et seulement si (B, ϵ) est une image épimorphique de $(A(K), u)$ dans \mathcal{G} .*

PREUVE:

(a) Supposons d'abord B fini. Si le problème de plongement $(K/k, B, \epsilon)$ possède une solution L , soit N la norme $N_{L/K}$. Par le corps de classes, on a une suite exacte $1 \rightarrow NL^\times \rightarrow K^\times \rightarrow B = \text{Gal}(L/K) \rightarrow 1$, et d'après le théorème de Šafarevič-Weil ([1], chap. 14), la projection $\pi: K^\times \rightarrow B$ induit un homomorphisme $\pi^*: H^2(G, K^\times) \rightarrow H^2(G, B)$ tel que $\pi^*(u) = \epsilon$. Comme B est un p -groupe, π se factorise à travers $A(K)$, i.e. on a un diagramme commutatif $K^\times \rightarrow B$, et (B, ϵ) est bien



une image épimorphique de $(A(K), u)$ dans \mathcal{G} .

La réciproque est évidente.

(b) Le passage à un noyau infini se fait de la même façon que dans la proposition 5. Q.E.D.

4.2. Équivalence de (4) et (7)

D'après la proposition 6, la propriété (4) équivaut à dire que tout objet (B, ϵ) de la catégorie \mathcal{F} est une image épimorphique de $(A(K), u)$. Mais tout objet de \mathcal{F} est une image épimorphique de (R_d^{ab}, χ) . Donc (4) équivaut à dire que (R_d^{ab}, χ) est une image épimor-

phique (donc un facteur direct, d'après le corollaire à la propo. (3) de $(A(K), u)$). Q.E.D.

4.3. Équivalence de (1) et (6), de (1) et (7)

(a) Supposons (1). Alors le module M (notation du théorème 3) contient la \mathbb{Z}_p -torsion de $A(K)$, i.e. μ_K , et est cohomologiquement trivial. (voir remarque 2). Donc $(1) \Rightarrow (6)$. Mais $(6) \Rightarrow (5) \Leftrightarrow (4) \Leftrightarrow (7) \Rightarrow (1)$.

(b) Evidemment $(7) \Rightarrow (1)$. Mais on a vu dans (a) que $(1) \Rightarrow (7)$. Q.E.D.

4.4. Équivalence de (5) et (8)

Rappelons que $\mu_q = \mu_K$. Il est clair, d'après la théorème de Demuškin-Šafarevič-Lur'e, que la propriété (5) est équivalente à la propriété suivante:

4(q) Tout problème de plongement $1 \rightarrow A \rightarrow E \rightarrow G \rightarrow 1$, où A est p -groupe abélien d'exposant q , tel que $d(E) = d(G)$, possède une solution.

Il nous reste donc à montrer $4(q) \Leftrightarrow (8)$. Mais cette équivalence n'est autre que la "q-version" de l'équivalence $(4) \Leftrightarrow (7)$, où l'on remplace \mathbb{Z}_p par \mathbb{Z}/q , (R_d^{ab}, χ) par $(R_d^{ab}(q), \chi(q))$ et $(A(K), u)$ par $(K^\times/K^{\times q}, u(q))$ (notations de la remarque 1). Q.E.D.

Le théorème principal est ainsi démontré.

§5 Cas particulier où $G = \text{Gal}(K/k)$ est abélien

Dans ce cas, nous allons voir que les conditions équivalentes du théorème 4 se reflètent dans des propriétés du corps de base k (ce qui est bien dans la philosophie du corps de classes). Dans toute cette section, on supposera que K/k est une p -extension abélienne de corps locaux irréguliers, avec $G = \text{Gal}(K/k)$ et $d = d(G)$. On fera l'hypothèse supplémentaire que $\mu_k \neq \{\pm 1\}$. Cela entraîne que le degré $n = [k : \mathbb{Q}_p]$ est pair.

5.1. Réduction au cas d'égale irrégularité

Nous allons, par une série de lemmes, nous remener au cas où $\mu_k = \mu_K$. Suivant Iwasawa ([12]), nous dirons qu'une p -extension abélienne \tilde{K}/k est cyclotomiquement scindée si $\tilde{K} = k(\mu_{\tilde{K}})$. $L, L \cap$

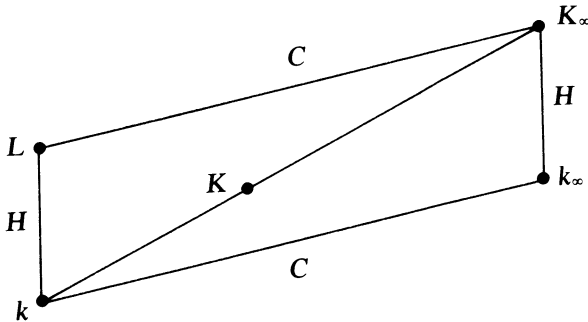
$k(\mu_{\bar{k}}) = k$, et nous chercherons à plonger toute p -extension abélienne K/k dans une surextension abélienne \tilde{K}/k cyclotomiquement scindée.

LEMME 2: *Toute p -extension abélienne K/k de corps locaux p -adiques irréguliers se plonge dans une p -extension abélienne \tilde{K}/k cyclotomiquement scindée, où \tilde{K} est une extension cyclotomique de K (i.e. $\tilde{K} = K(\mu_{\bar{k}})$), et les groupes de Galois de \tilde{K}/k et K/k ont même exposant.*

PREUVE-(d'après F. Laubie):

Soient $k_{\infty} = k(\mu_{\infty})$ et $K = K(\mu_{\infty})$ les extensions cyclotomiques absolues de k et K . L'extension K_{∞}/k est abélienne, et k_{∞}/k est une \mathbb{Z}_p -extension puisque $\mu_k \neq \{\pm 1\}$. D'après [12], lemme 4, on a alors une suite exacte scindée $1 \rightarrow H = \text{Gal}(K_{\infty}/k_{\infty}) \rightarrow \text{Gal}(K_{\infty}/k) \rightarrow C = \text{Gal}(k_{\infty}/k) \rightarrow 1$.

Il existe donc une extension abélienne L/k , de groupe de Galois isomorphe à H , telle que $K_{\infty} = k_{\infty} \cdot L$ et $k_{\infty} \cap L = k$



Soit N le sous-groupe de $\text{Gal}(k_{\infty}/k)$ correspondant à la projection de $\text{Gal}(K_{\infty}/K)$ sur $\text{Gal}(k_{\infty}/L)$. Soit \tilde{k} le sous-corps de k laissé fixé par N . Il suffit alors de prendre $\tilde{K} = L \cdot \tilde{k}$. Par construction, H et $\text{Gal}(\tilde{k}/k)$ sont tués par l'exposant de $\text{Gal}(K/k)$. Donc $\text{Gal}(\tilde{K}/k)$ et $\text{Gal}(K/k)$ ont même exposant. Q.E.D.

LEMME 3: *Soit \tilde{K}/K une extension cyclotomique, i.e. $\tilde{K} = K(\mu_{\bar{k}})$. Alors le $\text{Gal}(\tilde{K}/K)$ -module $\mu_{\bar{k}}$ est cohomologiquement trivial.*

PREUVE: voir par exemple [21], p. 81.

LEMME 4: *Conservons les hypothèses et les notations de la démonstration du lemme 2. Alors les trois extensions K/k , \tilde{K}/k et L/k sont simultanément de type quasi-régulier ou de type totalement irrégulier.*

PREUVE: Soient $\tilde{G} = \text{Gal}(\tilde{K}/k)$, $N = \text{Gal}(\tilde{K}/L)$, $H = \text{Gal}(L/k)$ (notations du lemme 2). On a un diagramme commutatif:

$$\begin{array}{ccccccc} H^2(H, \mu_L) & \xrightarrow{\sim} & H^2(\tilde{G}, \mu_{\tilde{K}}) & & & & \\ \downarrow & & \downarrow & & & & \\ 0 \longrightarrow & H^2(H, L^\times) \longrightarrow & H^2(\tilde{G}, \tilde{K}^\times) \longrightarrow & H^2(N, \tilde{K}^\times) \longrightarrow & 0 \end{array}$$

où l'isomorphisme de la première ligne résulte du lemme 3 et de l'inflation-restriction, et la suite exacte de la seconde ligne est celle du corps de classes local. Donc, d'après le théorème (4, 5), les extensions \tilde{K}/k et L/k sont simultanément de type quasi-régulier ou totalement irrégulier. De même, puisque \tilde{K} est une extension cyclotomique de K , les extensions \tilde{K}/k et K/k sont simultanément de type quasi-régulier ou totalement irrégulier. Q.E.D.

Donnons maintenant une condition de quasi-régularité pour une extension cyclotomiquement scindée.

LEMME 5: On conserve les notations du lemme 4. Soit $\tilde{G} = \text{Gal}(\tilde{K}/k)$. L'extension \tilde{K}/k est de type quasi-régulier si et seulement si l'application $H^2(\tilde{G}, \mu_k) \rightarrow H^2(\tilde{G}, \tilde{K}^\times)$ est nulle.

PREUVE: De même que dans la preuve du lemme 4, on a un diagramme commutatif:

$$\begin{array}{ccc} H^2(H, \mu_k) & \xrightarrow{\text{inf}} & H^2(\tilde{G}, \mu_k) \\ \downarrow & & \downarrow \\ 0 \longrightarrow & H^2(H, L^\times) \xrightarrow{\text{inf}} & H^2(\tilde{G}, \tilde{K}^\times) \end{array}$$

Donc la nullité de la flèche $H^2(\tilde{G}, \mu_k) \rightarrow H^2(\tilde{G}, \tilde{K}^\times)$ entraîne celle de $H^2(H, \mu_k) \rightarrow H^2(H, L^\times)$, c-à-d. la quasi-régularité de l'extension L/k (théo. (4, 5)), c-à-d. la quasi-régularité de l'extension \tilde{K}/k .

Réciproquement, si l'extension \tilde{K}/k est quasi-régulière, tout problème de plongement avec le noyau μ_k admet une solution, donc l'application $H^2(\tilde{G}, \mu_k) \rightarrow H^2(\tilde{G}, \tilde{K}^\times)$ est nulle. Q.E.D.

On s'est ainsi ramené au cas où le groupe abélien G opère trivialement sur les racines de l'unité.

5.2. Rappels sur la cohomologie d'un groupe abélien

Le groupe abélien G opérant trivialement sur un module A , la structure de $H^2(G, A)$ est bien connue.

PROPOSITION 7: (voir [28], [34]).

Soit G un groupe abélien opérant trivialement sur un groupe abélien A . Alors:

(i) $H^2(G, A)$ est engendré par $H^2(G, A)_{ab}$ et $H^2(G, A)_{\text{symp}}$, où $H^2(G, A)_{ab}$ est le sous-groupe des classes représentées par des cocycles symétriques ($\alpha(\sigma, \tau) = \alpha(\tau, \sigma)$) et $H^2(G, A)_{\text{symp}}$ est le sous-groupe des classes représentées par des formes bilinéaires symplectiques ($\alpha(\sigma, \sigma) = 0$). Les classes de $H^2(G, A)_{ab}$ correspondent aux extensions de G par A qui sont des groupes abéliens.

(ii) Soit $G = H_1 \times \cdots \times H_d$ une décomposition de G en produit de groupes cycliques H_i d'ordres h_i . Alors $H^2(G, A)_{ab} \simeq \prod_{i=1}^d H^2(H_i, A)$ et $H^2(G, A)_{\text{symp}} \simeq \prod_{1 \leq i < j \leq d} \text{Symp}(H_i, H_j; A)$, où $\text{Symp}(H_i, H_j; A)$ désigne le groupe des applications bilinéaires symplectiques de $H_i \times H_j$ dans A .

COROLLAIRE: Soit $G = H_1 \times \cdots \times H_d$ une décomposition de G en groupes cycliques H_i d'ordres h_i . Pour tout entier r , le groupe $H^2(G, \mathbb{Z}/p^r)$ est engendré par les images des applications $H^2(H_i, \mathbb{Z}/p^r) \xrightarrow{\text{inf}} H^2(G, \mathbb{Z}/p^r)$ et $H^1(H_i, \mathbb{Z}/p^{r_{ij}}) \times H^1(H_j, \mathbb{Z}/p^{r_{ij}}) \rightarrow H^1(G, \mathbb{Z}/p^{r_{ij}}) \xrightarrow{U} H^2(G, \mathbb{Z}/p^{r_{ij}}) \rightarrow H^2(G, \mathbb{Z}/p^r)$ où $1 \leq i \leq d$, $1 \leq i < j \leq d$, inf désigne l'inflation, U le cup-produit, et $p^{r_{ij}} = \text{pgcd}(p^r, h_i, h_j)$.

PREUVE: Cela résulte immédiatement de la proposition 7, (ii) et de la bilinéarité et de l'anti-commutativité de cup-produit. Q.E.D.

5.3. Relations avec le symbole de Hilbert

Nous pouvons maintenant énoncer les propriétés équivalentes du théorème 4 en termes de symbole de Hilbert.

THÉORÈME 6: Soit K/k une p -extension abélienne de corps locaux p -adiques irréguliers, de groupe de Galois G . Soit p^r l'indice d'irrégularité de k , i.e. $\mu_{p^r} = \mu_k$. Soit p^s le minimum de p^r et de l'exposant de G . Pour tout $h \leq s$, soit \mathcal{K}_h le sous- \mathbb{Z}/p^h -module de $k^\times/k^{\times p^h}$ correspondant par la théorie de Kummer à G/G^{p^h} , i.e. à la sous-extension abélienne maximale d'exposant p^h . Alors les conditions du théorème 4 sont équivalentes à la condition:

(9) $\mu_{p^r} \subset N_{K/k}(K^\times)$ et le \mathbb{Z}/p^h -module \mathcal{K}_h est totalement isotrope pour le symbole de Hilbert d'ordre p^h , pour tout $h \leq s$.

Il n'est pas difficile de voir que les extensions K et \tilde{K} (lemme 2) vérifient ou ne vérifient pas simultanément la condition 9 (l'entier s est le même pour ces deux extensions). En vertu des lemmes 4 et 5,

on peut supposer que l'extension K/k est cyclotomiquement scindée. Il suffit alors de traduire la condition de nullité de l'application $H^2(G, \mu_k) \rightarrow H^2(G, K^\times)$:

Soit D le groupe de Galois de la pro- p -extension maximale $k(p)$ de k . On a un diagramme commutatif:

$$\begin{array}{ccc}
 & & 0 \\
 & & \downarrow \\
 H^2(G, \mathbb{Z}/p^r) & \longrightarrow & H^2(G, K^\times) \\
 \text{inf} \downarrow & & \downarrow \text{inf} \\
 0 & \longrightarrow & H^2(D, \mathbb{Z}/p^r) \longrightarrow H^2(D, k^\times(p))
 \end{array}$$

où la ligne exacte du bas provient de la suite exacte de Kummer $1 \rightarrow \mu_{p^r} \rightarrow k^\times(p) \xrightarrow{p^r} k^\times(p) \rightarrow 0$. La condition (5) du théorème 4 équivaut ainsi à la nullité de l'inflation $H^2(G, \mathbb{Z}/p^r) \rightarrow H^2(D, \mathbb{Z}/p^r)$.

La nullité de l'application $H^2(G, \mathbb{Z}/p^r)_{ab} \rightarrow H^2(D, \mathbb{Z}/p^r)$ équivaut, d'après la propo. 7, (ii) et le corollaire 2 du théo. 4, à la condition $\mu_r \subset N_{K/k}(K^\times)$. Il reste à regarder la nullité de $H^2(G, \mathbb{Z}/p^r)_{\text{symp}} \rightarrow H^2(D, \mathbb{Z}/p^r)$. En reprenant les notations du corollaire de la propo. 7, on a un diagramme commutatif:

$$\begin{array}{ccccccc}
 H^1(H_i, \mathbb{Z}/p^{r_i}) \times H^1(H_j, \mathbb{Z}/p^{r_j}) & \xrightarrow{\text{inf} \times \text{inf}} & H^1(G, \mathbb{Z}/p^{r_i}) \times H^1(G, \mathbb{Z}/p^{r_j}) & \xrightarrow{\sim} & H^2(G, \mathbb{Z}/p^{r_i}) & \rightarrow & H^2(G, \mathbb{Z}/p^r) \\
 \downarrow \text{inf} \times \text{inf} & & \downarrow \text{inf} \times \text{inf} & & \downarrow \text{inf} & & \downarrow \text{inf} \\
 H^1(D, \mathbb{Z}/p^{r_i}) \times H^1(D, \mathbb{Z}/p^{r_j}) & \xrightarrow{\sim} & H^1(D, \mathbb{Z}/p^{r_i}) \times H^1(D, \mathbb{Z}/p^{r_j}) & \xrightarrow{\sim} & H^2(D, \mathbb{Z}/p^{r_i}) & \rightarrow & H^2(D, \mathbb{Z}/p^r)
 \end{array}$$

Mais l'on sait que $H^2(D, \mathbb{Z}/p^{r_i}) \simeq \mathbb{Z}/p^{r_i}$ et $H^2(D, \mathbb{Z}/p^r) \simeq \mathbb{Z}/p^r$. La nullité de l'application composée $H^1(H_i, \mathbb{Z}/p^{r_i}) \times H^1(H_j, \mathbb{Z}/p^{r_j}) \rightarrow H^2(D, \mathbb{Z}/p^r)$ est donc équivalente à la nullité de l'application composée $H^1(H_i, \mathbb{Z}/p^{r_i}) \times H^1(H_j, \mathbb{Z}/p^{r_j}) \rightarrow H^2(D, \mathbb{Z}/p^{r_i})$. La traduction en termes de symbole de Hilbert est aisée, et achève la démonstration du théorème. Q.E.D.

COROLLAIRE 1: *Supposons G abélien d'exposant p^r . Alors la condition (9) est vérifiée si et seulement si le \mathbb{Z}/p^h -module de $k^\times/k^{\times p^h}$ engendré par \mathcal{K}_h et μ_{p^h} est totalement isotrope, pour tout $h \leq r$.*

PREUVE: C'est immédiat. On a ainsi retrouvé un résultat de J. Sonn ([27], th. 7).

COROLLAIRE 2: (voir aussi [27], p. 178).

Pour qu'un pro- p -groupe libre F_d de rang d , soit quotient d'un groupe de Demuškin D_{n+2} , de rang $n+2$, il faut et il suffit que $d \leq n/2 + 1$.

PREUVE: Si F_d est quotient de D_{n+2} , on peut réaliser n'importe quel p -groupe G de rang d comme groupe de Galois d'une p -extension K/k , et cette extension est de type quasi-régulier d'après le théorème 4. Alors $d \leq n/2 + 1$ d'après la condition (9).

Réciproquement, $d \leq n/2 + 1$. Le groupe de Demuškin est engendré par x_1, \dots, x_{n+2} et la relation $x_1^{p'}[x_1, x_2] \dots [x_{n+1}, x_{n+2}] = 1$. Soit y_1, \dots, y_d une base de F_d . On peut définir un épimorphisme $\varphi: D_{n+2} \rightarrow F_d$ par $\varphi(x_{2i}) = y_i$ pour $1 \leq i \leq d$ et $\varphi(x_{2i-1}) = 1$ pour tout autre i . Q.E.D.

§6 Cas d'égalité irrégularité, catégorie des extensions centrales

L'étude du cas abélien a mis en évidence l'importance du cas d'une extension K/k d'égalité irrégularité, i.e. vérifiant $\mu_k = \mu_K$. Pour illustrer la méthode catégorielle adoptée dans ce travail, nous allons examiner le cas d'une extension d'égalité irrégularité, mais non nécessairement abélienne.

6.1. Catégorie des extensions centrales

Soit G un p -groupe fixé (non nécessairement abélien). Introduisons une sous-catégorie \mathcal{G}_0 de la catégorie \mathcal{G} définie au §1: les objets en seront les couples (A, ϵ) de \mathcal{G} où G opère trivialement sur A . De même, nous définissons une sous-catégorie \mathcal{F}_0 de la catégorie \mathcal{F} . Le résultat suivant est immédiat:

PROPOSITION 8: Soit $1 \rightarrow R \rightarrow F \rightarrow G \rightarrow 1$ une présentation libre de G . Soit χ_0 la classe de cohomologie de l'extension $1 \rightarrow R/[R, F] \rightarrow F/[R, F] \rightarrow G \rightarrow 1$. Alors $(R/[R, F], \chi_0)$ est un objet projectif de la catégorie \mathcal{G}_0 .

Comme $R/[R, F]$ est un quotient de R^{ab} , on en déduit:

COROLLAIRE: Si $1 \rightarrow R_d \rightarrow F_d \rightarrow G \rightarrow 1$ est une présentation minimale de G ($d = d(G)$), alors $(R_d/[R_d, F_d], \chi_0)$ est un objet projectif de la catégorie \mathcal{F}_0 .

6.2. Cas d'égalité irrégularité

Dans ce cas, les conditions du théorème 4 équivalent à une propriété portant seulement sur un quotient de $A(K)$.

PROPOSITION 9: Soit K/k une p -extension de corps locaux p -adiques irréguliers, de groupe de Galois G . On suppose que $\mu_k = \mu_K$. Alors les conditions du théorème 4 sont équivalentes à la condition:

(10) $(H_0(G, R_a^{ab}), \chi_0)$ est facteur direct de $(H_0(G, A(K)), u_0)$, où u_0 est l'image de la classe fondamentale induite par $A(K) \rightarrow A(K)/I_G A(K)$.

PREUVE: remarquons d'abord que $R/[R, F] = H_0(G, R^{ab}) = R^{ab}/I_G R^{ab}$, où I_G est l'idéal d'augmentation de l'algèbre $\mathbb{Z}_p G$.

D'après le théorème de Demuškin–Šafarevič–Lur'e, la nullité de $H^2(G, \mu_k) \rightarrow H^2(G, K^\times)$ équivaut à l'existence d'une solution pour tout problème de plongement $1 \rightarrow N \rightarrow E \rightarrow G = \text{Gal}(K/k) \rightarrow 1$ où N est un noyau G -trivial et $d(E) = d(G)$. Mais, puisque $\mu_k = \mu_K$, cela équivaut aussi, d'après le théorème 4, à la quasi-régularité de l'extension K/k . Les mêmes raisonnements que pour le théorème 4 permettent alors d'affirmer l'équivalence avec la condition (10). Q.E.D.

Il serait intéressant, pour les problèmes de ramification, de connaître la structure du $\mathbb{Z}_p G$ -module $H_0(G, A(K))$ filtré (voir [19]).

RAMARQUE 5: On pourrait également adapter la méthode catégorielle précédente à l'étude des " \mathbb{Z}_p -extensions multiples". Plus précisément: trouver une condition nécessaire et suffisante pour qu'une p -extension abélienne K/k se plonge dans une extension de groupe de Galois isomorphe à $\mathbb{Z}_p \times \cdots \times \mathbb{Z}_p$ (i.e. est un pro- p -groupe abélien libre). Il faut considérer la catégorie des $\mathbb{Z}_p G$ -modules triviaux pointés par $H^2(G, \cdot)_{ab}$ et chercher, comme précédemment, un objet projectif. Nous espérons y revenir dans un article ultérieur.

§7 Modules symplectiques

Etant donnée une extension K/k de type quasi-régulier, on se propose maintenant de déterminer la structure du module M (notations du théorème 3) qui intervient dans la décomposition de $A(K)$. Nous obtiendrons une réponse complète modulo q , où q est l'indice d'irrégularité de K . Dans toute cette section, nous supposons $p \neq 2$, afin d'utiliser la théorie des modules symplectiques développée par A.V. Jakovlev ([13]). Rappelons-en les principales définitions et propriétés, mais uniquement dans le cadre restreint qui nous intéresse.

7.1. Décomposition d'un module symplectique

Soit D un anneau commutatif noethérien. Supposons que D possède un idéal J tel que D/J vérifie la condition de chaîne descendante

sur les idéaux, et D est complet pour la J -topologie. On a alors le théorème dit "de Krull-Schmidt".

THÉORÈME 7: (voir [8], 10-2)

Soit G un groupe fini. Tout DG -module de type fini se décompose en somme directe de sous-modules indécomposables, et cette décomposition est unique à l'ordre et l'isomorphisme près des facteurs.

Supposons en outre que DG est muni d'un anti-automorphisme involutif tel que pour tous $x, y \in DG$, pour tout $\alpha \in D$, on ait: $(x + y)^* = x^* + y^*$, $(\alpha x)^* = \alpha x^*$, $(xy)^* = y^* x^*$. L'existence d'un tel anti-automorphisme permet de définir, pour tout DG -module X , une structure de DG -module sur $\text{Hom}_D(X, D)$ en posant:

$$\forall \varphi \in \text{Hom}_D(X, D), \quad \forall x \in DG, \quad \forall a \in X, \quad (x \cdot \varphi)(a) = \varphi(x^* \cdot a)$$

AVERTISSEMENT: Cette action n'est pas l'action habituelle sur le dual, qui est définie par:

$$(\sigma\varphi)(a) = \sigma(\varphi(\sigma^{-1}(a))) \quad \forall \sigma \in G.$$

Un DG -module symplectique S est un DG -module muni d'une forme bilinéaire antisymétrique non dégénérée $\langle \cdot, \cdot \rangle$ à valeurs dans D et vérifiant la propriété:

$$\forall x \in DG, \quad \forall m, n \in S, \quad \langle x \cdot m, n \rangle = \langle m, x^* \cdot n \rangle.$$

On a les notions habituelles d'orthogonalité, de somme directe orthogonale, etc. . . Un sous-module T d'un DG -module symplectique est appelé *sous-module symplectique* si la restriction de la forme bilinéaire à $T \times T$ en fait un module symplectique; *sous-module totalement isotrope* si la restriction est nulle. Un module symplectique est appelé *module hyperbolique* s'il est somme directe de deux sous-modules totalement isotropes *indécomposables*.

THÉORÈME 8: (voir [13], pp. 341 et 345).

Soit G un p -groupe. Supposons que l'idéal J de D contient p . Soit S un DG -module symplectique de type fini, uniquement divisible par 2. Alors S se décompose en somme directe orthogonale de sous-modules symplectiques indécomposables et de sous-modules hyperboliques.

EXEMPLE: K/k est une p -extension de corps locaux irréguliers;

$G = \text{Gal}(K/k)$, $D = \mathbb{Z}/q$, où q est l'indice d'irrégularité de K ; $S = K^\times/K^{\times q}$; $\langle ., . \rangle$ est le symbole de Hilbert d'ordre q ; l'involution de DG est induite par l'application: $\sigma \in G \rightarrow \mathcal{K}(\sigma)\sigma^{-1}$, où \mathcal{K} est le caractère de G défini par l'action de G sur μ_q .

7.2. Décomposition de $A(K)$ modulo q

Soit K/k une p -extension de type quasi-régulier de groupe de Galois G . Alors (théorème 3):

$$A(K) \xrightarrow{\sim} R_d^{ab} \times M \times (\mathbb{Z}_p G)^{n+2-2d-\delta} \quad (d = d(G)).$$

THÉORÈME 9: Soit K/k une p -extension de type quasi-régulier, de groupe de Galois G . Soit $\mu_q = \mu_K$. Pour tout entier r divisant q , on a un isomorphisme de $\mathbb{Z}/r[G]$ -modules:

$$K^\times/K^{\times r} \xrightarrow{\sim} (R_d^{ab} \otimes \mathbb{Z}/r) \times \text{Hom}(R_d^{ab}, \mu_r) \times (\mathbb{Z}/r[G])^{n+2-2d-\delta}.$$

(ici l'action sur Hom est l'action habituelle).

PREUVE: nous ferons seulement la démonstration pour q , la démonstration pour $r|q$ étant exactement pareille.

On a deux décompositions du $\mathbb{Z}/q[G]$ -module $K^\times/K^{\times q}$ en facteurs indécomposables:

$$(1) \quad K^\times/K^{\times q} \xrightarrow{\sim} (R_d^{ab} \otimes \mathbb{Z}/q) \times (M \otimes \mathbb{Z}/q) \times \mathbb{Z}/q[G]^{n+2-2d-\delta}$$

et

$$(2) \quad K^\times/K^{\times q} \xrightarrow{\sim} \left(\bigoplus_i S_i\right) \oplus \left(\bigoplus_j H_j\right),$$

où les S_i sont des sous-modules symplectiques indécomposables et chaque H_j est somme directe de deux sous-modules totalement isotropes indécomposables H'_j et H''_j . D'après le théorème de Krull-Schmidt, il y a isomorphisme (à l'ordre près) entre les facteurs indécomposables de ces deux décompositions. Or:

(a) $(R_d^{ab} \otimes \mathbb{Z}/q)$ est indécomposable (voir par exemple [20]). S'il pouvait être muni d'une structure de module symplectique, il serait G -isomorphe à $\text{Hom}(R_d^{ab}, \mu_q)$ donc aurait même cohomologie, ce qui ne se produit pas ([20], corol. 1.7 et 1.8). Donc $R_d^{ab} \otimes \mathbb{Z}/q$ est isomorphe à un facteur H'_j ou H''_j de la décomposition (2).

(b) $\mathbb{Z}/q[G]$ ne peut pas être non plus un sous-module symplectique,

car G est d'ordre impair ($p \neq 2$). Donc $Z/q[G]$ est isomorphe à un facteur H'_j ou H''_j .

(c) Il reste à regarder le facteur $M \otimes Z/q$.

– si $\delta = 0$: comme n est pair ($p \neq 2$), $n + 2 - 2d$ est pair, et le facteur $Z/q[G]^{n+2-2d}$ est isomorphe à une somme directe de sous-modules hyperboliques. Il en résulte que $M \otimes Z/q$ est isomorphe à un sous-module totalement isotrope, indécomposable, dont la somme directe avec $R_d^{ab} \otimes Z/q$ forme un module hyperbolique. Donc, en tant que groupe, $M \otimes Z/q$ est isomorphe à $\text{Hom}(R_d^{ab}, Z/q)$. Mais, par définition même de l'action de G (voir l'avertissement et l'exemple au début de cette section), $M \otimes Z/q$ est isomorphe, en tant que $Z/q[G]$ -module, à $\text{Hom}(R_d^{ab}, \mu_q)$.

– si $\delta = 1$: d'après les considérations précédentes, $M \otimes Z/q$ est somme directe d'un facteur $Z/q[G]$ et d'un sous-module indécomposable isomorphe à $\text{Hom}(R_d^{ab}, \mu_q)$.

Le théorème est ainsi démontré. Q.E.D.

COROLLAIRE 1: *Pour tout entier $r \mid q$, on a :*

$$M \otimes Z/r \xrightarrow{\sim} \text{Hom}(R_d^{ab}, \mu_r) \times Z/r[G]^\delta$$

(ici l'action sur Hom est l'action habituelle).

PREUVE: On l'a montré en montrant le théorème.

COROLLAIRE 2: *Si K/k est une extension de type quasi-régulier, $K^\times/K^{\times r}$ est somme directe de deux sous- $Z/r[G]$ -modules totalement isotropes, pour tout $r \mid q$.*

PREUVE: C'est clair. Notons qu'un résultat analogue est valable dans le cas modérément ramifié ([16], Satz 9).

COROLLAIRE 3: *Si K/k est une extension de type quasi-régulier, on a, pour tout $r \mid q$ et tout $i \in Z$: $\hat{H}^i(G, K^\times/K^{\times r}) \simeq \hat{H}^{i-2}(G, Z/r) \times \hat{H}^{i+2}(G, \mu_r)$.*

PREUVE: D'après le théorème, $\hat{H}^i(G, K^\times/K^{\times r}) = \hat{H}^i(G, R_d^{ab} \otimes Z/r) \times \hat{H}^i(G, \text{Hom}(R_d^{ab}, \mu_r))$. Or le premier groupe est isomorphe à $\hat{H}^{i-2}(G, Z/r)$ et le second à $\hat{H}^{i+2}(G, \mu_r)$ ([20], corol. 1.7 et 1.8). Q.E.D.

§8 F_d -extensions et modules d'Iwasawa

Dans toute cette section, on suppose $p \neq 2$; k est un corps local p -adique irrégulier, $n = [k : \mathbb{Q}_p]$, $d(G) = d \leq n/2 + 1$.

Une F_d -extension de k sera notée K_d^∞ . Elle est dite *cyclotomique* si elle contient μ_{p^∞} . Suivant Iwasawa ([11]), on note X_d^∞ le groupe de Galois de la pro- p -extension abélienne maximale de K_d^∞ , et on se propose d'étudier la structure du Λ_d -module X_d^∞ , où Λ_d est l'algèbre de Magnus de rang d . On en déduira, pour toute sous-extension finie K de K_d^∞ , des renseignements sur la structure du module $A(K)$.

8.1. L'algèbre de Magnus

Soit F_d un pro- p -groupe libre de rang d . Soit F_d^m une suite de sous-groupe ouverts tels que $F_d = \varprojlim F_d/F_d^m$. Par définition l'*algèbre complète* $\mathbb{Z}_p[[F_d]]$ est la limite projective des algèbres de groupes $\mathbb{Z}_p[F_d/F_d^m]$.

Soit Λ_d l'algèbre des séries formelle associatives (non nécessairement commutatives) en d indéterminées T_1, \dots, T_d , à coefficient dans \mathbb{Z}_p (c'est un complété de l'algèbre tensorielle du \mathbb{Z}_p -module $(\mathbb{Z}_p)^d$): c'est l'*algèbre de Magnus* de rang d .

PROPOSITION 10: (voir [26], I-7).

Soit x_1, \dots, x_d une base de F_d . Il existe un isomorphisme continu de $\mathbb{Z}_p[[F_d]]$ sur Λ_d , transformant x_i en $1 + T_i$ pour $1 \leq i \leq d$.

Pour $d = 1$, on retrouve l'algèbre d'Iwasawa $\Lambda_1 = \mathbb{Z}_p[[T]]$ (voir [11]).

8.2. Le module d'Iwasawa d'une F_d -extension cyclotomique

Dans cette sous-section, nous ferons les conventions suivantes: la suite F_d^m précédente sera choisie de façon que, si $G_m = F_d/F_d^m$, alors $d(G_m) = d$ pour tout m (prendre par exemple la suite descendante des sous-groupes de Frattini successifs). Si K_d^∞/k est une F_d -extension, on notera K_m le corps fixe de F_d^m ; alors $G_m = \text{Gal}(K_m/k)$, $\Lambda_d = \varprojlim \mathbb{Z}_p[G_m]$ et $X_d^\infty = \varprojlim A(K_m)$ (les morphismes de liaison étant induits par la norme).

Rappelons que pour tout pro- p -groupe H , tout sous-groupe fermé U et tout U -module A , le module induit relatif $\text{Ind}_H^U(A)$ est formé des applications continues $\alpha: H \rightarrow A$ telles que $\alpha(uh) = u.\alpha(h)$ pour tout $u \in U$, tout $h \in H$. Le groupe H opère pour: $g\alpha(h) = \alpha(hg)$ pour tous $g, h \in H$.

THÉORÈME 10: Soient K_d^∞/k une F_d -extension cyclotomique, et X_d^∞ le Λ_d -module associé. Soit x_1, \dots, x_d une base de F_d et, pour tout $1 \leq i \leq d$, soit $\text{Ind}_{F_d}^{(x_i)}(\mathbb{Q}_p/\mathbb{Z}_p)$ le module induit relatif à F_d et au sous-groupe fermé $\langle x_i \rangle$ engendré par x_i . Alors:

$$X_d^\infty \xrightarrow{\sim} \Lambda_d^{n+2-2d} \times \text{Hom}(I, \mu_{p^\infty}), \quad \text{où } I = \prod_{i=1}^d \text{Ind}_{F_d}^{(x_i)}(\mathbb{Q}_p/\mathbb{Z}_p)$$

et l'action sur Hom est l'action habituelle.

(Comparer au résultat obtenu par Iwasawa ([12], th. 3) dans le cas modérément ramifié).

Le démonstration du théorème va se faire en plusieurs étapes.

LEMME 6: Soient L/k une p -extension et K/k une sous-extension telle que $d(\text{Gal}(L/k)) = d(\text{Gal}(K/k))$. Alors $\mu_k = \mu_L$ si et seulement si $\mu_k = \mu_K$.

PREUVE: Supposons $\mu_k = \mu_K$. Si $\mu_k \neq \mu_L$, cela voudrait dire que dans l'extension L/K , on aurait ajouté des racines p -primaires d'éléments de $\mu_K = \mu_k$; mais ce faisant, on aurait augmenté le nombre de générateurs du groupe de Galois, i.e. $d(\text{Gal}(L/k)) > d(\text{Gal}(K/k))$, contrairement à l'hypothèse. Donc $\mu_k = \mu_L$. La réciproque est évidente. Q.E.D.

Pour tout m , soit q_m l'indice d'irrégularité de K_m ; le lemme précédent montre que, dans une F_d -extension cyclotomique, q_m tend vers l'infini avec m . On a alors: $X_d^\infty = \varprojlim_m K_m^\times / K_m^{\times q_m}$. Mais d'après le théorème 9, on a une décomposition:

$$(3) \quad K^\times / K^{\times q_m} \xrightarrow{\sim} (R_d^{ab}(G_m) \otimes \mathbb{Z}/q_m) \times \text{Hom}(R_d^{ab}(G_m), \mu_{q_m}) \times (\mathbb{Z}/q_m[G_m])^{n+2-2d}.$$

Regardons séparément les limites projectives des divers facteurs.

LEMME 7:

$$\varprojlim_m R_d^{ab}(G_m) \otimes \mathbb{Z}/q_m = \varprojlim_m R_d^{ab}(G_m) = 0.$$

PREUVE: Comme $\varprojlim_m q_m = +\infty$, on a $\varprojlim_m R_d^{ab}(G_m) \otimes \mathbb{Z}/q_m = \varprojlim_m R_d^{ab}(G_m)$. Il reste à montrer que $\varprojlim_m R_d^{ab}(G_m) = 0$. Pour $d = 1$, le calcul se fait directement et sans difficulté. Pour $d \geq 2$, on peut utiliser l'astuce suivante:

Soit k_0 un corps local p -adique régulier de degré $(d - 1)$ sur \mathbb{Q}_p (il en existe, puisque $p \neq 2$). D'après le théorème de Šafarevič, le groupe de Galois de la pro- p -extension maximale $k(p)$ de k est isomorphe à F_d . D'après le théorème 2 et le corps de classes, $\varprojlim_m R_d^{ab}(G_m)$ est isomorphe au groupe de Galois de la pro- p -extension abélienne maximale de $k(p)$, c'est-à-dire 0. Q.E.D.

LEMME 8: $\varprojlim_m \text{Hom}(R_d^{ab}(G_m), \mu_{q_m}) \simeq \text{Hom}(I, \mu_{p^\infty})$, I désignant le module dualisant de F_d .

PREUVE: On a évidemment un isomorphisme de groupes:

$$\varprojlim_m \text{Hom}(R_d^{ab}(G_m), \mu_{q_m}) \xrightarrow{\sim} \varprojlim_m \text{Hom}(R_d^{ab}(G_m), \mathbb{Z}/q_m).$$

Calculons cette dernière limite en faisant intervenir le module dualisant ([26], I et annexe).

Rappelons que, pour tout pro- p -groupe de dimension cohomologique finie ($cd(H) = r$), le module dualisant I_r de H (E_r dans la notation de [26], I.81) est isomorphe à $\varprojlim_{U,S} H'(U, \mathbb{Z}/S\mathbb{Z})^*$, où U parcourt les sous-groupes ouverts de H et $*$ désigne le dual de Pontrjagin. Dans le cas qui nous occupe, $H = F_d$ et $cd H = 1$, donc $\varprojlim_m H^1(R_d^{ab}(G_m), \mathbb{Z}/q_m)^*$ n'est autre que le module dualisant I de F_d , qui est isomorphe à $\prod_{i=1}^d \text{Ind}_{F_d}^{(\mathbb{Z}_p)}(\mathbb{Q}_p/\mathbb{Z}_p)$ d'après [26], V.24. Comme $H^1(R_d^{ab}(G_m), \mathbb{Z}/q_m) = \text{Hom}(R_d^{ab}(G_m), \mathbb{Z}/q_m)$, on en déduit que $\varprojlim_m \text{Hom}(R_d^{ab}(G_m), \mathbb{Z}/q_m) \xrightarrow{\sim} I^*$ (en tant que groupes). Compte tenu de l'action des G_m , on a bien: $\varprojlim_m \text{Hom}(R_d^{ab}(G_m), \mu_{q_m}) \xrightarrow{\sim} \text{Hom}(I, \mu_{p^\infty})$ en tant que Λ_d -modules. Q.E.D.

Dans le cas d'une \mathbb{Z}_p -extension cyclotomique, on retrouve le résultat suivant d'Iwasawa ([11], th. 25):

COROLLAIRE 1: Supposons $d = 1$. Alors $X_d^\infty \xrightarrow{\sim} \Lambda_1^n \times T(\mu_{p^\infty})$, où $T(\cdot)$ désigne le module de Tate.

PREUVE: Pour $d = 1$, le module induit $I = \text{Ind}_{F_1}^{(\mathbb{Z}_p)}(\mathbb{Q}_p/\mathbb{Z}_p)$ est évidemment isomorphe à $\mathbb{Q}_p/\mathbb{Z}_p$, donc $\text{Hom}(I, \mu_{p^\infty})$ est bien isomorphe à $T(\mu_{p^\infty})$. Q.E.D.

Revenons au cas général (d quelconque).

COROLLAIRE 2: Le groupe $\text{Gal}(k(p)/K_d^\infty)$ est un pro- p -groupe libre.

PREUVE: Le groupe $H = \text{Gal}(k(p)/K_d^\infty)$ est un sous-groupe fermé

d'un groupe de Demuškin, donc $\text{scd } H \leq 2$. On sait qu'alors H est un pro- p -groupe libre si et seulement si $H/[H, H]$ est \mathbb{Z}_p -libre. Ce qui est le cas d'après le théorème. Q.E.D.

On a ainsi exprimé le groupe de Demuškin comme extension d'un pro- p -groupe libre par un pro- p -groupe libre.

Soit maintenant K/k une p -extension de groupe de Galois G qui se plonge dans une F_d -extension cyclotomique X_d^∞ . D'après le théorème 3:

$A(K) \simeq R_d^{ab}(G) \times T_K$, où T_K est un $\mathbb{Z}_p G$ -module cohomologiquement trivial isomorphe à $M_K \times (\mathbb{Z}_p G)^{n+2-2d-\delta}$.

COROLLAIRE 3: Si K/k se plonge dans une F_d -extension cyclotomique, alors $\delta = 0$.

PREUVE: D'après le théorème, X_d^∞ contient un facteur direct isomorphe à Λ_d^{n+2-2d} . Donc le nombre de facteurs de $A(K)$ isomorphes à $\mathbb{Z}_p G$ est supérieur ou égal à $n + 2 - 2d$. D'où la nullité de δ . Q.E.D.

COROLLAIRE 4: Supposons que K/k se plonge dans une F_d -extension cyclotomique X_d^∞ . Alors M_K est un groupe de normes universelles. Plus précisément, soient $J = \text{Hom}(I, \mu_{p^\infty})$ et $R = \text{Gal}(K_d^\infty/K)$. Alors $M_K = N_R J$, où N_R est la limite projective des applications de norme relatives aux quotients finis de R .

PREUVE: Pour toute extension L/k contenue dans K_d^∞ , contenant K , de groupe de Galois E , on a: $A(L) \simeq R_d^{ab}(E) \times T_L$, où T_L est un $\mathbb{Z}_p E$ -module cohomologiquement trivial, isomorphe à $M_L \times (\mathbb{Z}_p E)^{n+2-2d}$. De la trivialité cohomologique, il résulte que $N_H(T_L) = (T_L)^H$ où $H = \text{Gal}(L/K)$. Or $A(L)^H = A(K)$ et $R_d^{ab}(E)^H = R_d^{ab}(G)$ d'après la propos. 1, et $(\mathbb{Z}_p E)^H = \mathbb{Z}_p G$ de façon évidente. Il en résulte que $M_K = N_H(M_L) = (M_L)^H$ d'où $M_K = N_R J$ par passage à la limite. Q.E.D.

COROLLAIRE 5: Si la p -extension cyclique K/k de groupe de Galois G se plonge dans une \mathbb{Z}_p -extension cyclotomique, alors $A(K) \simeq \mathbb{Z}_p \times \mu_K \times (\mathbb{Z}_p G)^n$.

PREUVE: C'est immédiat, d'après ce qui précède et en sachant que le module des pro-relations d'un p -groupe cyclique est \mathbb{Z}_p . On aurait pu aussi calculer le \mathbb{Z}_p -rang de $A(K)$ et en déduire que $M_K \simeq \mu_K$. Q.E.D.

§9 Tentative de globalisation

Dans toute cette section, k désigne une extension finie de \mathbb{Q} , et p un nombre premier fixé. On va essayer de globaliser les résultats des paragraphes précédents, d'abord en dressant des analogies entre le cas global et le cas local, ensuite en utilisant la conjecture de Leopoldt.

On adoptera les notations suivantes:

$S(k) = S =$ ensemble des places de k divisant p et des places archimédiennes.

$r_1(k) = r_1 =$ nombre des places réelles de k .

$r_2(k) = r_2 =$ nombre des places complexes de k .

$\Omega_S =$ extension maximale de k non ramifiée hors de S .

$k_S =$ pro- p -extension maximale de k non ramifiée hors de S .

$\mathcal{G}_S = \mathcal{G}_S(k) = \text{Gal}(\Omega_S/k)$.

$G_S = G_S(k) = \text{Gal}(k_S/k)$.

$\mathcal{C}(k) =$ groupe des classes d'idèles de k .

$\mathcal{C}(k, S) =$ groupe des classes de S -idèles de k .

$U(k, S) =$ sous-groupes des idèles de k dont les composantes valent 1 en les places de S et sont des unités hors de S (s'identifie à un sous-groupe de $\mathcal{C}(k)$).

$C(k) = \mathcal{C}(k, S)/U(k, S)$.

Définitions analogues pour toute extension K/k . S'il n'y a pas d'ambiguïté possible, on continue à désigner par S l'ensemble des places de K au-dessus de S . Soient enfin \mathcal{C} , U et C les limites inductives respectives de $\mathcal{C}(K)$, $U(k, S)$ et $\mathcal{C}(K, S)$ quand K parcourt les sous-extensions de Ω_S/k .

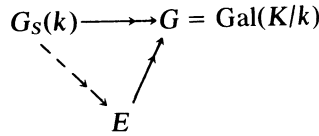
On sait (voir par ex. [9], 2.1) que $C = \mathcal{C}/U$ et que U est cohomologiquement trivial. Donc (\mathcal{G}_S, C) est une formation de classes ([1], chap. 14) au sens d'Artin-Tate. Pour chaque sous-corps K de Ω_S , le module correspondant de cette formation n'est autre que $C(K)$.

9.1. Analogies avec le cas local

Soit K/k une p -extension contenue dans k_S , de groupe de Galois G . Définissons d'abord le couple $(A(K), u)$. Pour $A(K)$, nous prendrons le quotient de $C(K)$ qui correspond, par le corps de classes global, au groupe de Galois $G_S(K)/[G_S(K), G_S K]$. Nous prendrons pour u l'image de la classe fondamentale $H^2(G, C(K))$ par l'homomorphisme induit $H^2(G, C(K)) \rightarrow H^2(G, A(K))$.

Les problèmes de plongement considérés dans le cas local seront

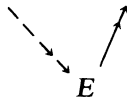
remplacés par les *S-problèmes de plongement*



Une solution (forte) de ce problème est donc une extension L/k , contenant K et contenue dans k_S , avec les conditions habituelles sur les groupes de Galois.

Une analogue global du théorème de Demuškin–Šafarevič est valable.

THÉORÈME 5 bis: Soit $1 \rightarrow A \rightarrow E \rightarrow G \rightarrow 1$ une extension de p -groupes, de noyau abélien A , telle que $d(E) = d(G)$, associée à une classe de cohomologie $\epsilon \in H^2(G, A)$. Alors le *S-problème de plongement* $G_S(k) \longrightarrow G = \text{Gal}(K/k)$ possède une solution (forte) si et



seulement si, pour tout caractère $\varphi \in \text{Hom}_G(A, C(K))$, on a $\varphi^*(\epsilon) = 0$.

PREUVE:

(a) Toute solution faible du *S-problème de plongement* précédent est une solution forte d'après la propos. 4, (iii).

(b) (D'après G. Poitou [23]). D'après le critère de Hoehsmann ([10]), le *S-problème de plongement* précédent possède une solution faible si et seulement si $\text{inf } \epsilon = 0$, où inf est l'inflation $H^2(G, A) \rightarrow H^2(\mathcal{G}_S, A)$. Pour tout $\varphi \in \text{Hom}_G(A, C(K))$, on a un diagramme commutatif:

$$\begin{array}{ccc}
 H^2(G, A) & \xrightarrow{\varphi^*} & H^2(G, C(K)) \\
 \downarrow \text{inf} & & \downarrow \text{inf} \\
 H^2(\mathcal{G}_S, A) & \longrightarrow & H^2(\mathcal{G}_S, C)
 \end{array}$$

où l'injectivité de la colonne de droite résulte de la formation de classes (\mathcal{G}_S, C) . Si $\text{inf } \epsilon = 0$, on a immédiatement $\varphi^*(\epsilon) = 0 \ \forall \varphi \in \text{Hom}_G(A, C(K))$. Réciproquement, supposons $\varphi^*(\epsilon) = 0$ pour tout $\varphi \in \text{Hom}_G(A, C(K)) = H^0(\mathcal{G}_S, \text{Hom}(A, C))$. D'après le théorème de dualité globale avec ramification restreinte ([9], [32]), $H^2(\mathcal{G}_S, A)$ se trouve en

dualité exacte avec un certain quotient de ce groupe H^0 , la dualité étant induite par le cup-produit. La nullité de $\inf \epsilon$ en découle immédiatement. Q.E.D.

Je ne sais pas si un analogue global du théorème de B.B. Lur'e est valable. Nous pouvons maintenant montrer un analogue global du théorème 4:

THÉORÈME 4 bis: *Supposons que K/k se plonge dans une F_d -extension ($d = d(G)$). Alors les conditions équivalentes suivantes sont vérifiées:*

- (i) tout S -problème de plongement $G_S(k) \longrightarrow G = \text{Gal}(K/k)$, dont
- $$\begin{array}{ccc}
 G_S(k) & \longrightarrow & G \\
 \searrow & & \nearrow \\
 & & E
 \end{array}$$

le noyau est un pro- p -groupe abélien et tel que $d(E) = d(G)$, possède une solution (forte).

(ii) l'inclusion $\text{Tor } C(K) \rightarrow C(K)$ induit un homomorphisme $H^2(G, \text{Tor } C(K)) \rightarrow H^2(G, C(K))$ qui est nul (Tor désigne la \mathbb{Z}_p -torsion).

(iii) (R_d^{ab}, χ) est facteur direct de $(A(K), u)$.

PREUVE: Les démonstrations sont analogues à celles du théorème 4, à quelques modifications près:

- le théorème 5 est remplacé par le théorème 5 bis.
- la proposition 5 (avec des noyaux abéliens) reste valable en remplaçant le lemme de Krasner par la finitude du nombre des extensions de degré donné non ramifiées hors de S ([26], II-48).
- la proposition 6 reste valable, car le théorème de Šafarevič-Weil s'applique aux classes d'idèles ([1], chap. 14). Q.E.D.

REMARQUE 6: Supposons $d = 1$. Alors les conditions du théorème 4 bis) sont nécessaires et suffisantes pour que K/k se plonge dans une \mathbb{Z}_p -extension. En effet, dans ce cas, tous les problèmes de plongement considérés sont à noyau abélien.

9.2. *Sur les conjectures de Leopoldt et de Tate*

Posons $\Sigma = \Sigma(k) =$ ensemble des places de k divisant p

$$\begin{aligned}
 V_S &= V_S(k) = \{x \in k^\times / v(x) \equiv 0 \pmod{p} \quad \forall v \notin S, \\
 &\quad x \in K_v^{\times p} \quad \forall v \in S\} / k_v^{xp}.
 \end{aligned}$$

A partir d'ici, nous supposons que k contient μ_4 si $p = 2$.

Nous allons d'abord rassembler des résultats plus ou moins connus ([4], [25]) sur la cohomologie de G_S . Une démonstration unifiée est rendue possible par l'emploi des théorèmes de dualité globale.

PROPOSITION 11: *Soient $d(G_S)$ et $r(G_S)$ les nombres minimaux de générateurs et de relations du pro- p -groupes G_S . Alors:*

$$d(G_S) = d(V_S) + w(\Sigma) + w(\mathbb{R}) + 1 + r_2 - \alpha$$

$$r(G_S) = d(V_S) + w(\Sigma) + w(\mathbb{R}) - \alpha$$

où $w(\Sigma)$ (resp. $w(\mathbb{R})$) est le nombre des places $v \in \Sigma$ (resp. des places v réelles) t.q. $\mu_p \subset k_v^\times$, et $\alpha = 1$ (resp. 0) si $\mu_p \subset k^\times$ (resp. $\mu_p \not\subset k^\times$).

PREUVE; Pour tout \mathcal{G}_S -module M fini dont l'ordre est une S -unité, on a la suite exacte de Tate ([9], [30])

$$0 \rightarrow H^0(\mathcal{G}_S, M) \rightarrow \prod_{v \in \Sigma} H^0(\mathcal{G}_v, M) \prod_{v \in \mathbb{R}} \hat{H}^0(\mathcal{G}_v, M) \rightarrow H^2(\mathcal{G}_S, M)^*$$

$$\rightarrow H^1(\mathcal{G}_S, M) \rightarrow \prod_{v \in S} H^1(\mathcal{G}_v, M) \rightarrow H^1(\mathcal{G}_S, M')^* \rightarrow H^2(\mathcal{G}_S, M)$$

$$\rightarrow \prod_{v \in S} H^2(\mathcal{G}_v, M) \rightarrow H^0(\mathcal{G}_S, M')^* \rightarrow 0,$$

où $*$ désigne le dual de Pontrjagin et $M' = \text{Hom}(M, \Omega_S^\times)$. De plus, la caractéristique partielle d'Euler-Poincaré est donnée par:

$$\frac{|H^0(\mathcal{G}_S, M)| \cdot |H^2(\mathcal{G}_S, M)|}{|H^1(\mathcal{G}_S, M)|} = \prod_{\text{varch.}} \frac{|\hat{H}^0(\mathcal{G}_v, M')|}{|H^0(\mathcal{G}_v, M')|}$$

$$= \prod_{\text{varch.}} \frac{|H^0(\mathcal{G}_v, M)|}{\|M\|_v} \quad ([9], [31]).$$

Il suffit alors de faire $M = \mu_p$ pour obtenir les ordres des groupes $H^i(\mathcal{G}_S, F_p)$ pour $i = 1, 2$. Or $H^i(G_S, F_p) \cong H^i(\mathcal{G}_S, F_p)$ ([9], 6-1), d'où la proposition. Q.E.D.

COROLLAIRE 1: *Soit $M(G_S)$ le multiplicateur de Schur de G_S (i.e. le dual de Pontrjagin de $H^2(G_S, \mathbb{Q}_p/\mathbb{Z}_p)$). Alors $d(M(G_S)) = -(1 + r_2) + \text{rang}_{\mathbb{Z}_p} G_S/[G_S, G_S]$.*

PREUVE: Il est connu que $d(M(H)) = r(H) - d(H) + \text{rang}_{\mathbb{Z}_p} H/[H, H]$ pour tout pro- p -groupe H . Il suffit alors d'appliquer les formules de la proposition. Q.E.D.

COROLLAIRE 2: *Supposons que k contient μ_p (resp. μ_4 si $p = 2$). Alors le pro- p -groupe G_S est libre si et seulement si $V_S = 0$ et $|\Sigma| = 1$, si et seulement si $G_S/[G_S, G_S] \cong \mathbb{Z}_p^{1+r_2}$.*

EXEMPLE: $k = \mathbb{Q}(\mu_p)$, où p est un nombre premier régulier.

PREUVE: Par définition, G_S est un pro- p -groupe libre si et seulement si $r(G_S) = 0$. Or si $\mu_p \subset k^\times$, la formule de la proposition s'écrit $r(G_S) = d(V_S) + |\Sigma| - 1$. La première assertion du corollaire en découle immédiatement. Pour la seconde assertion, on sait que $cd G_S \leq 2$, donc G_S est un pro- p -groupe libre si et seulement si $M(G_S) = 0$ et $G_S/[G_S, G_S]$ est \mathbb{Z}_p -libre. Il suffit alors d'appliquer le corollaire 1. Q.E.D.

Parmi les nombreuses formulations de la conjecture de Leopoldt (sur l'indépendance p -adique des unités de k), nous choisirons celle qui consiste à dire que k possède $(1 + r_2)$ \mathbb{Z}_p -extensions "indépendantes", autrement dit $\text{rang}_{\mathbb{Z}_p} G_S/[G_S, G_S] = 1 + r_2$ (voir [11]).

PROPOSITION 12: *La conjecture de Leopoldt est vérifiée pour p et k si et seulement si $H^2(G_S, \mathbb{Q}_p/\mathbb{Z}_p) = 0$.*

PREUVE: C'est immédiat, d'après le corollaire 1 précédent. Q.E.D.

COROLLAIRE 1: *Pour que k vérifie la conjecture de Leopoldt, il faut et il suffit que $r(G_S) = d(\text{Tor } G_S/[G_S, G_S])$ où Tor désigne la \mathbb{Z}_p -torsion. En particulier, si tel est le cas, G_S est un pro- p -groupe libre si et seulement si $\text{Tor } G_S/[G_S, G_S] = 0$ (analogue global du théorème de Šafarevič).*

PREUVE; C'est clair, car $d(\text{Tor } G_S/[G_S, G_S]) = d(G_S) - \text{rang}_{\mathbb{Z}_p} G_S/[G_S, G_S]$. Q.E.D.

COROLLAIRE 2: Les conditions suivantes sont équivalentes.

(i) $scd(G_S(k)) = 2$ ("conjecture de Tate"; voir [30]).

(ii) *la conjecture de Leopoldt est vérifiée pour toute extension finie de k contenue dans k_S .*

PREUVE: En effet, on sait que $cd G_S \leq 2$. Pour que $scd G_S = 2$, il faut et il suffit alors que $H^2(U, \mathbb{Q}_p/\mathbb{Z}_p) = 0$ pour tout sous-groupe ouvert U de G_S (voir [26]). Q.E.D.

EXEMPLE: Soit $k = \mathbb{Q}(\sqrt{15}, \sqrt{-3})$. Soit $p = 3$. Alors p possède seulement deux prolongements à k_S . Il en résulte que k vérifie la conjecture de Tate ([16b], §5, ex. 3).

9.3. Structure de $A(K)$

On obtient un analogue global du théorème 3 en supposant la conjecture de Tate.

THÉORÈME 3 bis: *Supposons que k vérifie la conjecture de Tate, et que la p -extension K/k , de groupe de Galois G , se plonge dans une F_d -extension ($d = d(G)$). Alors:*

$A(K) \simeq R_d^{ab}(G) \times M \times (\mathbb{Z}_p G)^h$, où M est un $\mathbb{Z}_p G$ -module cohomologiquement trivial contenant le groupe de \mathbb{Z}_p -torsion $\text{Tor } A(K)$ et ne contenant pas de facteur direct libre.

PREUVE: D'après le théorème 4 (bis), $A(K) \simeq R_d^{ab}(G) \times N$. Soit h le nombre maximal de facteurs de N isomorphes à $\mathbb{Z}_p G$. Alors $N = M \times (\mathbb{Z}_p G)^h$. Or, d'après la proposition 1, $A(K)$ et $R_d^{ab}(G)$ ont même cohomologie. Donc N et M sont cohomologiquement triviaux. Q.E.D.

Il semble difficile d'en savoir plus, car la détermination de $\text{Tor } A(K)$ est probablement un problème d'ordre analytique. Cependant:

COROLLAIRE (à rapprocher du coroll. 5, th. 10):

Supposons que l'extension cyclique K/k se plonge dans une \mathbb{Z}_p -extension K_1^∞/k , et soit X_1^∞ le module d'Iwasawa associé. Alors:

- (i) $h \leq r_2$, et $h = r_2$ si et seulement si $X_1^\infty / \text{Tor}_{\Lambda_1} X_1^\infty \simeq \Lambda_1^{r_2}$.
- (ii) si $h = r_2$, on a: $A(K) \simeq \mathbb{Z}_p \times \text{Tor } A(K) \times (\mathbb{Z}_p G)^{r_2}$, et $\text{Tor } A(K)$ est cohomologiquement trivial.

PREUVE: On sait que $X_1^\infty / \text{Tor}_{\Lambda_1} X_1^\infty$ s'identifie à un sous-module d'indice fini de $\Lambda_1^{r_2}$ (voir [11] dans le cas cyclotomique, [7] dans le cas général). L'assertion (i) en résulte immédiatement. De plus, si $h = r_2$, alors $\text{rang}_{\mathbb{Z}_p} M_K = 0$ donc $M_K = \text{Tor } A(K)$. Q.E.D.

BIBLIOGRAPHIE

- [1] ARTIN-TATE – *Class-field theory*. Harvard (1961).
- [1b] BERTRANDIAS-PAYAN – Γ -extensions et invariants cyclotomiques. *Ann. Scien. E.N.S.* 5 (1972) 517–543.
- [2] Z.I. BOREVIĆ – On the group of principal units of a normal p -extension of a regular local field. *Proc. Steklov Math. Inst.* 80 (1965) 31–47.
- [2b] Z.I. BOREVIĆ – On the multiplicative group of cyclic p -extensions of a local field. *Proc. Steklov Math. Inst.* 80 (1965) 15–30.

- [3] BOREVIČ–EL MUSA – Completion of the multiplicative group of p -extensions of an irregular local field. *J. Soviet Math.* 6,3 (1976) 6–23.
- [4] A. BRUMER – Galois groups of extensions of algebraic number fields with given ramification. *Michigan Math. J.* 13 (1966) 33–40.
- [5] S.P. DEMUŠKIN – The group of the maximal p -extension of a local field. *Amer. Math. Soc. Transl.* 2,46 (1965) 149–152.
- [6] DEMUŠKIN–ŠAFAREVIČ – The embedding problem for local fields. *Amer. Math. Soc. Transl.* 2,27 (1963) 267–288.
- [7] R. GREENBERG – On the structure of certain Galois groups. *Invent. Math.* 47 (1978) 85–99.
- [8] K.W. GRUENBERG – *Cohomological topics in group theory*. Springer Verlag n^0 143, 1970.
- [9] K. HABERLAND – *Galois cohomology of algebraic number fields*. Thesis, Berlin, 1978.
- [10] K. HOECHSMANN – Zum Einbettungsproblem. *J. reine angew. Math.* 229 (1968) 81–106.
- [11] K. IWASAWA – On Z_p -extensions of algebraic number fields. *Ann. Math.* 98 (1973) 246–326.
- [12] K. IWASAWA – On Galois groups of local fields. *Trans. Amer. Math. Soc.* 80 (1955) 448–469.
- [13] A.V. JAKOVLEV – Symplectic spaces with operators over commutative rings. *Vestnik Leningrad 3* (1976) 339–346.
- [14] JANNSEN-WINGBERG – Die p -Vervollständigung der multiplikativen Gruppe einer p -Erweiterung eines irregulären p -adischen Zahlkörpers. *J. reine angew. Math.* 307/308 (1979) 399–410.
- [15] Y. KAWADA – Cohomology of group extensions. *J. Fac. Sci. Univ. Tokyo* 1,7 (1954) 87–106.
- [16] H. KOCH – Über Darstellungsräume und die Struktur der multiplikativen Gruppe eines p -adischen Zahlkörpers. *Math. Nachr.* 26 (1963/1964) 67–100.
- [16b] L.V. KUZMIN – Local extensions associated with l -extensions with given ramification. *Math. USSR Izv.* 9,4 (1975) 693–727.
- [17] F. LAUBIE – *Sur la ramification d'une extension de Lie d'un corps local*. (En préparation).
- [18] B.B. LUR'E – Problem of immersion of local fields with a non abelian kernel. *J. Soviet Math.* 6,3 (1976) 298–306.
- [19] T. NGUYEN-QUANG-DO – Filtration de K^x/K^{x^p} et ramification sauvage. *Acta Arithm.* 34 (1976) 323–340.
- [20] T. NGUYEN-QUANG-DO – Sur le module des relations d'un p -groupe et la suite exacte d'inflation-restriction. *J. reine angew. Math.* 316 (1980) 110–121.
- [21] J. NEUKIRCH – Über das Einbettungsproblem der algebraischen Zahlentheorie. *Invent. Math.* 21 (1973) 59–116.
- [22] H. PIEPER – Die Einseinheitengruppe eines zahm-verzweigten Galois lokalen Körpers als Galois-modul. *Math. Nachr.* 54, 1,6 (1972) 173–210.
- [23] G. POITOU – Conditions globales pour les problèmes de plongement à noyau abélien. *Ann. Inst. Fourier* 29,1 (1979) 1–14.
- [24] I.R. ŠAFAREVIČ – On p -extensions. *Amer. Math. Soc. Transl.* 2,4 (1956) 59–72.
- [25] I.R. ŠAFAREVIČ – Extensions with given points of ramification. *Amer. Math. Soc. Transl.* 2,59 (1966) 128–149.
- [26] J.P. SERRE – *Cohomologie galoisienne*, Springer Verlag, n^0 5, 1965.
- [27] J. SONN – Epimorphisms of Demuškin groups. *Israel J. Math.*, 17,2 (1974) 176–190.
- [28] K. TAHARA – On the 2nd cohomology group of semi-direct products. *Math. Zeit.*, 129 (1972) 365–379.

- [29] J. TATE – The higher dimensional cohomology groups of class field theory. *Ann. Math.* 56 (1952) 294–297.
- [30] J. TATE – Duality theorems in Galois cohomology. *Proc. Int. Congress Stockholm* (1962) 288–295.
- [31] J. TATE – On the conjectures of Birch & Swinnerton-Dyer and a geometric analogue. *Sem. Bourbaki* 306 (1966).
- [32] K. WINGBERG – Die Einseinheitengruppe von p -Erweiterungen regulärer p -adischer Zahlkörper als Galoismodul. *J. reine angew. Math.* 305 (1979) 206–214.
- [33] K. UCHIDA – On Tate’s duality theorems in Galois cohomology. *Tohoku Math. J.* 21 (1969) 92–101.
- [34] K. YAMAZAKI – On projective representations and ring extensions of finite groups. *J. Fac. Sci. Univ. Tokyo* 10 (1964) 147–195.

(Oblatum 6-X1-1980, 14-V-1981 & 7-X-1981)

Nguyen-Quang-Do Thong
49 rue Pierre Valette
92240 Malakoff
France

U.E.R. de Mathématiques
de l’Université Paris VII
2 Place Jussieu
75221 Paris Cedex 05

Certains des résultats de cet article (plus précisément: l’équivalence des conditions (1), (4) et (5) du théo. 4, et le théo. 6 ont été obtenus indépendamment par Jannsen et Wingberg. Voir leur article “Einbettungsprobleme und Galoisstruktur lokaler Körper”, à paraître dans *J. reine angew. Math.*