ÉTUDE KUMMERIENNE DE LA q-SUITE CENTRALE DESCENDANTE D'UN GROUPE DE GALOIS

par

Thong Nguyen Quang Do

Résumé. — Soit $q = p^a$ une puissance d'un nombre premier p. Soit F un corps de caractéristique $\neq p$, contenant une racine primitive $q^{\text{ième}}$ de l'unité. On expose ici (et avec des démonstrations simplifiées) une série de résultats de Jan Mináč et ses collaborateurs sur des liens étroits entre l'algèbre de cohomologie $H^*(G_F, \mathbb{Z}/q)$ et le troisième quotient $G_F/G_F^{(3)}$ de la q-suite centrale descendante de G_F.

Abstract. — Let $q = p^a$ be a power of a fixed prime p. Let F be a field of characteristic $\neq p$, containing a primitive q^{th} root of unity. We give a survey (and simplified proofs) of a series of results by Jan Mináč and his collaborators on strong relationship between the cohomology algebra $H^*(G_F, \mathbb{Z}/q)$ and the third quotient $G_F/G_F^{(3)}$ of the q-central descending series of G_F.

Introduction

Soit G un groupe profini, et soit $q = p^a$ une puissance d'un nombre premier p. Au couple (G, q) on peut associer deux invariants importants relevant, l'un de la cohomologie galoisienne, l'autre de la théorie des groupes.

(i) L'algèbre de cohomologie $H^*(G, \mathbb{Z}/q)$ (avec action triviale sur $\mathbb{Z}/q$) : C'est l'algèbre

$$\bigoplus_{r=0}^{\infty} H^r(G, \mathbb{Z}/q),$$

graduée par le cup-produit.

(ii) La q-suite centrale descendante de G : Elle est définie inductivement par

$$G^{(1)} = G,\ G^{(i+1)} = (G^{(i)})^q[G^{(i)}, G],\ \text{pour } i = 1, 2, \ldots$$

***Classification mathématique par sujets* (2000).** — 12G05,12F10,11R34,11R70,19D45,19D05.

Mots clefs. — Conjecture de Milnor-Bloch-Kato, cup-produit, problème de plongement, ramification restreinte.

Donc $G^{(i+1)}$ est le sous-groupe fermé de G engendré par les puissances h^q et les commutateurs $[h,g] = h^{-1}g^{-1}hg$, pour $h \in G^{(i)}$ et $g \in G$. Tout $G^{(i)}$ est manifestement normal dans G ; le quotient $G/G^{(i)}$ sera noté $G^{[i]}$.

Soit maintenant un corps F de caractéristique $\neq p$, contenant le groupe μ_q des racines $q^{\text{ièmes}}$ de l'unité, et prenons pour G le groupe de Galois absolu G_F de F. De façon surprenante, Jan Mináč et ses collaborateurs ([**MSp**], [**EM**], [**CEM**]) ont pu établir que $G_F^{[3]}$ détermine $H^*(G_F, \mathbb{Z}/q)$ et inversement (voir les résultats précis dans le texte), en utilisant essentiellement certaines conséquences de la conjecture de Milnor (pour $p = 2$) et de Bloch-Kato (pour tout p). Rappelons que cette conjecture (maintenant le théorème de Voevodsky-Rost) stipule que le symbole galoisien établit un isomorphisme entre l'algèbre de Milnor $K_*^M(F)/q$ et l'algèbre de cohomologie $H^*(G_F, \mathbb{Z}/q)$. Le but de ce travail est de donner un aperçu des résultats de Mináč et al. et d'en redonner des démonstrations simplifiées faisant un usage systématique des techniques du problème de plongement. De fait, dans les articles [**EM**], [**CEM**] par exemple, les arguments sont purement cohomologiques, mais subtilement et ingénieusement agencés de façon à pouvoir traiter de groupes profinis plus généraux que les G_F, soumis à un nombre de conditions suffisantes minimales. De travailler avec les G_F permet une approche plus directe. La relation entre $G_F^{[3]}$ et l'algèbre de cohomologie implique des contraintes qui permettent de fabriquer des exemples de groupes profinis qui ne peuvent pas être réalisés comme groupes de Galois absolus (voir e.g. [**EM**], [**CEM**]). Notre intérêt allant plutôt vers les applications arithmétiques, nous avons, dans un dernier paragraphe, cherché à étendre l'approche précédente à des groupes de Galois avec ramification restreinte d'un corps de nombres (non-ramification en dehors des p-places). Une condition nécessaire et suffisante en vue d'une telle extension est la surjectivité d'un certain cup-produit (conjecture de McCallum-Sharifi dans [**MS**]). Une démonstration d'une version faible de cette conjecture pour les corps $\mathbb{Q}(\mu_{p^n})$ vient d'être exposée par Fukaya et Kato ([**FK**]) au colloque Iwasawa 2012 de Heidelberg.

Un mot sur la genèse de ce travail : au milieu des années 90, JanInáč était venu exposer au séminaire de Théorie des Nombres de Besançon le contenu de [**MSp**] (pour $p = 2$). À l'époque, la conjecture de Milnor-Bloch-Kato n'était pas disponible etInáč et Spira s'appuyaient sur le théorème de Merkurjev-Suslin (pour $p = 2$) en liaison avec l'anneau de Witt d'un corps F de caractéristique $\neq 2$ (le groupe $G_F^{[3]}$ était d'ailleurs baptisé "W-groupe"). Le présent auteur s'était alors persuadé qu'avec Merkurjev-Suslin pour p quelconque et un usage résolu des techniques cohomologiques, on devait pouvoir étendre [**MSp**] à p quelconque. Certains arguments et certains résultats de notre article (le théorème 2.1 en degré 2 ; le théorème 3.4 ; le théorème 4.5) sont tirés de notes rédigées (mais non publiées) pour un groupe de travail bisontin en 1996. Il n'en reste pas moins, et nous le disons clairement, que toutes les idées de fond sont dues à Mináč et al.

1. Quelques algèbres graduées

Nous rassemblons dans ce paragraphe des rappels sur quelques généralités concernant les algèbres graduées, et nous les illustrons par les deux exemples qui nous intéressent au premier chef, à savoir l'algèbre de Milnor $K_*^M(F)/q$ et l'algèbre de cohomologie $H^*(G_F, \mathbb{Z}/q)$ associées à un corps F et à une puissance q d'un nombre premier.

1.1. Algèbres graduées. — Soit R un anneau commutatif et $\mathcal{A} = \bigoplus_{r=0}^{\infty} A_r$ une R-algèbre associative, avec $A_0 = R$. Elle est graduée si $A_r . A_s \subset A_{r+s}$ pour tous $r, s \geq 0$, et anti-commutative si $ab = (-1)^{rs} ba$ pour tous $a \in A_r, b \in A_s$. Pour $r \geq 0$, on note $A_{r,dec}$ le R-sous-module de A_r engendré par tous les produits de r éléments de A_1 (par convention, $A_{0,dec} = A_0 = R$). La R-sous-algèbre graduée $\mathcal{A}_{dec} = \bigoplus_{r=0}^{\infty} A_{r,dec}$ est la partie décomposable de $\mathcal{A}$. On dit que A_r (resp. $\mathcal{A}$) est décomposable si $A_r = A_{r,dec}$ (resp. $\mathcal{A} = \mathcal{A}_{dec}$).

L'outil central introduit dans [**CEM**], inspiré de la K-théorie de Milnor, est la notion d'enveloppe quadratique $\widehat{\mathcal{A}}$: pour $r \geq 0$, soit T_r le R-sous-module de $A_1^{\otimes r}$ engendrée par tous les tenseurs $a_1 \otimes \ldots \otimes a_r$ tels qu'il existe $1 \leq i \neq j \leq r$ vérifiant $a_i a_j = 0$ dans A_2 (par convention, $A_1^{\otimes 0} = R, T_0 = 0$) ; alors $\widehat{\mathcal{A}}$ est la R-algèbre graduée $\bigoplus_{r=0}^{\infty} A_1^{\otimes r}/T_r$, la structure multiplicative étant induite par le produit tensoriel. Pratiquement par définition, on a un homomorphisme surjectif de R-algèbres graduées

$$\omega_{\mathcal{A}} \ : \ \widehat{\mathcal{A}} \to \mathcal{A}_{dec}$$

qui est l'identité en degré 1. L'algèbre $\mathcal{A}$ est dite quadratique si $\omega_{\mathcal{A}}$ est un isomorphisme.
Si $\varphi = (\varphi_r) : \mathcal{A} \to \mathcal{B}$ est un homomorphisme de R-algèbres graduées, on obtient par fonctorialité un carré commutatif

$$\begin{array}{ccc} \widehat{\mathcal{A}} & \xrightarrow{\widehat{\varphi}} & \widehat{\mathcal{B}} \\ {\scriptstyle \omega_{\mathcal{A}}}\downarrow & & \downarrow{\scriptstyle \omega_{\mathcal{B}}} \\ \mathcal{A}_{dec} & \xrightarrow{\varphi_{dec}} & \mathcal{B}_{dec} \end{array}$$

ainsi qu'un lemme évident :

Lemme 1.1. — *$\widehat{\varphi}$ est un isomorphisme si et seulement si φ_1 est un isomorphisme et $\varphi_{2,dec}$ est un homomorphisme injectif.*

1.2. Conjecture de Milnor-Bloch-Kato. — (voir e.g. [**GS**])
Soit F un corps. L'algèbre de Milnor $K_*^M(F)$ est l'anneau gradué anti-commutatif défini par les générateurs $\{a\}, a \in F^*$ et les relations

$$\{ab\} = \{a\} + \{b\}, \quad (a, b \in F^*),$$

$$\{a\} \cdot \{1 - a\} = 0 \quad (a \in F^* - \{1\}).$$

En d'autres termes, $K_*^M(F)$ est le quotient de l'algèbre tensorielle du $\mathbb{Z}$-module F^* par l'idéal bilatère engendré par les $a \otimes 1 - a$ pour $a \neq 1$. Plus concrètement, $K_0^M(F) = \mathbb{Z}$, $K_1^M(F) = F^*$, et pour $r \geq 2$, $K_r^M(F)$ est le quotient de $(F^*)^{\otimes r}$ par le sous-groupe engendré par les éléments $a_1 \otimes \ldots \otimes a_r$ tels qu'il existe un indice i satisfaisant $a_i + a_{i+1} = 1$.
Pour un nombre premier p fixé et une puissance $q = p^a$ fixée, on s'intéresse à l'algèbre $\mathcal{A}_F = K_*^M(F)/q$, qui est visiblement décomposable et quadratique : $\mathcal{A}_F = \mathcal{A}_{F,dec} = \widehat{\mathcal{A}}_F$.

Particularisons F : soit p un nombre premier fixé et $q = p^a$ comme précédemment ; supposons que F est de caractéristique $\neq p$ et contient le groupe μ_q des racines $q^{\text{ièmes}}$ de l'unité (on dira en abrégé que F vérifie les "hypothèses kummeriennes"). Le groupe de Galois absolu G_F opérant trivialement sur μ_q, notons $H^r(G_F) = H^r(G_F, \mu_q) = H^r(G_F, \mathbb{Z}/q)$ et considérons l'algèbre de cohomologie $\mathcal{B}_F = \bigoplus_{n=0}^{\infty} H^r(G_F)$, graduée par le cup-produit (et donc anti-commutative). Tate a montré que l'isomorphisme de Kummer $F^*/F^{*q} \xrightarrow{\simeq} H^1(G_F)$ peut s'étendre par cup-produit en un homomorphisme surjectif $h_F : \mathcal{A}_F \twoheadrightarrow \mathcal{B}_{F,dec}$, appelé communément symbole galoisien (voir e.g. **[GS]**, §4-6).

La conjecture de Milnor (pour $p = 2$) et Bloch-Kato (pour p quelconque) - maintenant un théorème de Voevodsky-Rost (voir e.g. **[Vo]**) - stipule que h_F est un isomorphisme. Il en résulte en particulier que $\mathcal{B}_F$ est aussi décomposable et quadratique : $\mathcal{B}_F = \mathcal{B}_{F,dec} = \widehat{\mathcal{B}}_F$.

Remarque 1.2. — La théorie de Kummer (h_F est un isomorphisme en degré 1) et le théorème de Merkurjev-Suslin (h_F est un isomorphisme en degré 2) suffisent à montrer que $\widehat{h}_F : \widehat{\mathcal{A}}_F \twoheadrightarrow \widehat{\mathcal{B}}_F$ est un isomorphisme d'après le lemme 1.1.

2. $G_F^{[3]}$ et $H^*(G_F)$

À partir de maintenant, $G = G_F$ est le groupe de Galois absolu $\mathrm{Gal}(F^{sep}/F)$ d'un corps F de caractéristique $\neq p$, contenant μ_q (avec $q = p^a$). On se référera à ces hypothèses comme étant les "hypothèses kummeriennes". On se propose de redonner une démonstration simplifiée (car plus directe) du résultat principal de Chebolu-Efrat-Mináč : $G_F^{[3]}$ détermine $H^*(G_F)$, et réciproquement.

Théorème 2.1 **([CEM], thm A)**. — *Sous les hypothèses kummeriennes, l'inflation induit un isomorphisme* $H^*(G_F^{[3]})_{dec} \xrightarrow{\simeq} H^*(G_F)$.

La démonstration de ce théorème va se faire en deux étapes : une première étape s'arrête au second degré de l'algèbre graduée $H^*(G_F)$ et utilise seulement le résultat de Merkurjev-Suslin ; une seconde étape passe de l'algèbre tronquée à l'algèbre $H^*(G_F)$ entière en exploitant certaines conséquences du théorème de Voevodsky-Rost. Notre outil technique sera la théorie du plongement des extensions de corps, dont voici un bref rappel :

2.1. Sur le problème du plongement. — (indépendamment des hypothèses kummeriennes). Soit K/F une extension galoisienne, de groupe de Galois H, et soit $1 \to A \to E \to H \to 1$ une extension de groupes. Le problème de plongement *fort* relatif à ces deux extensions (de corps et de groupes) consiste à trouver une surextension galoisienne $L/K/F$ telle que l'extension de groupes de Galois ainsi obtenue soit équivalente à l'extension de départ, i.e. qu'on ait un diagramme commutatif :

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \mathrm{Gal}(L/K) & \longrightarrow & \mathrm{Gal}(L/F)) & \longrightarrow & \mathrm{Gal}(K/F) & \longrightarrow & 1 \\ & & \downarrow \wr & & \downarrow \wr & & \| & & \\ 1 & \longrightarrow & A & \longrightarrow & E & \longrightarrow & H & \longrightarrow & 1 \end{array}$$

Cela équivaut à trouver un morphisme surjectif $\varphi : G_F \to E$ qui fasse commuter le diagramme :

$$\begin{array}{ccccccccc} & & & & G_F & & & & \\ & & & \swarrow^{\varphi} & \downarrow & & & & \\ 1 & \longrightarrow & A & \longrightarrow & E & \longrightarrow & H & \longrightarrow & 1 \end{array}$$

Pour des raisons techniques, il convient d'étudier le problème de plongement *faible* associé, obtenu en enlevant la condition de surjectivité sur φ, ce qui revient à remplacer les extensions de corps par des extensions d'algèbres galoisiennes (au sens de Hasse).

Remarque 2.2. — Si E et H sont des pro-p-groupes ayant le même nombre minimal de générateurs, les problèmes fort et faible sont équivalents.

Si le noyau A est abélien et est un H-module discret, la cohomologie galoisienne permet de donner un critère commode d'existence d'une solution au problème de plongement : l'extension de groupes de départ est décrite à équivalence près par une classe de cohomologie $\varepsilon \in H^2(H, A)$, et le critère de Hoechsmann ([**H**], 2-1) dit que le problème de plongement (faible) associé possède une solution si et seulement si $\inf(\varepsilon) = 0$, où inf désigne l'inflation de H à G_F.

2.2. Démonstration du théorème 2.1 - Première étape. — Les groupes G_F et $G_F^{[i]}$ admettent tous $G_F^{[2]}$ comme pro-p-quotient abélien maximal d'exposant q. Par dualité, il s'ensuit immédiatement que les inflations $H^1(G_F^{[2]}) \to H^1(G_F^{[3]}) \to H^1(G_F)$ sont des isomorphismes. Passons aux H^2. Le diagramme commutatif de cup-produits et d'inflations

$$\begin{array}{ccc} & & H^2(G_F) \\ & \nearrow & \uparrow \\ H^1(G_F) \otimes H^1(G_F) & \longrightarrow & H^2(G_F^{[3]}) \\ & \searrow & \uparrow \\ & & H^2(G_F^{[2]}) \end{array}$$

montre que l'homomorphisme naturel $H^2(G_F^{[3]})_{dec} \longrightarrow H^2(G_F)_{dec}$ est surjectif.
Pour comparer les noyaux des inflations

$$\inf_{2,3} \ : \ H^2(G_F^{[2]}) \longrightarrow H^2(G_F^{[3]})$$

et

$$\inf_{2,\infty} \ : \ H^2(G_F^{[2]}) \longrightarrow H^2(G_F),$$

appliquons les techniques du problème de plongement. Soit F_i le corps fixe de $G_F^{(i)}$. D'après le critère de Hoechsmann, une classe ε appartient à Ker $(\inf_{2,\infty})$ si et seulement si le problème de plongement associé à $G_F^{[2]}$ et ε possède une solution, i.e. s'il existe une surextension galoisienne $L/F_2/F$ telle que l'extension de groupes de Galois $1 \to \mathrm{Gal}\ (L/F_2) \to \mathrm{Gal}\ (L/F) \to \mathrm{Gal}\ (F_2/F) \to 1$ soit aussi décrite par la classe ε.
Mais, à cause de la maximalité de $G_F^{[2]}$, un tel $\mathrm{Gal}(L/F)$ est évidemment un quotient de $G_F^{[3]}$, autrement dit le problème de plongement possède une solution dans F^{sep} si, et seulement si, il possède une solution dans F_3. Donc $\mathrm{Ker}(\inf_{2,3}) = \mathrm{Ker}(\inf_{2,\infty})$ et $H^2(G_F^{[3]})_{dec} \xrightarrow{\simeq} H^2(G_F)_{dec}$. Comme l'algèbre $H^2(G_F)$ est décomposable d'après Merkurjev-Suslin, on a montré l'isomorphisme du théorème 2.1 jusqu'au second cran.

2.3. Seconde étape. — Pour passer du second cran à l'algèbre entière $H^*(G_F)$, l'idée de **[CEM]** est de passer par les enveloppes quadratiques. Soit π la projection $G_F \to G_F^{[3]}$. On vient de voir que $\pi_1^* : H^1(G_F^{[3]}) \to H^1(G_F)$ et $\pi_{dec,2}^* : H^2(G_F^{[3]})_{dec} \to H^2(G_F)_{dec}$ sont des isomorphismes. Il résulte alors du lemme 1.1 que $\widehat{\pi}^* : \widehat{H^*(G_F^{[3]})} \to \widehat{H^*(G_F)}$ est un isomorphisme. Le carré commutatif qui permet de comparer les algèbres quadratiques et décomposables (fin du § 1) s'écrit ici :

$$\begin{array}{ccc} \widehat{H^*(G_F^{[3]})} & \xrightarrow[\simeq]{\widehat{\pi}^*} & \widehat{H^*(G_F)} \\ \downarrow & & \downarrow \\ H^*(G_F^{[3]})_{dec} & \xrightarrow[\pi_{dec}^*]{} & H^*(G_F)_{dec} \end{array}$$

Mais l'algèbre $H^*(G_F)$ est à la fois quadratique et décomposable d'après Voevodsky-Rost, et en particulier la flèche verticale de droite est un isomorphisme. Une simple chasse dans le diagramme montre alors que la flèche verticale de gauche est aussi un isomorphisme, et donc π_{dec}^* est un isomorphisme, ce qui termine la preuve du théorème 2.1.

***Corollaire 2.3* ([CEM], thm. 6-5).** — *L'algèbre $H^*(G_F^{[3]})$ est quadratique.*

Pour énoncer une réciproque du théorème 2.1, il est commode de faire varier le corps de base :

***Théorème 2.4* ([CEM], thm. C).** — *Soient deux corps F_1, F_2 vérifiant les hypothèses kummeriennes, et soit un homomorphisme continu $\pi : G_{F_1} \to G_{F_2}$. Les propriétés suivantes sont équivalentes :*
(i) Le morphisme induit $\pi^* : H^*(G_{F_2}) \longrightarrow H^*(G_{F_1})$ est un isomorphisme.
(ii) Le morphisme induit $\pi^{[3]} : G_{F_1}^{[3]} \longrightarrow G_{F_2}^{[3]}$ est un isomorphisme.

Démonstration. — L'implication $(ii) \Rightarrow (i)$ résulte facilement du théorème 2.1. Montrons seulement l'implication inverse. En abrégeant systématiquement G_{F_i} en G_i, le morphisme $\pi^{[3]}$ prend place dans un diagramme commutatif :

$$\begin{array}{ccccccccc} 1 & \longrightarrow & G_1^{(2)}/G_1^{(3)} & \longrightarrow & G_1^{[3]} & \longrightarrow & G_1^{[2]} & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle \overline{\pi}} & & \downarrow{\scriptstyle \pi^{[3]}} & & \downarrow{\scriptstyle \pi^{[2]}} & & \\ 1 & \longrightarrow & G_2^{(2)}/G_2^{(3)} & \longrightarrow & G_2^{[3]} & \longrightarrow & G_2^{[2]} & \longrightarrow & 1 \end{array}$$

et l'isomorphie de $\pi^{[3]}$ proviendra de celle de $\pi^{[2]}$ et $\overline{\pi}$. Or :

- d'après (i), le morphisme $\pi_1^* \ : \ H^1(G_2) \longrightarrow H^1(G_1)$ est un isomorphisme, donc, par dualité, le morphisme $\pi^{[2]} \ : \ G_1^{[2]} \longrightarrow G_2^{[2]}$ est un isomorphisme.
- le morphisme $\overline{\pi} \ : \ G_1^{(2)}/G_1^{(3)} \longrightarrow G_2^{(2)}/G_2^{(3)}$ est visiblement dual du morphisme $(\pi^{(2)})_1^* \ : \ H^1(G_2^{(2)})^{G_2} \longrightarrow H^1(G_1^{(2)})^{G_1}$. Or, dans le diagramme commutatif (où trg est la transgression) :

$$\begin{array}{ccccccc} 0 & \longrightarrow & H^1(G_2^{(2)})^{G_2} & \xrightarrow{\text{trg}} & H^2(G_2^{[2]}) & \xrightarrow{\text{inf}} & H^2(G_2) \\ & & \downarrow{\scriptstyle (\pi^{(2)})_1^*} & & \downarrow{\scriptstyle (\pi^{[2]})_2^*} & & \downarrow{\scriptstyle \pi_2^*} \\ 0 & \longrightarrow & H^1(G_1^{(2)})^{G_1} & \xrightarrow{\text{trg}} & H^2(G_1^{[2]}) & \xrightarrow{\text{inf}} & H^2(G_1) \end{array}$$

on sait que π_2^* est un isomorphisme d'après (i) et que $(\pi^{[2]})_2^*$ est un isomorphisme par dualité à partir de $\pi^{[2]}$. Donc $(\pi^{(2)})_1^*$ est un isomorphisme, et l'implication $(i) \Rightarrow (ii)$ est démontrée.

□

Sous les hypothèses kummeriennes, la connaissance de l'algèbre de cohomologie $H^*(G_F)$ en entier se ramène donc à celle du "petit quotient" $G_F^{[3]}$. On va donner deux approches possibles de $G_F^{[3]}$: par générateurs et relations ; par la théorie de Galois.

3. Description de $G_F^{[3]}$ par générateurs et relations

On garde les hypothèses et les notations du § 2. On désigne par $\mathcal{G}_F$ le pro-p-quotient maximal de G_F.
Comme $G_F^{[i]} = \mathcal{G}_F^{[i]}$ de façon évidente, il est naturel de prendre comme point de départ une présentation de $\mathcal{G}_F$ par générateurs et relations, i.e. une suite exacte $1 \to R \to S \to \mathcal{G}_F \to 1$, où S est un pro-p-groupe libre.

3.1. Rappels sur les présentations par générateurs et relations. —
Soit $\mathcal{G}$ un pro-p-groupe. Une présentation $1 \to R \to S \to \mathcal{G} \to 1$ est dite minimale si le morphisme induit $S^{[2]} \twoheadrightarrow \mathcal{G}^{[2]}$ est un isomorphisme, ce qui revient à dire que $R \leq S^{(2)}$. Une présentation minimale n'existe pas forcément. Elle existe par exemple si $\mathcal{G}^{[2]}$ est de la forme $(\mathbb{Z}/q)^I$ (où I est un ensemble d'indices), ce qui est toujours le cas si $q = p$ (théorème de Burnside).

Lemme 3.1. — *Sous les hypothèses kummeriennes, $\mathcal{G}_F$ possède une présentation minimale.*

Démonstration. — Rappelons que $q = p^a$.
L'homomorphisme naturel $F^*/F^{*q} \to F^*/F^{*p^i}$ étant surjectif pour tout $1 \leq i \leq a$, la théorie de Kummer entraîne que le morphisme fonctoriel $H^1(\mathcal{G}_F, \mathbb{Z}/q) \to H^1(\mathcal{G}_F, \mathbb{Z}/p^i)$ est aussi surjectif pour tout $1 \leq i \leq a$, donc $\mathcal{G}_F^{[2]}$ est bien de la forme $(\mathbb{Z}/q)^I$. □

Passons au troisième cran. De la présentation donnée, on déduit immédiatement une suite exacte $1 \to RS^{(3)}/S^{(3)} \to S^{[3]} \to \mathcal{G}^{[3]} \to 1$, ce qui donne une description de $\mathcal{G}^{[3]}$ par générateurs (le groupe $S^{[3]}$) et relations (le noyau $RS^{(3)}/S^{(3)} \simeq R/R \cap S^{(3)}$). Si la présentation de $\mathcal{G}$ est minimale et si en outre $\mathcal{G}$ est de type fini topologiquement, on peut décrire les relations de $RS^{(3)}/S^{(3)}$ par le pro-p-analogue du procédé "d'assemblage" de M. Hall.
Introduisons d'abord quelques notations. Soit $1 \to R \to S \to \mathcal{G} \to 1$ une présentation minimale. La suite exacte de Hochschild-Serre s'écrit :

$$0 \longrightarrow H^1(\mathcal{G}) \xrightarrow[\simeq]{\inf} H^1(S) \xrightarrow{\text{res}} H^1(R)^{\mathcal{G}} \xrightarrow{\text{trg}} H^2(\mathcal{G}) \longrightarrow H^2(S) = 0,$$

où trg désigne la transgression ; en bref, $H^1(R)^{\mathcal{G}} \xrightarrow[\simeq]{\text{trg}} H^2(\mathcal{G})$.
Soit $\{s_i \mid i \in I\}$ un système minimal de générateurs topologiques de S, et soit $\{r_j \mid j \in J\}$ un système minimal de relations (i.e. un système minimal d'éléments de R qui engendrent R comme sous-groupe fermé distingué).
Pour tout $j \in J$, on peut définir un homomorphisme $\varphi_j : H^2(\mathcal{G}) \to \mathbb{Z}/q$ par $\varphi_j(\alpha) = (\text{trg}^{-1}(\alpha))(r_j)$. On peut aussi définir une base $\{\chi_\nu \mid \nu \in I\}$ de $H^1(\mathcal{G})$ par $\chi_\nu(s_\mu) = \delta_{\nu,\mu}$ pour $\nu, \mu \in I$. Alors :

***Proposition 3.2* ([K], satz 7.23)**. — *Si la présentation $1 \to R \to S \to \mathcal{G} \to 1$ est minimale et si $\mathcal{G}$ est topologiquement de type fini (i.e. I est fini, disons $I = \{1, 2, \ldots, d\}$), alors $RS^{(3)}/S^{(3)}$ est engendré par les classes r_j mod $S^{(3)} = \prod_{\kappa=1}^{d} s_\kappa^{qa_{j\kappa}} \prod_{\nu<\mu} [s_\nu, s_\mu]^{a_{j\nu\mu}}$ mod $S^{(3)}$, pour $j \in J$ et $\nu, \mu = 1, 2, \ldots, d$. Les exposants dans cette formule sont donnés par $a_{j\nu\mu} = -\varphi_j(\chi_\nu \cup \chi_\mu)$ si $\nu < \mu$, $a_{j,\kappa} = -\varphi_j(B\chi_\kappa)$, où $B : H^1(\mathcal{G}) \to H^2(\mathcal{G})$ est l'homomorphisme de Bockstein associé à la suite exacte $0 \longrightarrow \mathbb{Z}/q \xrightarrow{q} \mathbb{Z}/q^2 \longrightarrow \mathbb{Z}/q \longrightarrow 0$.*

Corollaire 3.3. — *Sous les hypothèses de la proposition 3.2, $\mathcal{G}^{[3]}$ est uniquement déterminé par $H^1(\mathcal{G})$, par le cup-produit $H^1(\mathcal{G}) \otimes H^1(\mathcal{G})$ et par le morphisme Bockstein $H^1(\mathcal{G}) \longrightarrow H^2(\mathcal{G})$.*

La proposition 3.2 est plus précise que le théo. B de **[CEM]** (voir ci-après), mais son application est limitée par l'hypothèse "de type fini", qui n'est pas vérifiée par tous les groupes de Galois (voir cependant le § 5). On pourrait peut-être se débarrasser de cette hypothèse en faisant des raisonnements d'induction et de convergence, mais il paraît plus simple de procéder directement en exploitant le théorème 2.1.

Théorème 3.4. — *Sous les hypothèses kummeriennes, soit $1 \longrightarrow R \longrightarrow S \longrightarrow \mathcal{G}_F \longrightarrow 1$ une présentation minimale. On a un diagramme commutatif où les lignes sont des accouplements parfaits :*

$$\begin{array}{ccccc} H^2(G_F) & \times & RS^{(3)}/S^{(3)} & \longrightarrow & \mathbb{Z}/q \\ \uparrow\!\!\uparrow & & \downarrow & & \| \\ H^2(G_F^{[2]}) & \times & S^{(2)}/S^{(3)} & \longrightarrow & \mathbb{Z}/q \end{array}$$

L'orthogonal de $RS^{(3)}/S^{(3)}$ dans l'accouplement du bas s'identifie à $H^1(G_F^{(2)})^{G_F}$.

Démonstration. — Pour simplifier, on omet l'indice F dans l'écriture des groupes de Galois. Par Hochschild-Serre, on a un diagramme commutatif

$$\begin{array}{ccccccccc} 0 & \longrightarrow & H^1(G^{(2)})^G & \xrightarrow{\text{trg}} & H^2(G^{[2]}) & \xrightarrow{\text{inf}} & H^2(G) & \longrightarrow & 0 \\ & & \downarrow & & \downarrow\wr & & & & \\ & & H^1(S^{(2)})^S & \xrightarrow[\text{trg}]{\sim} & H^2(S^{[2]}) & & & & \end{array}$$

La seconde ligne est un isomorphisme parce que $H^1(S^{[2]}) \xrightarrow{\sim} H^1(S)$ et $H^2(S) = 0$. Dans la première ligne, la transgression est injective parce que $H^1(G^{[2]}) \xrightarrow{\sim} H^1(G)$ et l'inflation est surjective d'après le théorème 2.1 (ou même seulement la première étape de sa démonstration). L'injectivité de la première flèche verticale s'obtient par dualité à partir de la surjectivité de $S^{(2)} \longrightarrow G^{(2)}$. La seconde flèche est un isomorphisme car $S^{[2]} \xrightarrow{\sim} G^{[2]}$ par minimalité de la présentation par générateurs et relations. Par dualité, on obtient un diagramme commutatif d'accouplements parfaits :

$$\begin{array}{ccccc} H^1(R)^S & \times & R/R^q[R,S] & \longrightarrow & \mathbb{Z}/q \\ \uparrow\!\!\uparrow & & \downarrow & & \| \\ H^1(S^{(2)})^S & \times & S^{(2)}/S^{(3)} & \longrightarrow & \mathbb{Z}/q \\ \uparrow & & \downarrow\!\!\downarrow & & \| \\ H^1(G^{(2)})^G & \times & G^{(2)}/G^{(3)} & \longrightarrow & \mathbb{Z}/q \end{array}$$

Dans la colonne de gauche, la flèche $H^1(G^{(2)})^G \hookrightarrow H^1(S^{(2)})^S$ est la première flèche verticale du diagramme commutatif de départ. En appliquant le lemme du serpent dans ce diagramme, on voit que le conoyau s'identifie à $H^2(G)$, qui est isomorphe à $H^1(R)^S$ par la transgression à cause de la minimalité de la présentation. La colonne de droite se déduit par dualité de celle de gauche. En particulier, comme $R \subset S^{(2)}$ par minimalité (et donc $R^q[R,S] \subset S^{(3)}$), l'image de la flèche $R/R^q[R,S] \longrightarrow S^{(2)}/S^{(3)}$ est $RS^{(3)}/S^{(3)}$ et son noyau est $R \cap S^{(3)}$. On en déduit que $R \cap S^{(3)} = R^q[R,S]$, et le théorème est démontré. □

***Corollaire 3.5* ([CEM], thm. 8-3).** — *Sous les hypothèses du théorème 3.4, on a*

$$R \cap S^{(3)} = R^q[R,S].$$

***Corollaire 3.6* ([CEM], thm. B).** — *Sous les hypothèses kummeriennes, $G_F^{[3]}$ est uniquement déterminé par $H^1(G_F)$ et le cup-produit sur $H^1(G_F) \otimes H^1(G_F)$.*

Démonstration. — $H^1(G_F)$ est dual de $G_F^{[2]}$, qui détermine le pro-p-groupe libre S de la présentation minimale $1 \longrightarrow R \longrightarrow S \longrightarrow \mathcal{G}_F \longrightarrow 1$. D'après le théorème 3.4, $RS^{(3)}/S^{(3)}$ est dual de $H^2(G_F)$, qui est l'image du cup-produit d'après le théorème 2.1 (ou même seulement sa version tronquée au second cran). □

***Remarque 3.7*.** — En réalité, le théorème B de **[CEM]** ajoute le morphisme de Bockstein $B : H^1(G_F) \longrightarrow H^2(G_F)$ (voir la proposition 3.2) aux paramètres déterminant $G_F^{[3]}$. Mais en fait, B est aussi un cup-produit, au sens suivant : soit κ_q l'homomorphisme de Kummer $F^* = H^0(G_F, (F^{sep})^*) \longrightarrow H^1(G_F, \mu_q)$, qu'on restreint à $\mu_q = H^0(G_F, \mu_q)$; en identifiant μ_q à $\mathbb{Z}/q$, on sait que pour tout $\psi \in H^1(G_F)$, $B(\psi) = \psi \cup \kappa_q(\zeta_q)$ dans $H^2(G_F)$ (**[EM]**, preuve de la proposition 3-2).

4. Description galoisienne de $G_F^{[3]}$

Toujours sous les hypothèses kummeriennes, et pour $q = p$, $G_F^{[3]}$ est le groupe de Galois sur F d'une extension galoisienne F_3 (le corps fixe de $G^{(3)}$) qui a été déterminée explicitement par Villegas (**[Vi]**) et par Mináč et Spira (**[MSp]**) pour $p = 2$, puis par Efrat et Mináč (**[EM]**) pour tout p. Ces deux derniers auteurs utilisent les techniques du problème de plongement, mais du point de vue des groupes (voir les rappels du § 2) car ils s'intéressent à des groupes profinis plus généraux que G_F, vérifiant des relations "de type galoisien" qui axiomatisent certaines propriétés de G_F (**[EM]**, § 3). Pour G_F lui-même, on va voir que les techniques kummeriennes de plongement des extensions de corps permettent d'arriver plus rapidement (car plus directement) au résultat.

4.1. Plongement d'une extension de corps. — On suppose que F vérifie les hypothèses kummeriennes (avec q une puissance de p). Soit K/F une extension galoisienne, de groupe H. Soit $L = K(\sqrt[q]{a})$, $a \in K^*$, une extension kummerienne de K. Notons que L dépend seulement de la classe $\overline{a} \in K^*/K^{*q}$.

***Lemme 4.1*.** — *Pour que l'extension L/F soit galoisienne, il faut et il suffit que $\overline{a}$ soit fixé par H : $\overline{a} \in (K^*/K^{*q})^H$.*

Démonstration. — Exercice de théorie de Galois. □

Pour qu'une classe $\overline{a} \in K/K^{*q}$ soit fixée par H, il faut et il suffit que $\forall\ \sigma \in H$, $\sigma(a)/a$ soit de la forme β_σ^q, avec $\beta_\sigma \in K^*$. Alors l'application $(\sigma, \tau) \mapsto \sigma(\beta_\tau)\beta_\sigma/\beta_{\sigma\tau}$ définit un 2-cocycle $\alpha_{\sigma,\tau}$ à valeurs dans μ_q.
Avec ces notations, on peut décrire la transgression $H^1(N)^H \to H^2(H)$, où N est le sous-groupe fermé distingué tel que $H = G_F/N = \mathrm{Gal}(K/F)$:

***Proposition 4.2* ([MN], théo. 4).** — *Sous les hypothèses kummeriennes, pour toute classe $\overline{a} \in H^1(N)^H$, $\mathrm{trg}\ (\overline{a})$ est la classe dans $H^2(H)$ du cocyle $\alpha_{\sigma,\tau}$ précédemment défini. Plus fonctoriellement, on a deux suites exactes canoniques :*

$$\longrightarrow F^*/F^{*q} \xrightarrow{nat} (K^*/K^{*q})^H \xrightarrow{\delta_0} H^1(H, K^{*q}) \longrightarrow H^1(H, K^*) = 0$$

et

$$0 \longrightarrow H^1(H, K^{*q}) \xrightarrow{\delta_1} H^2(H, \mu_q) \longrightarrow H^2(H, K^*) \longrightarrow$$

Démonstration. — Les deux suites cherchées proviennent par cohomologie des suites exactes de H-modules $1 \longrightarrow K^{*q} \longrightarrow K^* \longrightarrow K^*/K^{*q} \longrightarrow 1$ et $1 \longrightarrow \mu_q \longrightarrow K^* \longrightarrow K^{*q} \longrightarrow 1$. En sachant que $K^*/K^{*q} \simeq \text{ Hom } (N, \mu_q)$ et en identifiant μ_q à $\mathbb{Z}/q$, la transgression s'identifie évidemment à $\delta_1\delta_0$. Les calculs explicites proviennent du lemme 4.1. □

Dans la suite, on aura besoin de connaître l'image de la transgression dans un cas particulier :

Corollaire 4.3. — *Supposons en outre que H est cyclique. Alors l'image de la transgression est isomorphe à $(\mu_q \cap \mathrm{N}(K^*))/\mathrm{N}(\mu_q)$, où* N *est la norme de K/F.*

Démonstration. — D'après la proposition 4.2, on a une suite exacte :

$$(K^*/K^{*q})^H \xrightarrow{\delta_1\delta_0} H^2(H) \longrightarrow H^2(H, K^*)$$

Si H est cyclique, l'image de $\delta_1\delta_0$ est le noyau de $\mu_q/\mathrm{N}(\mu_q) \longrightarrow K^*/\mathrm{N}(K^*)$. □

4.2. Rappels sur la décomposition de $H^2(H)$ dans le cas abélien. — Si H est un groupe abélien fini opérant trivialement sur un module A, un 2-cocycle f est dit symétrique si $f(\sigma, \tau) = f(\tau, \sigma)$ pour tout $(\sigma, \tau) \in H \times H$. Tout 2-cobord étant symétrique, on peut définir $H^2(H, A)_{sym}$ comme étant le sous-groupe de $H^2(H, A)$ formé des classes de cocyles symétriques. Définissons aussi $\mathrm{Alt}(H, A)$ comme étant le groupe des applications $\mathbb{Z}$-bilinéaires $g : H \times H \longrightarrow A$ qui sont alternées, i.e. qui vérifient $g(\sigma, \sigma) = 0$ pour tout $\sigma \in H$ (alors g est anti-symétrique). Les résultats de décomposition suivants peuvent s'obtenir par des calculs directs de cocyles ([**Y**], thm 2.1) ou par des raisonnements plus fonctoriels faisant intervenir notamment le morphisme de Bockstein relatif à la suite exacte $0 \to \mathbb{Z}/q \to \mathbb{Z}/q^2 \to \mathbb{Z}/q \to 0$ ([**EM**], propos. 2.8) :

Proposition 4.4. —
(*i*) *Soit H un groupe abélien fini, opérant trivialement sur un module A. Alors,*

$$H^2(H, A) \simeq H^2(H, A)_{sym} \oplus \mathrm{Alt}(H, A).$$

(*ii*) *Si $H = \bigoplus_{i=1}^{n} H_i$, chaque H_i étant cyclique d'ordre q, alors*

$$H^2(H)_{sym} \simeq \bigoplus_{i=1}^{n} B(H^1(H_i))$$

et

$$H^2(H, A) \simeq H^2(H, A)_{sym} + H^2(H, A)_{dec}.$$

Si $q = 2$, $H^2(H, A) = H^2(H, A)_{dec}$.

On se propose maintenant de redémontrer par les techniques de plongement d'extensions de corps le résultat principal d'Efrat et Mináč. Une extension galoisienne sera dite de type X si son groupe de Galois est isomorphe à X.

***Théorème 4.5* ([EM], thm. 11.1).** — *On se place dans les hypothèses kummeriennes, avec $q = p$. Soit F_3 le corps fixe de $G_F^{(3)}$. Alors*
(i) Si $p = 2$, l'extension F_3/F est la composée de toutes les extensions galoisiennes de F qui sont de type $\mathbb{Z}/2$, $\mathbb{Z}/4$ et D_8.
(ii) Si $p \neq 2$, l'extension F_3/F est la composée de toutes les extensions galoisiennes de F qui sont de type $\mathbb{Z}/p$, $\mathbb{Z}/p^2$ et M_{p^3}, où M_{p^3} est le groupe extra-spécial d'ordre p^3 et d'exposant p^2.

Remarquons d'abord que, puisque $G_F^{[2]}$ est d'exposant p, l'extension F_2/F est la composée de toutes les extensions de F de type $\mathbb{Z}/p$. Il s'agit donc seulement de passer de F_2 à F_3 par les méthodes du plongement kummerien.

4.3. Plongement dans des extensions de degré p^2 ou p^3. — D'après le critère de Hoechsmann et le sous-paragraphe 4.2, on doit déterminer le noyau de l'inflation $H^2(G_F^{[2]}) \longrightarrow H^2(G_F)$. D'après la proposition 4.4 (ii), cela revient à résoudre des problèmes de plongement sur F associés à des classes $\varepsilon \in B(H^1(C_p)) = H^2(C_p)$ ou à des cup-produits $\alpha \cup \beta$, où $\alpha, \beta \in H^1(C_p)$ et C_n désigne le groupe cyclique d'ordre n.

4.3.1. Solutions abéliennes. — Elles sont classifiées par les classes de cocycles symétriques. Dans notre cas, grâce à la proposition 4.4 (ii), nous aurons seulement à résoudre des problèmes de plongement sur F associés à des classes de $H^2(C_p)$. Autrement dit, à trouver, pour une extension $K = F(\sqrt[p]{a})$ de type C_p, une surextension $L/K/F$ de type $C_p \times C_p$ ou C_{p^2}. Une solution au premier problème consiste évidemment à composer K avec une autre extension $F(\sqrt[p]{b})$ de type C_p. Le second problème consiste à tuer $\inf(B(\psi_a))$, où ψ_a est le caractère de Kummer associé à K. D'après le corollaire 4.3, il admet une solution si et seulement si $\zeta_p \in \mathrm{N}(K^*)$, ζ_p désignant une racine primitive $p^{\text{ième}}$ de l'unité.

4.3.2. Solutions non abéliennes. — Ce sont d'éventuelles surextensions non abéliennes de degré p^3, où $K = F(\sqrt[p]{a}, \sqrt[p]{b})$ est de type $C_p \times C_p$. Notre référence standard sera la partie purement algébrique de [**MN**]. Rappelons d'abord la structure des groupes non abéliens d'ordre p^3, qui sont :
(i) Si $p = 2$:

- le groupe diédral $\mathrm{D}_8 =< r, s | r^4 = s^2 = (rs)^2 = 1 >$. Un seul des trois sous-groupes d'ordre 4 est cyclique.
- le groupe quaternionien $\mathrm{H}_8 =< r, s | r^4 = 1, [r, s] = r^2 = s^2 >$. Les trois sous-groupes d'ordre 4 sont cycliques.

(i) Si $p \neq 2$:

- le groupe extra-spécial d'ordre p^3 et d'exposant p^2,

$$\mathrm{M}_{p^3} =< r, s | r^{p^2} = s^p = 1, [r, s] = r^p > .$$

Un seul des $(p + 1)$ sous-groupes d'ordre p^2 est non cyclique.

- le groupe de Heisenberg d'ordre p^3 et d'exposant p,

$$\mathrm{H}_{p^3} =< r, s, t | r^p = s^p = t^p = 1, [r,t] = [s,t] = 1, [r,s] = t > .$$

Les $(p+1)$ sous-groupes d'ordre p^2 sont non cycliques.

Les deux cas se traitent de la même façon par les techniques de plongement. Si $p = 2$ (resp. $p \neq 2$), il s'agit de plonger l'extension biquadratique $K = F(\sqrt{a}, \sqrt{b})$) (resp. l'extension de type $C_p \times C_p$, $K = F(\sqrt[p]{a}, \sqrt[p]{b})$) dans une surextension L/F galoisienne de degré p^3, d'un des types précédemment décrits. Pour abréger, on étudiera seulement le cas $p \neq 2$ (en principe, d'après la proposition 4.4, on n'aurait même pas besoin de considérer le type H_{p^3}). Les raisonnements algébriques de [**MN**], théorème 14, donnent sans difficulté le résultat suivant :

Proposition 4.6. — *Soit $K = F(\sqrt[p]{a}, \sqrt[p]{b})$; soit $H = Gal(K/F)$, de type $C_p \times C_p$, engendré par σ et τ tels que $\sigma(\sqrt[p]{a})/\sqrt[p]{a} = \tau(\sqrt[p]{b})/\sqrt[p]{b} = \zeta_p$, $\sigma(\sqrt[p]{b})/\sqrt[p]{b} = \tau(\sqrt[p]{a})/\sqrt[p]{a} = 1$. Notons ψ_a, ψ_b les caractères de Kummer associés à $F(\sqrt[p]{a})/F$ et à $F(\sqrt[p]{b})/F$.*
(i) Une extension de H de type H_{p^3} est classifiée par $\psi_a \cup \psi_b$. Le problème de plongement associé possède une solution si et seulement si a est une norme de $F(\sqrt[p]{b})/F$ (ou b est une norme de $F(\sqrt[p]{a})/F$; c'est une relation symétrique).
(ii) Une extension de H de type M_{p^3} est classifiée par $B(\psi_a) + (\psi_a \cup \psi_b)$, en convenant que dans la présentation de M_{p^3}, le seul sous-groupe de type (p,p) de M_{p^3} est engendré par r^p et s, r s'envoyant sur σ et s sur τ. Le problème de plongement associé possède une solution si, et seulement si, il existe $c, d \in F^*$ tels que $K = F(\sqrt[p]{c}, \sqrt[p]{d})$ et $\zeta_p d$ soit une norme dans $F(\sqrt[p]{c})/F$.

Remarque 4.7. — Contrairement à ce qui se passe d'habitude, le cas $p = 2$ est moins compliqué car, dans ce cas, le Bockstein est nul.

Le théorème 4.5 est ainsi démontré. Pour compléter l'étude, disons comment la proposition 4.2 permet de construire les surextensions cherchées quand elles existent, i.e. quand les conditions dans 4.6 (i), (ii) et dans la section 4.3.1 sont remplies. On se limite à $p \neq 2$ pour abréger.

Proposition 4.8. — *On garde les notations de la proposition 4.6 : $K = F(\sqrt[p]{a}, \sqrt[p]{b})$, etc.*
(i) Si $y \in F(\sqrt[p]{a})$ vérifie $\mathrm{N}(y) = b$, posons $x = y.\sigma(y^2)\ldots\sigma^{p-2}(y^{p-1})$. Alors $\delta_1(\delta_0(\overline{x})) = \psi_a \cup \psi_b$.
(ii) Si $y \in F(\sqrt[p]{a})$ vérifie $\mathrm{N}(y) = \zeta_p b$, posons $x = \sqrt[p]{a}.y.\sigma(y^2)\ldots\sigma^{p-2}(y^{p-1})$. Alors $\delta_1(\delta_0(\overline{x})) = B(\psi_a) + (\psi_a \cup \psi_b)$.

Démonstration. — Simples calculs à partir de la proposition 4.2. □

4.4. Digression. — Les résultats précédents s'appliquent manifestement à des extensions plus générales que F_3/F_2. Par exemple, pour toute extension abélienne K/F, de groupe H, contenant F_2, la proposition 4.8 (et son analogue pour $p = 2$) permettent de déterminer $(K^*/K^{*p})^H$. Mais cette description, bien qu'"explicite", n'est pas assez "canonique" pour permettre de dégager éventuellement une famille remarquable de générateurs. Pour nous en

convaincre, examinons de près un exemple qui nécessite des renseignements d'ordre arithmétique : $F = \mathbb{Q}$, $K = \mathbb{Q}^{ab}$, $H = \mathrm{Gal}\,(\mathbb{Q}^{ab}/\mathbb{Q}) = G_{\mathbb{Q}}^{ab}$, $p = 2$. Par maximalité de $\mathbb{Q}^{ab}$, il est clair d'après les propositions 4.2 et 4.4 que

$$(K^*/K^{*2})^H \simeq \mathrm{Alt}\ (H, \mathbb{Z}/2) = \bigwedge^2 H^1(H, \mathbb{Z}/2) \simeq \bigwedge^2 (\mathbb{Q}^*/\mathbb{Q}^{*2}).$$

Une base canonique du $\mathbb{F}_2$-espace vectoriel $(K^*/K^{*2})^H$ a été construite par G. Anderson ([**A**], main thm.).
Fixons quelques notations : soit $\mathcal{A}$ le groupe abélien libre sur les symboles $[a] \in \mathbb{Q}/\mathbb{Z}$; pour tous nombres premiers $r < q$, posons

- si $r \neq 2$, $a_{rq} = \sum_{i=1}^{\frac{r-1}{2}} \left([\frac{i}{r}] - \sum_{k=0}^{\frac{q-1}{2}} [\frac{i}{rq} + \frac{k}{q}] \right) - \sum_{j=1}^{\frac{q-1}{2}} \left([\frac{j}{q}] - \sum_{h=0}^{\frac{r-1}{2}} [\frac{j}{rq} + \frac{h}{p}] \right)$

- si $r = 2, a_{2q} = \left([\frac{1}{4}] - \sum_{k=0}^{\frac{q-1}{2}} [\frac{1}{4q} + \frac{k}{q}] \right) - \sum_{j=1}^{\frac{q-1}{2}} \left([\frac{j}{q}] + [-\frac{1}{2q} + \frac{j}{q}] - [\frac{j}{2q}] - [-\frac{1}{4q} + \frac{j}{2q}] \right)$

Soit $\sin\ : \mathcal{A} \to (\mathbb{Q}^{ab})^*$ l'unique homomorphisme tel que

$$\sin[a] = \begin{cases} 2\sin\pi a \ \text{ si } \ 0 < a < 1, \ (a \in \mathbb{Q} \cap [0,1]) \\ 1 \ \text{ si } \ a = 0 \end{cases}$$

On a le résultat suivant, baptisé par son auteur ([**A**], main thm.) Kronecker-Weber plus epsilon.

Théorème 4.9. —
Une $\mathbb{F}_2$-base de $H^0\big(G_{\mathbb{Q}}^{ab}, (\mathbb{Q}^{ab})^*/(\mathbb{Q}^{ab})^{*2}\big)$ est formée des classes mod $(\mathbb{Q}^{ab})^{*2}$ de $\{\sqrt{\ell}\} \cup \{\sin(a_{rq})\}$, où ℓ parcourt l'ensemble des nombres premiers et (r, q) l'ensemble des couples de nombres premiers tels que $r < q$.

On peut douter qu'un tel résultat puisse s'obtenir par des considérations purement algébriques.

5. Ramification restreinte

Désormais F est un corps de nombres, $q = p^a$ et $p \neq 2$. On sait que $cd_p\, G_F \leq 2$, donc l'algèbre de cohomologie s'arrête au second cran : $H^*(G_F) = \bigoplus_{r=0}^{2} H^r(G_F)$, et pour sa description dans la situation kummerienne, on peut se contenter du § 3. Pour avoir des applications arithmétiques plus conséquentes, il convient d'introduire des conditions de ramification. Fixons quelques notations : S_p désignera l'ensemble des p-places de F, S_∞ l'ensemble des places archimédiennes de F, $S = S_p \cup S_\infty$ (on omet la référence à F) ; $G_S = G_{F,S}$ est le groupe de Galois sur F de l'extension algébrique maximale de F qui est S-ramifiée (i.e. non ramifiée en dehors de S) ; $\mathcal{O}_S = \mathcal{O}_{F,S}$ dénotera l'anneau des S-entiers de F, $\mathcal{O}_S^* = \mathcal{O}_{S,F}^*$ le groupe des S-unités.

5.1. $K_2(\mathcal{O}_S)$ **et** $K_2^M(\mathcal{O}_S)$**.** — L'arithmétique du corps F par rapport au nombre premier p se concentrant dans l'anneau $\mathcal{O}_S$, la K-théorie de Quillen semblerait ici mieux adaptée que la K-théorie de Milnor. En effet, $K_1(\mathcal{O}_S) \simeq \mathcal{O}_S^*$, et

$$K_2(\mathcal{O}_S)/q \xrightarrow[\simeq]{c_q} H^2_{\text{ét}}\left(\mathcal{O}_S, \mu_q^{\otimes 2}\right) \simeq H^2\left(G_S, \mu_q^{\otimes 2}\right)$$

d'après un théorème de Tate (un cas particulier de la conjecture de Quillen-Lichtenbaum, devenue maintenant une conséquence - non triviale - du théorème de Voevodsky-Rost). Cependant, dans l'optique du théorème 2.1 par exemple, il faut faire intervenir le cup-produit $H^1(G_S, \mu_q) \otimes H^1(G_S, \mu_q) \to H^2(G_S, \mu_q^{\otimes 2})$ et réintroduire les symboles de la K-théorie de Milnor. Rappelons que pour tout anneau commutatif R,

$$K_2^M(R) := (R^* \otimes R^*)/\langle a \otimes 1 - a \ ; \ a, 1-a \in R^* \rangle.$$

Le lien entre $K_2^M(\mathcal{O}_S)$ et $K_2(\mathcal{O}_S)$ réside dans l'identification (non triviale, via c_q) de $K_2(\mathcal{O}_S)$ avec le noyau modéré :

$$K_2(\mathcal{O}_S) \simeq \ \text{Ker}\left(K_2^M(F) = K_2(F) \xrightarrow{t} \bigoplus_{v \notin S} f_v^*\right),$$

où f_v désigne le corps résiduel de F en v et t est la somme des symboles modérés.

Lemme 5.1 **([MS], propos. 3-1)**. — *On a un triangle commutatif*

$$\begin{array}{ccc} K_2^M(\mathcal{O}_S)/q & \xrightarrow{\quad h_q \quad} & H^2(G_S, \mu_q^{\otimes 2}) \\ & {\scriptstyle k_q} \searrow \quad \nearrow {\scriptstyle c_q}_{\simeq} & \\ & K_2(\mathcal{O}_S)/q & \end{array}$$

Remarque 5.2. — L'homorphisme h_q est le S-analogue du symbole galoisien. Dans le contexte étale de la conjecture de Quillen-Lichtenbaum, l'isomorphisme c_q est induit par une classe de Chern (voir **[So]**), mais **[T]** procède autrement, en passant par le noyau modéré. Enfin, l'homomorphisme k_q sera construit à partir de l'identification de $K_2(\mathcal{O}_S)$ avec le noyau modéré.

Démonstration. — Définissons d'abord l'homomorphisme h_q. La suite exacte de Kummer (où la référence à F est sous-entendue)

$$1 \longrightarrow \mathcal{O}_S^*/q \longrightarrow H^1(G_S, \mu_q) \longrightarrow \mathcal{C}\ell_S[q] \longrightarrow 0,$$

où $\mathcal{C}\ell_S$ désigne le groupe des classes de $\mathcal{O}_S$, permet d'identifier $\mathcal{O}_S^*/q$ à un sous-groupe de $H^1(G_S, \mu_q)$.

Soit $(.,.)_S : (\mathcal{O}_S^*/q)^{\otimes 2} \longrightarrow H^2(G_S, \mu_q^{\otimes 2})$ l'homomorphisme induit par le cup-produit. Si $a \in \mathcal{O}_S^*$ et $1-a \in \mathcal{O}_S^*$, on sait ([**MS**], coroll. 2.5) que $(a, 1-a)_S = 0$. La propriété universelle de K_2^M donne alors un homomorphisme $h_q : K_2^M(\mathcal{O}_S/q) \longrightarrow H^2(G_S, \mu_q^{\otimes 2})$ qui factorise le cup-produit $(.,.)_S$.

Définissons ensuite l'homomorphisme k_q. Puisque les éléments de $\mathcal{O}_S^*$ sont des unités en toute place $v \notin S$, il résulte de la définition des symboles locaux modérés qu'ils se trivialisent sur toute paire de tels éléments. L'identification de $K_2(\mathcal{O}_S)$ avec le noyau modéré et la propriété universelle montrent alors l'existence de k_q et la commutativité du triangle. □

5.2. Conjecture et hypothèse de McCallum-Sharifi. — En vue d'une extension des calculs du § 3 au cas S-ramifié, on se pose la question de la surjectivité du cup-produit $(.\,,.\,)_S\ :\ (\mathcal{O}_S^*/q)^{\otimes 2} \to H^2(G_S, \mu_q^{\otimes 2})$. Les équivalences suivantes sont claires :

Lemme 5.3. — *Les surjectivités des applications* (i) *à* (iv) *sont équivalentes :*
(i) *Le cup-produit* $(.\,,.\,)_S : (\mathcal{O}_S^*/q)^{\otimes 2} \longrightarrow H^2(G_S, \mu_q^{\otimes 2})$.
(ii) *L'homomorphisme* $h_q : K_2^M(\mathcal{O}_S)/q \longrightarrow H^2(G_S, \mu_q^{\otimes 2})$.
(iii) *L'homomorphisme* $k_q : K_2^M(\mathcal{O}_S)/q \longrightarrow K_2(\mathcal{O}_S)/q$.
(iv) *L'homomorphisme* $k : K_2^M(\mathcal{O}_S) \otimes \mathbb{Z}_p \longrightarrow K_2(\mathcal{O}_S) \otimes \mathbb{Z}_p$.

Malgré notre désir d'appliquer ces surjectivités comme dans le § 3, nous ne voyons a priori aucune raison qu'elles soient vérifiées par n'importe quel corps de nombres. C'est pourquoi nous les appellerons simplement *hypothèse de McCallum-Sharifi*, en abrégé (HMS), pour le corps F. Mais pour les corps cyclotomiques, l'hypothèse devient une conjecture, en abrégé (CMS) : pour $F = \mathbb{Q}(\mu_p)$, c'est la conjecture 5-3 de **[MS]** ; pour $F = \mathbb{Q}(\mu_{p^r N})$, la conjecture 5-4 de **[Sh2]**. Résumons rapidement les résultats en direction de la conjecture (CMS) :
- dans le cas de $\mathbb{Q}(\mu_p)$, (CMS) a été démontrée pour $p = 37$ par des méthodes ad hoc dans **[MS]** ; pour tout $p < 10^3$, dans **[Sh1]** comme conséquence d'une relation particulière entre la structure de certains modules d'Iwasawa sur des extensions kummeriennes de $\mathbb{Q}(\mu_{p^r N})$ et la structure d'algèbres de Hecke ordinaires de formes modulaires localisées en l'idéal d'Eisenstein.
- dans le cas $\mathbb{Q}(\mu_{p^r N})$, **[Sh2]** montre que (CMS) provient en grande partie d'une conjecture reliant les valeurs prises par le cup-produit $(.\,,.\,)_S$ sur des paires de p-unités cyclotomiques, aux valeurs de fonctions L_p associées à des formes propres cuspidales qui vérifient des congruences mod p avec des séries d'Eisenstein.
- enfin, Fukaya et Kato ont exposé à la conférence Iwasawa 2012 une démonstration du résultat suivant :

Théorème 5.4 **([FK])**. — *La conjecture (CMS) est vraie pour tout* $\mathbb{Q}(\mu_{p^r})$ *sous l'une des deux hypothèses*

(i) *La fonction zêta p-adique n'a pas de zéro multiple.*

(ii) *Pour tout premier* $\mathcal{P}$ *de hauteur 1 de l'algèbre* $\mathcal{H} = \varprojlim \mathcal{H}(p^n)$ *(où* $\mathcal{H}(p^n)$ *est la partie ordinaire de l'algèbre de Hecke duale pour* $S_2(X_1(p^n))$*) qui contient l'idéal d'Eisenstein, l'algèbre localisée* $\mathcal{H}_\mathcal{P}$ *est de Gorenstein.*

Remarque 5.5. — - Ces hypothèses sont vérifiées sur tous les exemples connus.
- Fukaya et Kato démontrent en fait une forme faible de la conjecture de **[Sh2]**, moyennant les hypothèses précédentes.

5.3. Applications. — Soit F un corps de nombres contenant μ_q.
On se contentera de donner une liste des résultats qui se transposent directement de G_F à G_S, avec hypothèse supplémentaire ou pas :
- sous l'hypothèse (HMS) (i.e. la surjectivité du cup-produit $(.\,,.\,)_S$), les théorèmes 2.1, 2.4 et 3.4 restent valables en remplaçant G_F par G_S.
- sans l'hypothèse (HMS) (on n'a pas besoin de la surjectivité de $(.\,,.\,)_S$), la proposition 3.2 s'applique au pro-p-quotient maximal $G_S(p)$, dont on sait qu'il est de type fini. Le

théorème 4.5 reste valable car les techniques cohomologiques de plongement, et notamment le critère de Hoechsmann, continuent à s'appliquer en remplaçant G_F par G_S.

Références

[A] G.W. Anderson, Kronecker-Weber plus epsilon, *Duke Math. J.* **114**, 3 (2002), 439-475.

[CEM] S.K. Chebolu, I. Efrat, J. Mináč, Quotients of absolute Galois groups which determine the entire Galois cohomology, *Math. Annalen* **352** (2012), 205-221.

[EM] I. Efrat, J. Mináč, On the descending central sequence of absolute Galois groups, *Amer. J. of Math.* **133** (2011), 1503-1532.

[FK] T. Fukaya, K. Kato, On conjectures of Sharifi, Conf. Iwasawa 2012, Heidelberg, July 30-August 3, 2012.

[GS] P. Gille, T. Szamuely, Central simple algebras and Galois cohomology, Cambridge Stud. Adv. Math., vol. 101, Cambridge, 2006.

[H] K. Hoechsmann, Zum Einbettungsproblem, *J. reine ang. Math.* **229** (1968), 81-106.

[K] H. Koch, Galois theory of p-extensions, Springer Monogr. Math., Berlin, 2002.

[M] J. Milnor, Introduction to algebraic K-theory, Ann. of Math. Studies, Princeton, 1971.

[MN] R. Massy, T. Nguyen Quang Do, Plongement d'une extension de degré p^2 dans une surextension non abélienne de degré p^3 : étude locale-globale, *J. reine ang. Math.* **291** (1977), 149-161.

[MS] W. McCallum, R. Sharifi, A cup product in the Galois cohomology of number fields, *Duke Math. J.* **120** (2003), 269-310.

[MSp] J. Mináč, M. Spira, Witt rings and Galois groups, *Ann. of Math.* (2) **144** (1996), no 1, 35-60.

[MSu] A.S. Merkurjev, A.A. Suslin, K-cohomology of Severi-Brauer varieties and the norm residue homomorphism, *Math. USSR Izv.* **21** (1983), 307-340.

[Sh1] R. Sharifi, Iwasawa theory and the Eisenstein ideal, *Duke Math. J.* **137** (2007), 63-101.

[Sh2] R. Sharifi, A reciprocity map and the two-variable p-adic L-function, *Ann. of Math.* **173** (2011), 251-300.

[So] C. Soulé, K-théorie des anneaux d'entiers de corps de nombres et cohomologie étale, *Invent. Math.* **55** (1979), 251-295.

[T] J. Tate, Relations between K_2 and Galois cohomology, *Invent. Math.* **36** (1976), 257-274.

[Vi] F.R. Villegas, Relations between quadratic forms and certain Galois extensions, Ohio State Univ., 1988. *http ://www.math.utexas.edu/users/villegas/osu.pdf*

[Vo] V. Voevodsky, On motivic cohomology with $\mathbb{Z}/\ell$-coefficients, *Ann. of Math.* **174** (2011), 401-438.

[W] C.A. Weibel, The proof of the Bloch-Kato conjecture, *ICTP Lecture Notes series* **23** (2008), 1-28.

[Y] K. Yamazaki, On projective representations and ring extensions of finite groups, *J. Fac. Sci. Tokyo* **10** (1964), 147-195.

26 septembre 2012

Thong Nguyen Quang Do, Laboratoire de Mathématiques de Besançon, UFR ST, 16 route de Gray, Besançon, F-25030 • *E-mail :* thong.nguyen-quang-do@univ-fcomte.fr