Cohomologie galoisienne et théorie des nombres, M2, Orsay

David Harari

2011/2012 (semestre 2)

Table des matières

Les démonstrations en petits caractères sont celles qui n'ont pas été faites en détails en cours par manque de temps.

Je remercie M. Chen, Z. Gao, C. Gomez, Y. Liang, G. Lucchini-Servetto, A. Pirutka, J. Riou, A. Schmidt, et J. Xun pour leurs commentaires qui m'ont permis de corriger des erreurs et d'améliorer la rédaction.

1. Cohomologie des groupes : généralités

Dans toute cette section, G désigne un groupe (dont la loi est notée multiplicativement et l'élément neutre 1). Rappelons que *l'algèbre du groupe* G est l'ensemble $\mathbf{Z}[G]$ des sommes formelles presque nulles

$$\sum_{g\in G} n_g g, \quad n_g \in \mathbf{Z}$$

muni de l'addition évidente et du produit de convolution

$$(\sum_{g\in G} n_g g)(\sum_{g\in G} m_g g) := \sum_{(g,g')\in G\times G} n_g m_{g'} gg'$$

En particulier $\mathbf{Z}[G]$ est un anneau, non commutatif si G n'est pas abélien.

1.1. Notion de G-module

Définition 1.1 Un *G-module* est la donnée d'un groupe abélien $(A,+)$ et d'une action $(g,x)\mapsto g.x$ de G sur A telle que pour tout g de G l'application $\varphi_g : x\mapsto g.x$ de A dans A soit un morphisme de groupes abéliens.

On a donc les règles de calcul : $g.(g'.x) = (gg').x$, $1.x = x$, et $g.(x+y) = g.x + g.y$, valables pour tous g, g' de G et pour tous x, x' de A.

Notons aussi que φ_g est un automorphisme de A, de réciproque $\varphi_{g^{-1}}$. Si A est un groupe abélien, se donner une structure de G-module sur A revient à se donner un morphisme de groupes de G dans $(\mathtt{Aut}\,(A), \circ)$, où $\mathtt{Aut}\,(A)$ est l'ensemble des automorphismes du groupe abélien A. De façon équivalente, un G-module est la donnée d'un module (à gauche) sur l'anneau $R := \mathbf{Z}[G]$: en effet si A est un module sur l'anneau R, on définit une structure de G-module sur A via $g.x = gx$ pour tout $(g,x)\in G\times A$; réciproquement si A est un G-module, on le munit d'une structure de module sur R en posant $(\sum_{g\in G} n_g g)x = \sum_{g\in G} n_g(g.x)$.

Définition 1.2 Un *morphisme de G-modules* (ou *G-morphisme*) $f : A \to A'$ est un morphisme de groupes abéliens qui commute aux opérations de G, i.e. tel que $f(g.x) = g.f(x)$ pour tout x de A et tout g de G. Cela revient à dire que f est un morphisme de R-modules.

On définit de manière évidente les notions d'isomorphisme de G-modules, de sous G-module, de suite exacte de G-modules etc. Si A et A' sont des G-modules, on note alors $\mathrm{Hom}_G(A, A')$ l'ensemble des G-morphismes de A dans A' ; c'est un groupe abélien pour l'addition, qui est un sous-groupe du groupe $\mathrm{Hom}_{\mathbf{Z}}(A, A')$ des morphismes de groupes abéliens de A dans A' (non nécessairement compatibles avec l'action de G).

Exemples. a) Pour tout groupe abélien A, l'action triviale de G sur A (définie par $g.x = x$ pour tout $g \in G$ et tout $x \in A$) fait de A un G-module.

b) Le groupe abélien $\mathbf{Z}[G]$ est muni d'une structure canonique de G-module via l'action à gauche de G sur lui-même par translation.

c) Posons $G = \{\pm 1\}$ et $M = \mathbf{Z}$. Alors l'opération de G sur M définie par $g.x = gx$ fait de M un G-module.

d) Soit L une extension finie galoisienne de groupe G d'un corps K. Alors L et L^* sont tous deux des G-modules pour l'action de $G = \mathrm{Gal}\,(L/K)$.

L'exemple suivant va être particulièrement important dans la suite de ce cours :

Définition 1.3 Soit G un groupe et soit H un sous-groupe de G. Soit A un H-module. On définit un groupe abélien $I_G^H(A)$ comme l'ensemble des applications $f : G \to A$ vérifiant $f(hg) = hf(g)$ pour tous $g \in G$, $h \in H$. Ce groupe abélien est alors muni d'une structure de G-module via la formule $(g.f)(g') = f(g'g)$ pour tous g, g' de G. On dit que $I_G^H(A)$ est l'*induit* de H à G du H-module A. En particulier si H est le sous-groupe trivial et A est un groupe abélien, on note simplement $I_G(A)$ l'induit correspondant, qu'on appelle *G-module induit* du groupe abélien A.

Définition 1.4 On dit qu'un G-module M est *induit*[1] s'il existe un groupe abélien A tel que M soit isomorphe à $I_G(A)$.

1. Dans la terminologie de [13], ces modules sont appelés co-induits (nous suivons ici la terminologie de [14]). On peut aussi dire que ce sont les modules de la forme $\mathrm{Hom}_{\mathbf{Z}}(\mathbf{Z}[G], A)$, l'action de G étant sur le premier facteur. Si G est fini, ce sont aussi les modules que nous appellerons co-induits, i.e. de la forme $\mathbf{Z}[G] \otimes A$ (lesquels sont appelés induits dans [13]).

Remarque : Si A est déjà muni d'une structure de G-module, alors $I_G(A)$ est isomorphe au G-module $\mathcal{F}(G, A)$ défini comme l'ensemble des applications de G dans A avec l'action $(g.f)(x) := g.f(g^{-1}.x)$; un isomorphisme est en effet donné par $f \mapsto (g \mapsto g.f(g^{-1}))$ (je remercie Alexander Schmidt pour cette remarque).

1.2. La catégorie des G-modules

Soit $f : A \to A'$ un morphisme de G-modules. Il résulte immédiatement des définitions que le noyau, l'image et le conoyau de f (vu comme morphisme de groupes abéliens) sont encore des G-modules pour l'action évidente de G. Par suite, les G-modules (le groupe G étant fixé) forment une *catégorie abélienne* (cf. par exemple [8], chapitre VIII pour les généralités sur les catégories abéliennes). On la notera $\mathcal{M}od_G$ (elle est bien sûr équivalente à la catégorie $\mathcal{M}od_R$ des R-modules à gauche, où $R = \mathbf{Z}[G]$).

Pour tous G-modules A et A', le foncteur covariant $\mathrm{Hom}_G(A, .)$ et le foncteur contravariant $\mathrm{Hom}_G(., A')$ sont exacts à gauche (vérification immédiate).

Définition 1.5 Un G-module A est dit *projectif* si $\mathrm{Hom}_G(A, .)$ est exact. Un G-module A' est dit *injectif* si $\mathrm{Hom}_G(., A')$ est exact.

Exemples a) Tout G-module qui est libre en tant que module sur l'anneau $\mathbf{Z}[G]$ est projectif (plus généralement un G-module est projectif si et seulement s'il est facteur direct d'un $\mathbf{Z}[G]$-module libre).

b) Prenons pour G le groupe trivial (de sorte que la notion de G-module coïncide avec celle de groupe abélien). Alors tout groupe abélien A *divisible* (i.e. tel que pour tout $n > 0$, le morphisme $x \mapsto nx$ soit surjectif de A dans A) est injectif (c'est une conséquence facile du lemme de Zorn, cf. [16], Cor. 2.3.2.).

c) Une somme directe (éventuellement infinie) de G-modules projectifs est un G-module projectif. Un produit direct (éventuellement infini) de G-modules injectifs est injectif. En particulier une somme directe finie de G-modules injectifs est également un G-module injectif (vu qu'elle s'identifie au produit direct des G-modules en question).

Proposition 1.6 *Soit A un G-module. Soit I un sous G-module injectif de A. Alors I est un facteur direct de A (autrement dit il existe un sous G-module B de A tel que $A = I \oplus B$).*

Démonstration : Par définition d'un G-module injectif, l'identité $I \to I$ se prolonge en un morphisme de G-modules $r : A \to I$. Il suffit alors de poser $B = \ker r$.

□

Proposition 1.7 *Pour tout G-module A, il existe un G-module induit I muni d'un G-morphisme injectif $A \to I$.*

Démonstration : Soit $I = I_G(A) = \mathrm{Hom}_{\mathbf{Z}}(\mathbf{Z}[G], A)$ l'induit de A. On plonge alors A dans $I_G(A)$ en associant à tout $a \in A$ l'application $g \mapsto g.a$ de G dans A. On vérifie immédiatement avec la définition de $I_G(A)$ que ceci définit un morphisme de G-modules, qui est injectif (si $g.a = 0$ pour tout g de G, on obtient $a = 0$ en faisant $g = 1$).

□

Définition 1.8 On dit qu'un G-module est *relativement injectif* (ou faiblement injectif) s'il est facteur direct d'un G-module induit $I_G(A)$ (où A est un groupe abélien).

Notons que d'après les propositions 1.7 et 1.6, tout G-module injectif est relativement injectif.

La catégorie $\mathcal{M}od_G$ *possède suffisamment d'injectifs* (i.e. tout G-module est isomorphe à un sous-module d'un G-module injectif). C'est en fait une propriété générale des catégories de modules :

Proposition 1.9 *Pour tout anneau R, la catégorie $\mathcal{M}od_R$ des modules (à gauche) sur R possède suffisamment d'injectifs.*

Démonstration (esquisse): (voir le paragraphe 2.3. de [16]). On montre d'abord que si I est injectif dans la catégorie des groupes abéliens, alors le R-module $\mathrm{Hom}_{\mathbf{Z}}(R, I)$ est injectif dans $\mathcal{M}od_R$. On prend alors $I = \mathbf{Q}/\mathbf{Z}$ et pour tout groupe abélien A, on note $A' := \mathrm{Hom}_{\mathbf{Z}}(A, \mathbf{Q}/\mathbf{Z})$. Si A est un R-module, le R-module A' peut s'écrire comme quotient d'un R-module libre (somme directe de copies de R). En appliquant encore $'$, on obtient que $(A')'$ se plonge dans un R-module M qui est le produit de R-modules du type R'. Comme on l'a vu plus haut, R' est injectif dans $\mathcal{M}od_R$ donc M l'est aussi. On conclut en remarquant que la flèche canonique $A \mapsto (A')'$ est injective.

□

Il en résulte que pour tout foncteur additif, covariant et exact à gauche $F : \mathcal{M}od_G \to \mathcal{B}$ (où $\mathcal{B}$ est une catégorie abélienne, par exemple la catégorie

$\mathcal{A}b$ des groupes abéliens), on peut définir les *foncteurs dérivés* (à droite) R^iF pour $i \geq 0$. Rappelons qu'en particulier $R^0F = F$ et si

$$0 \to A' \to A \to A'' \to 0$$

est une suite exacte dans $\mathcal{M}od_G$, on a des morphismes naturels (i.e. fonctoriels vis à vis des morphismes de suites exactes) $\delta^i : R^iF(A'') \to R^{i+1}F(A')$ qui induisent une longue suite exacte

$$... \to R^iF(A') \to R^iF(A) \to R^iF(A'') \xrightarrow{\delta^i} R^{i+1}F(A') \to ...$$

On pourra se reporter au chapitre 2 de [16] pour les propriétés générales des foncteurs dérivés. Rappelons seulement comment on obtient les $R^iF(A)$ à partir d'une résolution injective[2] de A (i.e. une suite exacte où tous les I_j sont des G-modules injectifs)

$$0 \to A \to I_0 \to I_1 \to I_2 \to ...$$

Les $R^iF(A)$ sont les groupes de cohomologie du complexe

$$0 \to F(I_0) \to F(I_1) \to F(I_2) \to ...$$

(par exemple $R^1F(A)$ s'obtient comme le quotient de $\ker[F(I_1) \to F(I_2)]$ par $\mathrm{Im}\,[F(I_0) \to F(I_1)]$). Plus généralement, on peut calculer les $R^iF(A)$ avec n'importe quelle résolution (I_j) telle que les tous les I_j soient *acycliques*, i.e. vérifient $R^iF(I_j) = 0$ pour tout $i > 0$, cf. [16], paragraphe 2.4.

Notons aussi que tout G-module est quotient d'un G-module projectif (par exemple d'un module libre sur l'anneau $R := \mathbf{Z}[G]$), autrement dit la catégorie des G-modules possède *suffisamment de projectifs*. Nous allons voir que les groupes de cohomologie $H^i(G, A)$ pour un G-module A, bien que définis comme foncteurs dérivés droits (donc se calculant en théorie via des résolutions injectives de A), se calculent en fait plus facilement via une résolution projective du G-module $\mathbf{Z}$ (équipé de l'action triviale de G).

1.3. Les groupes de cohomologie $H^i(G, A)$

Pour tout G-module A, notons A^G le sous-groupe de A constitué des éléments x qui vérifient $g.x = x$ pour tout g de G. Le foncteur $F : A \mapsto A^G$ de $\mathcal{M}od_G$ dans $\mathcal{A}b$ est covariant et exact à gauche. On peut donc définir ses foncteurs dérivés à droite R^iF et on pose

$$H^i(G, A) := R^iF(A)$$

2. L'existence d'une telle résolution découle de ce que la catégorie des G-modules possède suffisamment d'injectifs.

pour tout G-module A. Ces groupes sont "fonctoriels en A" de façon covariante, c'est-à-dire qu'un morphisme de G-modules $\varphi : A \to B$ induit pour tout $i \geq 0$ un homomorphisme de groupes abéliens $\varphi_* : H^i(G, A) \to H^i(G, B)$, avec de plus la formule $(\varphi + \psi)_* = \varphi_* + \psi_*$; en particulier si φ est la multiplication par un entier $m > 0$ dans un G-module A, alors φ_* est la multiplication par m dans $H^i(G, A)$. On en déduit que si A est de m-torsion, alors $H^i(G, A)$ est de m-torsion. Si G est le groupe trivial, on a bien entendu $H^i(G, A) = 0$ pour tout $i > 0$ vu que le foncteur $A \mapsto A^G$ est évidemment exact dans ce cas.

Les $H^i(G, A)$ peuvent se calculer à partir d'une résolution injective (ou même d'une résolution acyclique) comme expliqué au paragraphe précédent. Les propriétés générales des foncteurs dérivés (qui découlent de ce calcul) donnent alors :

Theorème 1.10 *a) On a $H^0(G, A) = A^G$.*

b) On a $H^i(G, A) = 0$ pour tout G-module injectif A et tout $i > 0$.

c) Pour toute suite exacte courte

$$0 \to A \to B \to C \to 0$$

de G-modules, on a une suite exacte longue

$$0 \to A^G \to B^G \to C^G \xrightarrow{\delta^0} H^1(G, A) \to H^1(G, B) \to H^1(G, C) \xrightarrow{\delta^1} H^2(G, A) \to ...$$

et les δ^i dépendent fonctoriellement de la suite exacte considérée.

On obtient aussi immédiatement :

Proposition 1.11 *Pour tous G-modules A et B, on a $H^i(G, A \oplus B) = H^i(G, A) \oplus H^i(G, B)$.*

Remarque : La proposition 1.11 s'étend sans problème à la somme directe d'une famille finie de G-modules, ou encore au produit direct d'une famille quelconque de G-modules (utiliser le fait qu'un produit direct de G-modules injectifs est injectif). Elle n'est en revance plus valable sans hypothèse supplémentaire sur G si la famille est infinie (voir l'exercice 4 de ce chapitre), le problème étant qu'une somme directe infinie de G-modules injectifs n'est pas en général un G-modules injectif, ni même relativement injectif. On verra un peu plus loin (proposition 1.15) que la situation est meilleure quand G est fini.

Comme il est plus facile de construire des G-modules projectifs (par exemple libres) qu'injectifs, on a souvent intérêt à utiliser un autre procédé pour calculer les $H^i(G,A)$. On observe que le foncteur $A \to A^G$ de $\mathcal{M}od_G$ dans Ab s'identifie au foncteur $A \to \mathrm{Hom}_G(\mathbf{Z}, A)$ (où l'action de G sur $\mathbf{Z}$ est triviale). Il en résulte que $H^i(G,A) = \mathrm{Ext}^i_G(\mathbf{Z}, A)$, les $\mathrm{Ext}^i_G(\mathbf{Z}, .)$ étant par définition les foncteurs dérivés du foncteur $\mathrm{Hom}_G(\mathbf{Z}, .)$. Une propriété générale des Ext dans les catégories de modules ([16], théorème 2.7.6.) donne que les $\mathrm{Ext}^i_G(\mathbf{Z}, A)$ s'obtiennent également comme les foncteurs dérivés (appliqués à $\mathbf{Z}$) du foncteur contravariant $\mathrm{Hom}_G(., A)$. On peut donc les calculer en choisissant une résolution projective de $\mathbf{Z}$ (par exemple par des G-modules libres) :

$$... \to P_i \to P_{i-1} \to ... \to P_1 \to P_0 \to \mathbf{Z} \to 0$$

et les $H^i(G,A)$ apparaissent alors comme les groupes de cohomologie du complexe

$$0 \to \mathrm{Hom}_G(P_0, A) \to \mathrm{Hom}_G(P_1, A) \to \mathrm{Hom}_G(P_2, A)...$$

Par exemple $H^1(G,A)$ est le quotient de $\ker[\mathrm{Hom}_G(P_1, A) \to \mathrm{Hom}_G(P_2, A)]$ par $\mathrm{Im}\,[\mathrm{Hom}_G(P_0, A) \to \mathrm{Hom}_G(P_1, A)]$.

On aimerait maintenant généraliser le theorème 1.10, b) en utilisant cette nouvelle méthode de calcul de la cohomologie. On commence pour cela par une proposition générale.

Proposition 1.12 *Soient G un groupe et H un sous-groupe de G. Soit A un H-module. Alors pour tout G-module B, le groupe* $\mathrm{Hom}_H(B, A)$ *s'identifie canoniquement à* $\mathrm{Hom}_G(B, I^H_G(A))$.

Démonstration : Soit $\psi \in \mathrm{Hom}_H(B, A)$. Pour tout b de B, on définit un élément $\varphi(b)$ de $I^H_G(A)$ par la formule $(\varphi(b))(g) = \psi(gb)$ pour tout g de G, car on vérifie immédiatement que pour tout h de H on a

$$(\varphi(b))(hg) = \psi(hgb) = h.\psi(gb) = h.(\varphi(b)(g))$$

Pour tous g, g' de G et tout b de B, on a également

$$(\varphi(g.b))(g') = \psi(g'gb) = (\varphi(b))(g'g) = (g.\varphi(b))(g')$$

ce qui montre que φ est un G-morphisme de B dans $I^H_G(A)$. Posons $\varphi = u(\psi)$, alors $u : \mathrm{Hom}_H(B, A) \to \mathrm{Hom}_G(B, I^H_G(A))$ est un morphisme de groupes abéliens. Son noyau est nul car si $\varphi(b) = 0$ pour tout b de B, alors en particulier $(\varphi(b))(1) = \psi(b)$ est nul pour tout b de B. Enfin, si φ est un

G-morphisme de B dans $I_G^H(A)$, on a $(\varphi(gb))(g') = \varphi(b)(g'g)$ pour tous g, g' de G et tout b de B. En faisant $g' = 1$, on obtient $(\varphi(b))(g) = (\varphi(gb))(1)$. Soit ψ l'élément de $\mathrm{Hom}_{\mathbf{Z}}(B, A)$ défini par $\psi(b) = (\varphi(b))(1)$. Alors on a $\psi \in \mathrm{Hom}_H(B, A)$ via le fait que $\varphi(b) \in I_G^H(A)$, et $\varphi = u(\psi)$ d'après le calcul ci-dessus, d'où la surjectivité de u. Finalement u est un isomorphisme.

□

On peut alors obtenir :

Proposition 1.13 *Soit A un G-module relativement injectif. Alors pour tout $i > 0$ on a $H^i(G, A) = 0$.*

Autrement dit : les G-modules relativement injectifs sont acycliques.

Démonstration : Comme A est facteur direct d'un G-module induit, on se ramène immédiatement via la proposition 1.11 d) au cas où A est lui-même induit, i.e. de la forme $A = I_G(X)$ pour un certain groupe abélien X. Considérons alors une résolution de $\mathbf{Z}$ par des G-modules projectifs

$$... \to P_i \to P_{i-1} \to ... \to P_1 \to P_0 \to \mathbf{Z} \to 0$$

et appliquons le foncteur $\mathrm{Hom}_G(., A)$ à ce complexe. D'après la proposition 1.12, on obtient les $H^i(G, A)$ comme groupes de cohomologie du complexe

$$0 \to \mathrm{Hom}_{\mathbf{Z}}(P_0, X) \to \mathrm{Hom}_{\mathbf{Z}}(P_1, X) \to ...$$

c'est-à dire (via la résolution projective de $\mathbf{Z}$ par les P_i) comme les $\mathrm{Ext}^i_{\mathbf{Z}}(\mathbf{Z}, X)$ (la notation $\mathrm{Ext}^i_{\mathbf{Z}}$ signifiant qu'on prend les Ext dans la catégorie des groupes abéliens). Comme ces $\mathrm{Ext}^i_{\mathbf{Z}}$ peuvent aussi se calculer (toujours d'après [16], théorème 2.7.6.) comme les foncteurs dérivés du foncteur de $\mathcal{A}b$ dans $\mathcal{A}b$ défini par $M \to \mathrm{Hom}_{\mathbf{Z}}(\mathbf{Z}, M) = M$, qui est évidemment exact, le résultat en découle.

□

Corollaire 1.14 *Soit*

$$0 \to A \to I \to B \to 0$$

une suite exacte de G-modules avec I relativement injectif (par exemple induit). Alors pour tout $i > 0$, on a $H^i(G, B) = H^{i+1}(G, A)$ et la flèche "cobord" $H^0(G, B) \to H^1(G, A)$ est surjective.

Démonstration : Cela résulte de la suite exacte longue de cohomologie et de la proposition précédente.

□

Ce corollaire est utile car il permet souvent de démontrer des propriétés des $H^i(G, A)$ par "décalage" en raisonnant par récurrence sur i.

Proposition 1.15 *Supposons le groupe G fini. Soit $(A_j)_{j\in J}$ un système inductif*[3] *de G-modules et $A := \varinjlim_j A_j$ le G-module limite inductive des A_j. Alors pour tout $i \geq 0$ on a*

$$H^i(G, A) = \varinjlim_j H^i(G, A_j)$$

En particulier on voit que *quand le groupe G est fini*, "la cohomologie de G commute avec les sommes directes".

Démonstration : Pour $i = 0$, le résultat est immédiat. Comme $\varinjlim$ est un foncteur exact dans la catégorie des groupes abéliens et qu'on peut calculer la cohomologie avec n'importe quelle résolution acyclique (par exemple composée de G-modules relativement injectifs, cf. proposition 1.13), il suffit de savoir qu'une limite inductive de G-modules relativement injectifs est un G-module relativement injectif, et même (par définition d'un module relativement injectif) qu'une limite inductive de G-modules induits est un G-module induit. Mais ceci résulte de ce que pour G fini, les notions de G-modules induits et co-induits coïncident et de ce que $\varinjlim$ commute avec $\otimes$.

□

Remarques : a) Pour démontrer la proposition 1.15, on peut aussi raisonner par récurrence sur i en utilisant le corollaire 1.14, une fois acquis qu'une limite inductive de G-modules injectifs est acyclique quand G est fini (attention : il faut d'abord traiter le cas $i = 1$ via le lemme des cinq vu que le corollaire 1.14 ne s'applique directement que pour $i \geq 1$).

b) L'analogue de la proposition 1.15 avec "limite projective" au lieu de "limite inductive" est en général faux (voir l'exercice 3 de ce chapitre).

1.4. Calcul de la cohomologie avec les cochaînes

Pour les petits degrés ($i = 1$, $i = 2$), on a intérêt à avoir une description explicite des groupes $H^i(G, A)$. Pour cela on va construire une résolution

3. Par convention, les systèmes inductifs que l'on considérera dans ce cours seront toujours associés à des ensembles ordonnés filtrants. Sans cette hypothèse une limite inductive de groupes abéliens n'est bien définie que comme ensemble et pas comme groupe abélien.

explicite du G-module $\mathbf{Z}$ (équipé de l'action triviale de G) par des $\mathbf{Z}[G]$-modules libres.

Pour tout $i \geq 0$, soit E_i l'ensemble des $(i+1)$-uplets $(g_0, ..., g_i)$ d'éléments de G. Soit L_i le $\mathbf{Z}$-module libre de base E_i. L'opération de G sur E_i par translation

$$s.(g_0, ..., g_i) := (sg_0, ..., sg_i) \quad s \in G, \quad (g_0, ..., g_i) \in L_i$$

définit une structure de G-module sur L_i. Comme G opère librement sur E_i, le $\mathbf{Z}[G]$-module L_i est libre (on en obtient une base en choisissant un élément dans chaque orbite pour l'action de G sur E_i). Soit alors $d_i : L_i \to L_{i-1}$ le morphisme de G-modules défini par la formule (où le symbole $\hat{g}_j$ signifie comme d'habitude que l'indice j est omis) :

$$d_i(g_0, ..., g_i) = \sum_{j=0}^{i} (-1)^j (g_0, ..., \hat{g}_j, ..., g_i)$$

si $i > 0$ et $d_0 : L_0 \to \mathbf{Z}$ le morphisme de G-modules qui envoie tout (g_0) sur 1.

Lemme 1.16 *La suite*

$$... \to L_2 \stackrel{d_2}{\to} L_1 \stackrel{d_1}{\to} L_0 \stackrel{d_0}{\to} \mathbf{Z} \to 0$$

est exacte (ainsi c'est une résolution de $\mathbf{Z}$ *par des* $\mathbf{Z}[G]$*-modules libres, donc projectifs).*

Démonstration : Montrons d'abord que $d_i \circ d_{i+1} = 0$ pour tout $i \geq 0$. C'est immédiat pour $i = 0$. Supposons $i \geq 1$. Alors pour tout $(g_0, ..., g_{i+1}) \in L_{i+1}$, on a :

$$(d_i \circ d_{i+1})((g_0, ..., g_{i+1})) = \sum_{k=0}^{i+1} (-1)^k d_i(g_0, ..., \hat{g}_k, ..., g_{i+1}) =$$

$$\sum_{k=0}^{i+1} (-1)^k \, [\sum_{j=0}^{k-1} (-1)^j (g_0, ..., \hat{g}_j, ...\hat{g}_k, ..., g_{i+1}) + \sum_{j=k+1}^{i+1} (-1)^{j-1} (g_0, ..., \hat{g}_k, ...\hat{g}_j, ..., g_{i+1}) \,]$$

Pour toute paire (r, s) avec $0 \leq r < s \leq i+1$, le terme $(g_0, ..., \hat{g}_r, \hat{g}_s, ...g_{i+1})$ apparaît deux fois dans la somme : une fois avec le signe $(-1)^{r+s}$ pour $j = r, k = s$, et une fois avec le signe $(-1)^{r+s-1}$ pour $k = r, j = s$; la somme est donc bien nulle.

Définissons alors des morphismes de groupes abéliens (ce ne sont pas des G-morphismes en général) $u_i : L_i \to L_{i+1}$ par $u_0(1) = (1)$, et $u_i(g_0, ..., g_i) =$

$(1, g_0, ..., g_i)$ si $i \geq 1$. On a alors $u_{i-1} \circ d_i + d_{i+1} \circ u_i = \mathrm{Id}_{L_i}$ pour tout $i \geq 0$. En effet :

$$(u_{i-1} \circ d_i + d_{i+1} \circ u_i)(g_0, ..., g_i) =$$

$$\sum_{j=0}^{i} (-1)^j (1, g_0, ..., \hat{g}_j, ..., g_i) + (g_0, ..., g_i) + \sum_{j=1}^{i+1} (-1)^j (1, g_0, ..., \hat{g}_{j-1}, ..., g_i) =$$

qui est bien égal à $(g_0, ..., g_i)$ (les termes se simplifient deux à deux). Soit alors x dans $\ker d_i$, on obtient $x = d_{i+1}(u_i(x))$ donc $x \in \mathrm{Im}\, d_{i+1}$. Comme $d_i \circ d_{i+1} = 0$, on a aussi $\mathrm{Im}\, d_{i+1} \subset \ker d_i$ et donc finalement $\mathrm{Im}\, d_{i+1} = \ker d_i$, d'où l'exactitude voulue. □

Soit alors A un G-module. Un élément de $K^i := \mathrm{Hom}_G(L_i, A)$ s'identifie à une fonction $f : G^{i+1} \to A$ vérifiant

$$f(s.g_0, ..., s.g_i) = s.f(g_0, ..., g_i)$$

("cochaîne homogène"), les cobords $K^i \to K^{i+1}$ s'obtenant par une formule analogue à la précédente. Une telle fonction est uniquement déterminée par sa valeur sur les éléments de G^{i+1} de la forme $(1, g_1, g_1g_2, ..., g_1...g_i)$. Finalement, on peut voir les éléments de K^i comme des *cochaînes non homogènes*, à savoir :

Theorème 1.17 *Les groupes $H^i(G, A)$ pour $i \geq 1$ s'obtiennent comme les groupes de cohomologie du complexe*

$$K^0 \to K^1 \to K^2 \to ....$$

où $K^0 = A$ (vu comme l'ensemble des fonctions de $G^0 := \{1\}$ dans A) et pour $i \geq 1$, K^i est le groupe abélien constitué des fonctions $f : G^i \to A$, le cobord $d^i : K^i \to K^{i+1}$ étant donné par la formule

$$df(g_1, ..., g_{i+1}) = g_1 f(g_2, ..., g_{i+1}) + \sum_{j=1}^{i} (-1)^j f(g_1, ..., g_j g_{j+1}, ..., g_{i+1}) + (-1)^{i+1} f(g_1, ..., g_i)$$

En particulier l'ensemble des 1-cochaînes (non homogènes) K^1 est constitué des fonctions de G dans A, l'ensemble des 1-cocyles $Z^1(G, A) \subset K^1$ est le sous-groupe des fonctions f vérifiant de plus $f(g_1g_2) = f(g_1) + g_1 f(g_2)$ pour tous g_1, g_2 de G, et l'ensemble des 1-cobords $B^1(G, A)$ est l'ensemble des fonctions de la forme $g \mapsto g.a - a$ avec $a \in A$. On a $H^1(G, A) = Z^1(G, A)/B^1(G, A)$.

Corollaire 1.18 *Si G et A sont finis, tous les groupes $H^i(G, A)$ sont finis.*

Remarque : Ce dernier corollaire peut aussi s'obtenir par décalage avec le corollaire 1.14, en remarquant que si A et G sont finis, alors A se plonge dans le module induit $I_G(A)$ qui est également fini. On verra un peu plus loin que la conclusion est encore valable pour $i \geq 1$ si A est seulement supposé de type fini en tant que $\mathbf{Z}$-module.

Exemples ; a) Un élément de $Z^1(G, A)$ s'appelle un *homomorphisme croisé*. Quand l'action de G sur A est triviale, un homomorphisme croisé est simplement un homomorphisme et $B^1(G, A) = 0$, ce qui fait que $H^1(G, A)$ est alors l'ensemble des morphismes de groupes de G dans A.

b) On déduit de a) que pour tout groupe fini G agissant trivialement sur un groupe abélien sans torsion A, on a $H^1(G, A) = 0$. De même, si $G = \mathbf{Z}/p$ agit trivialement sur un groupe abélien A, on a $H^1(G, A) \simeq A[p]$, où $A[p]$ est le sous-groupe de p-torsion de A.

c) Un 2-cocycle est une application f de $G \times G$ dans A vérifiant :

$$g_1 f(g_2, g_3) - f(g_1 g_2, g_3) + f(g_1, g_2 g_3) - f(g_1, g_2) = 0$$

On dit que c'est un *système de facteurs.* [4]

1.5. La suite spectrale de Hochschild-Serre

Dans ce paragraphe, on ne va plus travailler avec un seul groupe G, mais considérer ce qui se passe quand on change le groupe qui agit. Soit donc A un G-module et soit G' un groupe équipé d'un morphisme $f : G' \to G$. On peut alors munir A d'une structure de G'-module en posant

$$g'.a := f(g').a \quad g' \in G', \quad a \in A$$

Notons f^*A (ou simplement A si cela ne prête pas à confusion) ce G'-module. Comme A^G est alors un sous-groupe de $(f^*A)^{G'}$, on obtient un morphisme de foncteurs de $H^0(G, .)$ dans $H^0(G', f^*.)$. La propriété universelle des foncteurs dérivés ([16], Th. 2.4.7) montre alors que pour tout entier $i \geq 0$, on a une unique famille de morphismes de foncteurs

$$f_i^* : H^i(G, .) \to H^i(G', .)$$

qui sont compatibles avec les applications δ^i des longues suites exactes de cohomologie (en un sens évident). On a ainsi obtenu un *morphisme de foncteurs cohomologiques.*

4. On peut montrer ([16], Th. 6.6.3) que $H^2(G, A)$ classifie les extensions de groupes E de G par A telles que l'action (par conjugaison dans E) de G sur A correspondant à E soit l'action donnée par la structure de G-module de A. Le cas où cette action est triviale correspond aux extensions centrales.

Soient maintenant A' un G'-module et $u : A \to A'$ un morphisme de groupes abéliens. Si de plus u est *f-compatible*, i.e. vérifie

$$u(f(g').a) = g'.u(a) \quad g' \in G', \quad a \in A$$

alors u est un G'-homomorphisme de f^*A dans A' et il induit un homomorphisme $u_* : H^i(G', f^*A) \to H^i(G', A')$. En le composant avec f_i^*, on obtient finalement un homomorphisme

$$H^i(G, A) \to H^i(G', A')$$

associé au morphisme de groupes $f : G' \to G$ et au morphisme f-compatible $u : A \to A'$. Cet homomorphisme s'exprime de manière évidente en utilisant la définition explicite des H^i par les cochaînes. De plus si on a un morphisme f-compatible de suites exactes courtes de la suite $0 \to A \to B \to C \to 0$ vers $0 \to A' \to B' \to C' \to 0$, les morphismes correspondant entre les H^i sont encore compatibles avec les applications δ^i des longues suites exactes associées à ces suites exactes courtes (on a donc encore un morphisme de foncteurs cohomologiques).

Définition 1.19 a) Soient G un groupe, A un G-module, et H un sous-groupe de G. En prenant pour f l'injection canonique de H dans G, on obtient pour $i \geq 0$ un homomorphisme Res : $H^i(G, A) \to H^i(H, A)$ qu'on appelle homomorphisme de *restriction*.

b) Soient G un groupe et A un G-module. Pour tout sous-groupe distingué H de G, le groupe quotient G/H agit sur A^H et l'inclusion $A^H \to A$ est compatible avec la surjection canonique $G \to G/H$. On en déduit pour $i \geq 0$ un homomorphisme Inf : $H^i(G/H, A^H) \to H^i(G, A)$ qu'on appelle homomorphisme d'*inflation*.

Soit maintenant H un sous-groupe d'un groupe G et soit A un H-module. On dispose du G-module $I_G^H(A)$. En associant à tout $u \in I_G^H(A)$ sa valeur en 1, on obtient un morphisme de groupes abéliens $I_G^H(A) \to A$ qui est compatible avec l'injection $H \to G$. On en déduit des homomorphismes

$$H^i(G, I_G^H(A)) \to H^i(H, A)$$

Theorème 1.20 (Lemme de Shapiro) *Les homomorphismes*

$$H^i(G, I_G^H(A)) \to H^i(H, A)$$

définis ci-dessus sont des isomorphismes.

Démonstration : La proposition 1.12 donne

$$\mathrm{Hom}_G(B, I_G^H(A)) = \mathrm{Hom}_H(B, A)$$

pour tout G-module B. On en déduit immédiatement que $A \mapsto I_G^H(A)$ préserve les injectifs ; d'autre part, en appliquant la formule ci-dessus à $B = \mathbf{Z}$, on obtient pour tout H-module A l'égalité $(I_G^H(A))^G = A^H$. Pour obtenir le résultat (via une résolution injective du H-module A, à laquelle on applique $I_G^H(.)$), il suffit alors de vérifier que $A \mapsto I_G^H(A)$ est un foncteur exact de $\mathcal{M}od_H$ dans $\mathcal{M}od_G$. Or on a

$$I_G^H(A) = \mathrm{Hom}_H(\mathbf{Z}[G], A)$$

et le résultat découle alors de ce que $\mathbf{Z}[G]$ est un $\mathbf{Z}[H]$-module libre : une base est constituée d'un système de représentants $(g_j)_{j\in J}$ des classes à droite de G selon H car tout élément g de G s'écrit alors de manière unique $g = hg_j$ avec $j \in J$.

□

Une autre construction va être utile dans la suite. Soient G un groupe et A un G-module. Soit $t \in G$; prenons $G' = G$, $A' = A$, et notons $f : g \mapsto tgt^{-1}$ l'automorphisme intérieur associé à t. L'homomorphisme de groupes abéliens $u : a \mapsto t^{-1}a$ de A dans A est alors f-compatible, et il induit donc pour tout $i \geq 0$ un homomorphisme $\sigma_t : H^i(G, A) \mapsto H^i(G, A)$.

Proposition 1.21 *L'application σ_t est l'identité.*

Démonstration : On procède par récurrence sur i. Le cas $i = 0$ est immédiat. Dans le cas général, on plonge A dans un module induit I et on pose $B = I/A$. On a alors un diagramme commutatif à lignes exactes :

$$\begin{array}{ccccc} H^i(G,B) & \xrightarrow{\delta} & H^{i+1}(G,A) & \longrightarrow & 0 \\ \downarrow{\scriptstyle \sigma_t} & & \downarrow{\scriptstyle \sigma_t} & & \\ H^i(G,B) & \xrightarrow{\delta} & H^{i+1}(G,A) & \longrightarrow & 0 \end{array}$$

d'où le résultat par récurrence sur i.

□

Si H est un sous-groupe distingué de G, on peut de même faire opérer G sur $H^i(H, A)$ via l'action par conjugaison de G sur H. La proposition 1.21 dit alors que H opère trivialement sur $H^i(H, A)$, autrement dit G/H opère sur $H^i(H, A)$.

Theorème 1.22 (Restriction-inflation) *Soit G un groupe. Soient H un sous-groupe distingué de G et A un G-module. Alors la suite*

$$0 \to H^1(G/H, A^H) \overset{\text{Inf}}{\to} H^1(G, A) \overset{\text{Res}}{\to} H^1(H, A)$$

est exacte.

Démonstration : [5] Il est immédiat (via par exemple la description par les cochaînes) que la suite est un complexe. Montrons d'abord l'injectivité de Inf. Soit $f : G/H \to A^H$ un 1-cocycle cohomologue à 0 dans $H^1(G, A)$. On peut aussi voir f comme une application de G dans A constante sur chaque classe modulo H. Il existe alors $a \in A$ tel que $f(s) = s.a - a$ pour tout s de G ; pour tout t de h, on a $f(t) = f(1)$ donc $t.a = a$. Ainsi $a \in A^H$ et la classe de f dans $H^1(G/H, A^H)$ est bien nulle.

Montrons maintenant qu'un élément de $\operatorname{Ker}\text{Res}$ est dans Im Inf. Soit $f : G \to A$ un 1-cocycle. Dire que $\text{Res}(f) = 0$, c'est dire qu'il existe $a \in A$ tel que $f(t) = t.a - a$ pour tout t de H. Quitte à remplacer f par le cocycle cohomologue $G \to A,\ t \mapsto f(t) - (t.a - a)$, on peut supposer $f(t) = 0$ pour tout t de H. Comme pour tous s, t de G on a $f(st) = f(s) + s.f(t)$, on obtient alors que f se factorise en une application $\bar{f} : G/H \to A$. Pour s dans H, les classes de st et t dans G/H sont les mêmes (bien noter que H est distingué dans G) ; la formule donne donc $\bar{f}(t) = s\bar{f}(t)$ pour tous $t \in G, s \in H$, ce qui montre que $\bar{f}$ est à valeurs dans A^H ; c'est un cocycle qui induit un élément de $H^1(G/H, A^H)$ dont l'image par Inf est f.

□

Comme on l'a vu après la proposition 1.21, le groupe G/H opère sur les groupes de cohomologie $H^i(H, A)$. On peut alors voir la suite de restriction-inflation comme la suite exacte des termes de bas degré d'une suite spectrale, donnée par le théorème suivant :

Theorème 1.23 (Hochschild-Serre) *Soit G un groupe. Soient H un sous-groupe distingué de G et A un G-module. Alors on a une suite spectrale*

$$E_2^{pq} = H^p(G/H, H^q(H, A)) \Rightarrow H^{p+q}(G, A)$$

5. Ce résultat peut se déduire de la suite spectrale de Hochschild-Serre donnée plus bas, mais il est instructif de faire la vérification directement, d'autant que cette méthode se généralise au "H^1 non-abélien", cf. [13], annexe au chapitre VII.

Démonstration (esquisse): C'est un cas particulier de la suite spectrale des foncteurs composés de Grothendieck ([16], Th. 5.8.3.). Le foncteur $A \mapsto A^G$ de $\mathcal{M}od_G$ dans $\mathcal{A}b$ est le composé du foncteur $A \mapsto A^H$ de $\mathcal{M}od_G$ dans $\mathcal{M}od_{G/H}$ et du foncteur $B \mapsto B^{G/H}$ de $\mathcal{M}od_{G/H}$ dans $\mathcal{A}b$. Il suffit alors de vérifier que le premier de ces deux foncteurs préserve les injectifs, ce qui est facile car c'est l'adjoint à droite du foncteur d'oubli de $\mathcal{M}od_{G/H}$ vers $\mathcal{M}od_G$; de façon explicite on a pour tout G/H-module B (qu'on peut aussi voir comme un G-module avec action triviale de H) et pour tout G-module A :

$$\mathrm{Hom}_G(B, A) = \mathrm{Hom}_{G/H}(B, A^H)$$

□

Cela signifie en particulier que pour chaque $n > 0$; on a une filtration de $H^n(G, A)$ par une suite décroissante $F^0 = H^n(G, A) \supset ... \supset F^{n+1} = 0$, où F^p/F^{p+1} (pour $p = 0, ..., n$) est isomorphe à un sous-quotient de $H^p(G/H, H^{n-p}(H, A))$. La suite exacte des termes de bas degré de cette suite spectrale s'écrit

$$0 \to H^1(G/H, A^H) \overset{\mathrm{Inf}}{\to} H^1(G, A) \overset{\mathrm{Res}}{\to} H^1(H, A)^{G/H} \to H^2(G/H, A^H) \overset{\mathrm{Inf}}{\to} H^2(G, A)$$

(la flèche sans nom s'appelle la *transgression*). On obtient aussi le résultat suivant, qui généralise la suite exacte de restriction-inflation :

Corollaire 1.24 *Soit G un groupe. Soient H un sous-groupe distingué de G et A un G-module. On fait l'hypothèse supplémentaire que $H^i(H, A) = 0$ pour $1 \leq i \leq q-1$. Alors la suite*

$$0 \to H^q(G/H, A^H) \overset{\mathrm{Inf}}{\to} H^q(G, A) \overset{\mathrm{Res}}{\to} H^q(H, A)$$

est exacte.

On peut également démontrer ce corollaire directement par récurrence sur i (cf. [13], proposition 5 p. 126) en commençant par plonger A dans le G-module induit $I_G(A)$, qui est aussi induit en tant que H-module vu que $\mathbf{Z}[G]$ est un $\mathbf{Z}[H]$-module libre, ce qui implique qu'on peut écrire

$$\mathbf{Z}[G] = \mathbf{Z}[H] \otimes_{\mathbf{Z}} M$$

(où M est un groupe abélien), puis

$$\mathrm{Hom}_{\mathbf{Z}}(\mathbf{Z}[G], X) = \mathrm{Hom}_{\mathbf{Z}}(\mathbf{Z}[H], \mathrm{Hom}_{\mathbf{Z}}(M, X))$$

pour tout groupe abélien X.

1.6. Corestriction ; applications

Soit H un sous-groupe *d'indice fini* d'un groupe G. Soit A un G-module. Dans cette situation particulière, on va voir que l'on peut définir des homomorphismes $H^i(H, A) \to H^i(G, A)$ "en sens inverse" de la restriction. On commence par le cas $i = 0$. La corestriction est alors définie par la *norme* :

$$N_{G/H} : a \mapsto \sum_{s \in G/H} s.a$$

de A^H vers A^G, où G/H est l'ensemble (qui est fini par hypothèse) des classes à gauche selon H. Il est immédiat que $s.a$ ne dépend que de la classe de s dans G/H (parce que $a \in A^H$) et que $N_{G/H}(a) \in A^G$.

On peut alors prolonger la corestriction en degré 0 en un unique morphisme du foncteur cohomologique $\{H^i(H, f^*.), \delta\}$ dans le foncteur cohomologique $\{H^i(G, .), \delta\}$, où f est l'inclusion $H \to G$. Ceci est possible (cf. [16], pp. 48–49) car le premier de ces foncteurs est *effaçable*[6] en degré ≥ 1, donc universel. On obtient ainsi des homomorphismes de *corestriction*

$$\mathrm{Cor} : H^i(H, A) \to H^i(G, A)$$

qui sont compatibles avec les morphismes de suites exactes courtes au sens habituel.

Theorème 1.25 *Soit $m = [G : H]$ l'indice de H dans G. Alors la composée* $\mathrm{Cor} \circ \mathrm{Res}$ *est la multiplication par m dans $H^i(G, A)$.*

Démonstration : C'est clair pour $i = 0$. On en déduit le cas général par décalage (en plongeant A dans un module induit I) via le corollaire 1.14.

□

Corollaire 1.26 *Soit G un groupe fini de cardinal m. Soit A un G-module. Alors pour $i > 0$, les groupes $H^i(G, A)$ sont de m-torsion.*

En particulier si A est de plus de n-torsion avec n premier à m, on obtient $H^i(G, A) = 0$ pour $i > 0$.

Démonstration : Il suffit d'appliquer le théorème 1.25 dans le cas $H = \{1\}$.

□

Corollaire 1.27 *Soit G un groupe fini. Alors pour tout G-module A qui est de type fini comme $\mathbf{Z}$-module, on a $H^i(G, A)$ fini pour $i > 0$.*

6. Si I est induit pour G, il est induit pour H et $H^i(H, I) = 0$ pour tout $i > 0$; or tout G-module se plonge dans un G-module induit I.

Démonstration : La description via les cochaînes montre que les groupes $H^i(G, A)$ sont de type fini. Comme pour $i > 0$ ils sont de torsion d'après le corollaire 1.26, ils sont finis.

□

Corollaire 1.28 *Soit G un groupe fini. Soit A un groupe abélien uniquement divisible muni d'une action de G (ex. $A = \mathbf{Q}$ avec action triviale de G). Alors $H^i(G, A) = 0$ pour tout $i > 0$.*

Démonstration : En effet le corollaire 1.26 dit que pour $i > 0$, le groupe $H^i(G, A)$ est de torsion ; mais d'un autre côté la multiplication par n dans A est un isomorphisme pour tout $n > 0$ par hypothèse, donc la multiplication par n dans $H^i(G, A)$ est également un isomorphisme.

□

Exemple : Soit $A = \mathbf{Q}/\mathbf{Z}$ avec action triviale d'un groupe fini G. D'après le corollaire précédent et la suite exacte longue de cohomologie, on a $H^i(G, \mathbf{Q}/\mathbf{Z}) = H^{i+1}(G, \mathbf{Z})$ pour tout $i > 0$. En particulier $H^2(G, \mathbf{Z}) = H^1(G, \mathbf{Q}/\mathbf{Z})$ est le *groupe des caractères* de G. On a aussi $H^1(G, \mathbf{Z}) = 0$ vu que $\mathbf{Z}$ n'a pas de sous-groupes finis non triviaux.

1.7. Exercices

Dans tous ces exercices, G désigne un groupe.

1. Soit H un sous-groupe d'indice fini de G. Soit A un G-module.

a) Montrer qu'on définit un homomorphisme surjectif $\pi : I_G^H(A) \to A$ de G-modules par la formule :

$$\pi(f) = \sum_{g \in G/H} g.f(g^{-1}) \quad , f \in I_G^H(A)$$

b) Soit $i \geq 0$. Soit $\pi_* : H^i(H, A) = H^i(G, I_G^H(A)) \to H^i(G, A)$ l'homomorphisme induit sur la cohomologie. Montrer que π_* est la corestriction.

2. Soit G un groupe fini. On dit qu'un G-module A est un *G-module de permutation* s'il existe un sous-groupe H de G tel que A soit isomorphe à $I_G^H(\mathbf{Z})$ (où $\mathbf{Z}$ est muni de l'action triviale).

a) Montrer que si A est un G-module de permutation, alors $H^1(G, A) = 0$.

b) A-t-on $H^2(G, A) = 0$ pour tout module de permutation A ?

c) Montrer qu'un G-module A est de permutation si et seulement si le $\mathbf{Z}$-module A possède une base finie $(e_1, ..., e_n)$ telle qu'il existe une permutation transitive σ de l'ensemble $\{1, ..., n\}$ avec $g.e_i = e_{\sigma(i)}$ pour tout i de $\{1, ..., n\}$.

3. Soit $G = \mathbf{Z}/p$ (avec p premier) et soit (pour $n \in \mathbf{N}$) A_n le G-module $\mathbf{Z}$ avec action triviale de G. Soit ℓ un nombre premier différent de p, considérons le système projectif (A_n), les flèches de transition étant la multiplication par ℓ. Comparer $\varprojlim_n H^2(G, A_n)$ et $H^2(G, \varprojlim_n A_n)$.

4. Soit G le groupe additif $\mathbf{Z}^{(\mathbf{N})}$, agissant trivialement sur une famille infinie $(A_j)_{j \in J}$ de groupes abéliens. Montrer que

$$H^1(G, \bigoplus_j A_j) = (\bigoplus_j A_j)^{\mathbf{N}}$$

mais qu'on a

$$\bigoplus_j H^1(G, A_j) = \bigoplus_j (A_j)^{\mathbf{N}}$$

et en déduire que ces deux groupes ne coïncident pas (merci à Joël Riou qui m'a signalé cet exemple).

5. Soit X un ensemble et soit G le groupe libre sur X. Soit I_G l'idéal d'augmentation de $\mathbf{Z}[G]$, défini comme noyau de l'homomorphisme $\sum_{g \in G} a_g g \mapsto \sum_{g \in G} a_g$ de $\mathbf{Z}[G]$ dans $\mathbf{Z}$.

a) Montrer que I_G est un $\mathbf{Z}[G]$-module libre de base $\{x - 1, x \in X\}$.

b) En déduire que le G-module $\mathbf{Z}$ admet une résolution

$$0 \to I_G \to \mathbf{Z}[G] \to \mathbf{Z} \to 0$$

par des $\mathbf{Z}[G]$-modules libres.

c) Conclure que si A est un G-module et $n \geq 2$, on a $H^n(G, A) = 0$.

2. Cohomologie des groupes finis

Dans tout ce chapitre, G désignera un groupe *fini* (sauf mention expresse du contraire).

2.1. Les groupes de cohomologie modifiés de Tate

Il se trouve (notamment pour les théorèmes de dualité en arithmétique, lorsque les corps de nombres considérés ont des places réelles ou encore lorsque l'on veut développer le formalisme des formations de classes) qu'il est souvent commode dans le cas d'un groupe G fini d'introduire des groupes $\widehat{H}^i(G,A)$ pour tout $i \in \mathbf{Z}$, qui coïncident avec les $H^i(G,A)$ pour $i \geq 1$ mais donnent un peu plus d'information pour $i \leq 0$. C'est surtout le cas $i = 0$ qui sera utile, à part quand nous aborderons les formations de classes où on utilisera aussi le cas $i = -2$.

Définition 2.1 La *norme* de l'algèbre de groupe $\mathbf{Z}[G]$ est l'élément $\sum_{g\in G} g$. L'*idéal d'augmentation* I_G de l'algèbre de groupe $\mathbf{Z}[G]$ est le noyau de l'homomorphisme $\mathbf{Z}[G] \to \mathbf{Z}$ défini par $\sum_{g\in G} a_g g \mapsto \sum_{g\in G} a_g$.

Noter que la définition de la norme est spécifique au cas où G est fini. On peut aussi dire que I_G est l'ensemble des combinaisons linéaires (à coefficients dans $\mathbf{Z}$) des $(g-1)$, $g \in G$. Si A est un G-module, la norme définit un endomorphisme $N : A \to A$ par la formule $N(x) = \sum_{g\in G} g.x$. Noter que $I_G A \subset \ker N$ et $\operatorname{Im} N \subset H^0(G,A)$.

Définition 2.2 Soit A un G-module. Le G-module des *co-invariants* est le G-module $A_G = H_0(G,A) := A/I_G A$. C'est le plus grand G-module quotient de A sur lequel G agit trivialement.

Par passage au quotient, on a donc un homomorphisme (qu'on peut aussi noter N_A^* s'il y a ambigüité)

$$N^* : H_0(G,A) \to H^0(G,A)$$

Définition 2.3 On pose $\widehat{H}_0(G,A) = \ker N^*$ et $\widehat{H}^0(G,A) = \operatorname{coker} N^*$.

Autrement dit $\widehat{H}_0(G,A) =_N A/I_G A$ et $\widehat{H}^0(G,A) = A^G/NA$, où ${}_N A$ est le noyau de la norme dans A. Noter que ces groupes sont nuls si G est le groupe trivial (ce qui n'était pas le cas de $H_0(G,A)$ et $H^0(G,A)$).

Le foncteur $A \mapsto H_0(G,A)$ est covariant et exact à droite. On peut alors définir les *groupes d'homologie* $H_i(G,A)$ comme ses foncteurs dérivés à gauche. On obtient un foncteur homologique, i.e. si $0 \to A \to B \to C \to 0$ est une suite exacte de G-modules, on a une suite exacte longue fonctorielle :

$$\ldots \to H_1(G,A) \to H_1(G,B) \to H_1(G,C) \to H_0(G,A) \to H_0(G,B) \to H_0(G,C) \to 0$$

De plus $H_i(G,A) = 0$ pour $i > 0$ si A est projectif, ou même relativement projectif (=facteur direct d'un co-induit) ; les démonstrations sont exactement du même type que pour la cohomologie (et cette construction ne nécessite pas G fini).

Voici un exemple de groupe d'homologie, qui sera utile plus tard (quand on appliquera au chapitre 7 le théorème de Tate-Nakayama aux corps p-adiques) :

Proposition 2.4 *Soit G un groupe. Alors $H_1(G,\mathbf{Z})$ est l'abélianisé $G^{\mathrm{ab}} = G/D(G)$ de G, où $D(G)$ est le sous-groupe dérivé de G.*

Démonstration : Soit $\Lambda = \mathbf{Z}[G]$ l'algèbre du groupe G. Considérons la suite exacte de G-modules

$$0 \to I_G \to \Lambda \stackrel{\pi}{\to} \mathbf{Z} \to 0$$

où $\pi : \sum_g n_g g \mapsto \sum_g n_g$ est l'homomorphisme d'augmentation. On a alors $H_0(G,I_G) = I_G/I_G^2$, ce qui fait que l'image de $H_0(G,I_G)$ dans $H_0(G,\Lambda) = \Lambda/I_G\Lambda$ est nulle. D'autre part $H_1(G,\Lambda) = 0$ vu que Λ est libre sur $\mathbf{Z}[G]$, d'où un isomorphisme (via la suite exacte d'homologie)

$$d : H_1(G,\mathbf{Z}) \to H_0(G,I_G) = I_G/I_G^2$$

Définissons alors $f : G \to I_G/I_G^2$ par $f(g) = g-1$. La formule $gh-1 = (g-1)+(h-1)+(g-1)(h-1)$ (valable pour g,h dans G) montre que c'est un morphisme. Comme I_G/I_G^2 est abélien, f induit un morphisme (noté encore f) de $G/D(G)$ vers I_G/I_G^2, qui est clairement surjectif. Enfin le morphisme de groupes $u : I_G \to G/D(G)$ défini par $u(g-1) = \bar{g}$ passe au quotient par I_G^2 car si $x = (g-1)(h-1)$ est dans I_G^2, alors $u(x) = u((gh-1)-(g-1)-(h-1)) = \overline{gh}\bar{g}^{-1}\bar{h}^{-1}$ est l'élément neutre de $G/D(G)$ vu que $ghg^{-1}h^{-1}$ est un commutateur. On obtient donc un morphisme $\bar{u} : I_G/I_G^2 \to G/D(G)$ tel que $\bar{u} \circ f$ soit l'identité, donc f est bijective.

□

On va maintenant "raccorder" les suites exactes longues d'homologie et de cohomologie associées à une suite exacte de G-modules via les *groupes de cohomologie modifiés* de Tate. C'est l'objet de la définition suivante :

Définition 2.5 Soit G un groupe fini. Soit A un G-module. On définit les groupes $\widehat{H}^n(G,A)$ pour $n \in \mathbf{Z}$ par la formule :

$$\widehat{H}^n(G,A) = H^n(G,A) \quad n \geq 1$$

$$\widehat{H}^0(G,A) = A^G/NA$$
$$\widehat{H}^{-1}(G,A) = \widehat{H}_0(G,A) =_N A/I_G A$$
$$\widehat{H}^{-n}(G,A) = H_{n-1}(G,A) \quad n \geq 2$$

L'intérêt réside dans le théorème suivant :

Theorème 2.6 *Soit* $0 \to A \to B \to C \to 0$ *une suite exacte de G-modules. Alors on a une suite exacte longue "fonctorielle" :*

$$...\widehat{H}^{-2}(G,C) \to \widehat{H}^{-1}(G,A) \to \widehat{H}^{-1}(G,B) \to \widehat{H}^{-1}(G,C)$$

$$\stackrel{\delta}{\to} \widehat{H}^0(G,A) \to \widehat{H}^0(G,B) \to \widehat{H}^0(G,C) \to H^1(G,A) \to ...$$

De plus si A est relativement injectif (=relativement projectif), on a $\widehat{H}^n(G,A) = 0$ *pour tout* $n \in \mathbf{Z}$.

Démonstration : Les suites exactes d'homologie et de cohomologie fournissent un diagramme commutatif à lignes exactes :

$$\begin{array}{ccccccccc}
H_1(G,C) & \longrightarrow & H_0(G,A) & \longrightarrow & H_0(G,B) & \longrightarrow & H_0(G,C) & \longrightarrow & 0 \\
\downarrow & & {\scriptstyle N_A^*}\downarrow & & {\scriptstyle N_B^*}\downarrow & & {\scriptstyle N_C^*}\downarrow & & \downarrow \\
0 & \longrightarrow & H^0(G,A) & \longrightarrow & H^0(G,B) & \longrightarrow & H^0(G,C) & \longrightarrow & H^1(G,A)
\end{array}$$

Un tel diagramme définit canoniquement un homomorphisme

$$\delta : \ker N_C^* \to \operatorname{coker} N_A^*$$

(si $c \in \ker N_C^*$, on le relève en $b \in H_0(G,B)$, puis on relève $N_B^*(b)$ en $a \in H^0(G,A)$; on vérifie alors que la classe $\bar{a} := \delta(c)$ de a dans $\operatorname{coker} N_A^*$ ne dépend pas du choix de b). On a donc défini $\delta : \widehat{H}_0(G,C) \to \widehat{H}^0(G,A)$. Le lemme du serpent ([16], 1.3.2.), joint aux suites exactes longues d'homologie et de cohomologie, donne alors la suite exacte voulue vu que pour tout G-module M, $\widehat{H}_0(G,M)$ est un sous-groupe de $H_0(G,M)$ et $\widehat{H}^0(G,M)$ est un quotient de $H^0(G,M)$ (ce qui permet de faire les "raccords").

Montrons maintenant que si A est relativement injectif, tous les $\widehat{H}^n(G,A)$ sont nuls. Pour $n \geq 1$, c'est la proposition 1.13. La preuve pour $n \leq -2$ est exactement similaire (en remplaçant les induits par les co-induits, les injectifs par les projectifs etc.). Vérifions le directement pour $n = 0$ (le cas $n = -1$ est similaire). Il suffit de traiter le cas où $A = \mathbf{Z}[G] \otimes_{\mathbf{Z}} X$ est co-induit (=induit vu que G est fini). Alors X s'identifie à un sous-groupe de A, et A est la somme directe des gX pour $g \in G$. Tout élément x de A s'écrit alors de

façon unique $x = \sum_{g \in G} g x_g$ avec $x_g \in X$, et un tel élément est dans A^G ssi tous les x_g sont égaux, i.e. ssi $a = Nx$ avec $x \in X$. Ainsi $\widehat{H}^0(G, A) = 0$.

□

Les $\widehat{H}^n$ forment ainsi un foncteur cohomologique, vérifiant $\widehat{H}^n(G, A) = 0$ pour tout G-module induit (ou co-induit) A et tout $n \in \mathbf{Z}$. En particulier on a :

Corollaire 2.7 *Soit*

$$0 \to A \to I \to B \to 0$$

une suite exacte de G-modules avec I relativement injectif (par exemple induit). Alors pour tout $n \in \mathbf{Z}$, on a $\widehat{H}^n(G, B) = \widehat{H}^{n+1}(G, A)$.

Cela permet de montrer des propriétés par décalage en écrivant un G-module quelconque comme sous G-module ou G-module quotient d'un induit.

2.2. Changement de groupe

Soit A un G-module. Soit H un sous-groupe de G. On a $N_G A \subset N_H A$ (pour le voir, regrouper les éléments de G en classes à droite selon H), d'où par passage au quotient un homomorphisme de restriction Res : $\widehat{H}^0(G, A) \to \widehat{H}^0(H, A)$.

D'autre part on peut également définir des homomorphismes de restriction et corestriction en homologie, mais l'hypothèse que le sous-groupe H est d'indice fini est cette fois nécessaire pour la restriction (et non pour la corestriction). La corestriction $H_i(H, A) \to H_i(G, A)$ $(i \geq 0)$ est simplement le foncteur homologique qui pour $i = 0$ correspond à la surjection canonique $A/I_H A \to A/I_G A$; la restriction $H_i(G, A) \to H_i(H, A)$ (laquelle si G est quelconque n'est définie que quand H est d'indice fini dans G) est le foncteur cohomologique qui pour $i = 0$ est donné par l'homomorphisme $N'_{G/H} : A/I_G A \to A/I_H A$ défini par

$$N'_{G/H}(x) = \sum_{s \in G/H} s^{-1}.x$$

(si s et t sont dans la même classe à gauche selon H, alors $s^{-1}.x$ et $t^{-1}.x$ coïncident modulo $I_H A$). On vérifie immédiatement que l'homomorphisme de restriction $H_0(G, A) \to H_0(H, A)$ induit par passage aux sous-groupes un homomorphisme Res : $\widehat{H}_0(G, A) \to \widehat{H}_0(H, A)$.

Finalement on a défini pour tout $n \in \mathbf{Z}$ des homomorphismes Res : $\widehat{H}^n(G, A) \to \widehat{H}^n(H, A)$. On obtient encore un morphisme de foncteurs cohomologiques via

Lemme 2.8 *La famille d'homomorphismes* Res : $\widehat{H}^n(G,.) \to \widehat{H}^n(H,.)$ *est compatible avec les suites exactes.*

Démonstration : Soit $0 \to A \to B \to C \to 0$ une suite exacte de G-modules. Il s'agit de vérifier que le diagramme

$$\begin{array}{ccc} \widehat{H}^n(G,C) & \xrightarrow{\delta} & \widehat{H}^{n+1}(G,A) \\ {\scriptstyle \mathrm{Res}}\downarrow & & {\scriptstyle \mathrm{Res}}\downarrow \\ \widehat{H}^n(H,C) & \xrightarrow{\delta} & \widehat{H}^{n+1}(H,A) \end{array}$$

commute. Ceci a déjà été vu pour $n \geq 0$ et pour $n \leq -2$, il reste à vérifier directement le cas $n = -1$. Alors $\widehat{H}^n(G,C) =_N C/I_G C$ et $\widehat{H}^{n+1}(G,A) = A^G/NA$ (et de même pour H). Soit donc $c \in_N C$ dont on note $\bar{c}$ la classe dans $\widehat{H}^{-1}(G,C)$. La classe de $\delta(\bar{c})$ s'obtient en relevant c en un $b \in B$ et en prenant la classe de $N_G(b)$ dans $A^G/N_G A$. La classe de $N_G(b)$ dans $A^G/N_H A$ est donc $\mathrm{Res}(\delta(\bar{c}))$.

D'un autre côté, $\mathrm{Res}(\bar{c})$ est la classe de $\sum_{i\in I} s_i c$, où $(s_i)_{i\in I}$ est un système de représentants des classes à droite $H \setminus G$. Alors $\delta(\mathrm{Res}(\bar{c})) = N_H(\sum_{i\in I} s_i b)$, qui est bien égal à $N_G(B)$.

□

On a de même des morphismes de corestriction (donnant un morphisme de foncteurs cohomologiques) Cores : $\widehat{H}^n(H,A) \to \widehat{H}^n(G,A)$. Pour $n = 0$, la corestriction est induite par $x \mapsto \sum_{g\in G/H} g.x$ de A^H dans A^G et pour $n = -1$, elle est induite par la surjection canonique $H_0(H,A) \to H_0(G,A)$ par passage aux sous-groupes $\widehat{H}_0(H,A)$ et $\widehat{H}_0(G,A)$.

On alors une généralisation des résultats du chapitre 1 :

Theorème 2.9 *Soit G un groupe fini. Soit H un sous-groupe de G d'indice m. Soit $n \in \mathbf{Z}$. Alors :*

a) La composée Cor $\circ$ Res *est la multiplication par m dans $\widehat{H}^n(G,A)$.*

b) Le groupe $\widehat{H}^n(G,A)$ est annulé par l'ordre de G.

c) Si A est de type fini, tous les groupes $\widehat{H}^n(G,A)$ sont finis.

Noter en particulier que contrairement à ce qui se passe pour $H^0(G,A)$ (non modifié), les résultats sont ici valables pour $n = 0$.

Démonstration : C'est tout à fait analogue au théorème 1.25 et à ses corollaires, une fois qu'on a vérifié directement que Cor $\circ$ Res est la multiplication par m dans $\widehat{H}^0(G,A)$.

□

2.3. Cohomologie d'un groupe cyclique

Soit G un groupe cyclique de cardinal n. L'un des intérêts de la cohomologie modifiée de Tate est que dans ce cas, la suite des groupes $\widehat{H}^q(G,A)$ (pour $q \in \mathbf{Z}$) est 2-périodique, ce qui permet de les calculer facilement en se ramenant à $\widehat{H}^0(G,A)$ et $\widehat{H}^{-1}(G,A)$, qui admettent des descriptions explicites. On a en effet le théorème suivant :

Theorème 2.10 *On suppose que le groupe fini G est cyclique d'ordre n. Soit A un G-module. Alors pour tout $q \in \mathbf{Z}$, les groupes $\widehat{H}^q(G,A)$ et $\widehat{H}^{q+2}(G,A)$ sont isomorphes.*

Démonstration : La preuve va consister à identifier les $\widehat{H}^q(G,A)$ à la cohomologie d'un certain complexe qui sera 2-périodique par construction. Fixons un générateur s de G et posons $D = s-1$ dans $\mathbf{Z}[G]$. On a d'autre part $N = \sum_{t\in G} t = \sum_{i=0}^{n-1} s^i$. Définissons alors un complexe $K(A)$ par $K^i(A) = A$ pour tout $i \in \mathbf{Z}$, les cobords $d^i : K^i(A) \to K^{i+1}(A)$ étant donnés par les formules : d^i est la multiplication par D si i est pair et d^i est la multiplication par N si i est impair (il s'agit bien d'un complexe car $ND = DN = 0$).

Pour toute suite exacte $0 \to A \to B \to C \to 0$ de G-modules, on a une suite correspondante de complexes

$$0 \to K(A) \to K(B) \to K(C) \to 0$$

d'où une suite exacte longue associée avec des opérateurs de cobord δ^i. On obtient ainsi un foncteur cohomologique $(H^q(K(.))_{q\in\mathbf{Z}}, \delta)$ qui est clairement 2-périodique par rapport à q. Pour conclure il nous suffit de montrer qu'il est isomorphe au foncteur $(\widehat{H}^q(G,.),\delta)$.

Comme G est engendré par s, on a $A^G = \ker D$ et $I_G = \operatorname{Im} D$. Il en résulte que pour $q = 0$ et $q = -1$, on a bien $\widehat{H}^q(G,A) = H^q(K(A))$ et l'opérateur de cobord entre le degré -1 et le degré 0 est le même. En particulier si A est relativement injectif, on a $H^q(K(A)) = 0$ pour $q = -1, 0$, donc pour tout $q \in \mathbf{Z}$ vu que le complexe $K(A)$ est 2-périodique. On conclut que pour tout G-module A et tout $q \in \mathbf{Z}$, les groupes $\widehat{H}^q(G,A)$ et $H^q(K(A))$ sont isomorphes en raisonnant par exemple par décalage via le corollaire 2.7, après avoir écrit A comme sous-module (resp. comme quotient) d'un G-module induit I (resp I').

□

On trouvera plus de détails sur la cohomologie d'un groupe cyclique dans l'exercice 3 de ce chapitre.

2.4. Cup-produits

Soit G un groupe (pas forcément fini dans un premier temps). Soient A et B deux G-modules, alors on peut voir $A \otimes B := A \otimes_{\mathbf{Z}} B$ comme un G-module via la formule $g.(a \otimes b) = ga \otimes gb$ pour tout $g \in G$ et tout $(a, b) \in A \times B$. On en déduit une application bilinéaire au niveau des groupes de cochaînes homogènes (définies au paragraphe 1.4.) :

$$K^p(G, A) \times K^q(G, B) \stackrel{\cup}{\to} K^{p+q}(G, A \otimes B)$$

définie (pour tous entiers naturels p, q) par la formule :

$$(a \cup b)(g_0, ..., g_{p+q}) = a(g_0, ..., g_p) \otimes b(g_p, ...g_{p+q})$$

On a a alors

Theorème 2.11 *Si a et b sont des cocycles, alors $a \cup b$ est également un cocycle. Si l'une des deux cochaînes a ou b est un cobord et l'autre est un cocycle, alors $a \cup b$ est un cobord. L'application $\cup$ induit une application bilinéaire*

$$H^p(G, A) \times H^q(G, B) \to H^{p+q}(G, A \otimes B)$$

notée encore $\cup$, et appelée cup-produit.

Démonstration : Il suffit de vérifier la formule :

$$d(a \cup b) = (da) \cup b + (-1)^p (a \cup db) \tag{1}$$

où d est le cobord entre groupes de cochaînes. Or on a

$$d(a \cup b)(g_0, ...g_{p+q+1}) = \sum_{i=0}^{p} (-1)^i a(g_0, ..., \hat{g}_i, ..., g_{p+1}) \otimes b(g_{p+1}, ..., g_{p+q+1}) +$$

$$\sum_{i=p+1}^{p+q+1} (-1)^i a(g_0, ..., g_p) \otimes b(g_p, ..., \hat{g}_i, ..., g_{p+q+1})$$

et

$$(da \cup b)(g_0, ...g_{p+q+1}) = \sum_{i=0}^{p+1} (-1)^i a(g_0, ..., \hat{g}_i, ..., g_{p+1}) \otimes b(g_{p+1}, ..., g_{p+q+1})$$

ainsi que

$$(a \cup db)(g_0, ...g_{p+q+1}) = a(g_0, ..., g_p) \otimes \sum_{i=0}^{q+1} (-1)^i b(g_p, ..., \hat{g}_{p+i}, ..., g_{p+q+1}) =$$

$$a(g_0,...,g_p)\otimes\sum_{i=p}^{p+q+1}(-1)^{i-p}b(g_p,...,\hat{g}_i,...,g_{p+q+1})$$

On obtient alors la formule au terme près suivant

$$(-1)^{p+1}a(g_0,...,\hat{g}_{p+1},...,g_{p+1})\otimes b(g_{p+1},...,g_{p+q+1})+$$

$$(-1)^p a(g_0,...,g_p)\otimes b(g_p,...,\hat{g}_p,...,g_{p+q+1})$$

qui se simplifie, doù le résultat.

□

Notons que pour $p=q=0$, le cup-produit est simplement l'application $(a,b)\mapsto a\otimes b$ de $A^G\times B^G$ dans $(A\otimes B)^G$. Il est immédiat qu'il est fonctoriel en A et B. On peut alors plus généralement définir un cup-produit associé à une application bilinéaire $\varphi: A\times B\to C$ entre G-modules en utilisant le fait qu'une telle application se factorise à travers $A\otimes B$. On notera souvent encore $\cup$ le cup-produit ainsi obtenu si φ est sous-entendue. On a en outre les deux propriétés de compatibilité suivantes du cup-produit :

Proposition 2.12 *a) Soit $0\to A\to A'\to A''\to 0$ une suite exacte de G-modules. Soit B un G-module tel que la suite*

$$0\to A\otimes B\to A'\otimes B\to A''\otimes B\to 0$$

reste exacte (ex. B sans torsion). Alors pour tout $\alpha''\in H^p(G,A'')$ et tout $\beta\in H^q(G,B)$, on a

$$(\delta\alpha'')\cup\beta=\delta(\alpha''\cup\beta)\in H^{p+q+1}(G,A\otimes B)$$

où δ est le cobord entre groupes de cohomologie.

b) Soit $0\to B\to B'\to B''\to 0$ une suite exacte de G-modules. Soit A un G-module tel que la suite

$$0\to A\otimes B\to A\otimes B'\to A\otimes B''\to 0$$

reste exacte (ex. A sans torsion). Alors pour tout $\alpha\in H^p(G,A)$ et tout $\beta''\in H^q(G,B'')$, on a

$$\alpha\cup(\delta\beta'')=(-1)^p\delta(\alpha\cup\beta'')\in H^{p+q+1}(G,A\otimes B)$$

Noter que les propriétés de cette proposition jointes au fait que le cup-produit est "bifonctoriel" et à sa définition pour $p=q=0$ caractérisent uniquement le cup-produit (par décalage).

Démonstration : Montrons par exemple b). Relevons α en un cocycle $a \in Z^p(G, A)$ et β'' en un cocycle $b'' \in Z^q(G, B'')$. On peut relever b'' en une cochaîne homogène $b' \in K^q(G, B')$ (en effet $K^q(G, B') = X^q(G, B')^G$, où $X^q(G, B')$ est le G-module induit consitué des fonctions de G^{q+1} dans B', donc le foncteur $K^q(G, .)$ est exact). Identifions B avec son image dans B' et $A \otimes B$ avec son image dans $A \otimes B'$; alors $\delta(\beta'')$ est représenté par $db' \in Z^{q+1}(G, B)$ et $\delta(\alpha \cup \beta'')$ par $d(a \cup b') \in Z^{p+q+1}(G, A \otimes B)$. Comme $da = 0$, la formule (1) donne

$$d(a \cup b') = (-1)^p(a \cup db')$$

d'où le résultat en passant aux classes de cohomologie.

□

On obtient également par décalage :

Proposition 2.13 *a) Si on identifie $(A \otimes B) \otimes C$ à $A \otimes (B \otimes C)$, alors $(a \cup b) \cup c = a \cup (b \cup c)$.*

b) Si on identifie $A \otimes B$ et $B \otimes A$, on a $(a \cup b) = (-1)^{pq}(b \cup a)$ si $a \in H^p(G, A)$ et $b \in H^q(G, B)$.

c) Si H est un sous-groupe de G, A et B des G-modules et Res *la restriction, alors* $\mathrm{Res}(a \cup b) = \mathrm{Res}(a) \cup \mathrm{Res}(b)$.

d) Si H est un sous-groupe distingué de G, A et B des G/H-modules et Inf *l'inflation, alors* $\mathrm{Inf}(a \cup b) = \mathrm{Inf}(a) \cup \mathrm{Inf}(b)$.

e) Si H est un sous-groupe d'indice fini de G, A et B des G-modules et Cores *la corestriction, alors* $\mathrm{Cores}(a \cup \mathrm{Res}(b)) = \mathrm{Cores}(a) \cup b$.

Enfin, voici une dernière compatibilité qui sera utile pour les théorèmes de dualité :

Proposition 2.14 *Soient*

$$0 \to A' \to A \to A'' \to 0; \quad 0 \to B' \to B \to B'' \to 0$$

des suites exactes de G-modules. Soit C un G-module et $\varphi : A \times B \to C$ une application bilinéaire (compatible avec l'action de G) telle que $\varphi(A' \times B') = 0$, de sorte que φ induit des accouplements $\varphi' : A' \times B'' \to C$ et $\varphi'' : A'' \times B' \to C$. Alors les cup-produits induits

$$H^p(G, A'') \times H^q(G, B') \to H^{p+q}(G, C)$$

et

$$H^{p+1}(G, A') \times H^{q-1}(G, B'') \to H^{p+q}(G, C)$$

sont compatibles (au signe près) avec les cobords δ. Plus précisément on a

$$(\delta\alpha) \cup \beta + (-1)^p(\alpha \cup \delta\beta) = 0$$

pour tous $\alpha \in H^p(G, A'')$ et $\beta \in H^{q-1}(G, B'')$.

Démonstration : On relève α en un cocycle $a'' \in Z^p(G, A'')$ et de même β en $b'' \in Z^{q-1}(G, B'')$, puis a'' et b'' respectivement en des cochaînes a et b de $C^p(G, A)$ et $C^{q-1}(G, B)$. Alors da et db proviennent respectivement de $a' \in C^{p+1}(G, A')$ et $b' \in C^q(G, B')$, qui représentent respectivement $\delta\alpha$ et $\delta\beta$. On vérifie alors que

$$a' \cup b'' + (-1)^p(a'' \cup b') = d(a \cup b)$$

est un cobord, donc est nul dans $H^{p+q}(G, C)$.

□

Il est également possible (cf [12], Prop. 1.4.7.) de définir pour G fini le cup-produit $\widehat{H}^p(G, A) \times \widehat{H}^q(G, B) \otimes \widehat{H}^{p+q}(G, A \otimes B)$ pour tous $p, q \in \mathbf{Z}$, avec les mêmes propriétés. Pour $p = q = 0$, la définition est immédiate. Il faut faire un peu plus de calculs dans le cas où p ou q est négatif. Dans le cas où G est un groupe fini cyclique, on peut obtenir l'isomorphisme de $\widehat{H}^q(G, A)$ avec $\widehat{H}^{q+2}(G, A)$ en faisant le cup-produit avec la classe de $\widehat{H}^2(G, \mathbf{Z}) = \mathrm{Hom}(G, \mathbf{Q}/\mathbf{Z})$ obtenue en envoyant un générateur (qu'il faut choisir) s de G sur la classe de $1/m$ dans $\mathbf{Q}/\mathbf{Z}$, où m est l'ordre de G.

2.5. Exercices

1. Soit G un groupe fini. Pour tout G-module A, on note A^* le G-module $\mathrm{Hom}_{\mathbf{Z}}(A, \mathbf{Q}/\mathbf{Z})$, où l'action de G est donnée par $(g.f)(x) = f(g^{-1}.x)$ pour tout $g \in G$ et tout $x \in A$. En particulier si B est simplement un groupe abélien, le groupe abélien B^* est défini.

a) Montrer que pour tout groupe abélien B, l'homomorphisme canonique $B \to (B^*)^*$ (qui envoie x sur $f \mapsto f(x)$ pour $x \in B$ et $f \in B^*$)) est injectif.

b) Donner un exemple de groupe abélien B tel que $(B^*)^*$ ne soit pas isomorphe à B. Que se passe-t-il si B est fini ?

c) Montrer que si A est un G-module relativement injectif, alors A^* est encore relativement injectif.

d) Montrer que pour tout G-module A et pour tout entier $i \geq 0$, le groupe $H_i(G, A)^*$ est isomorphe à $H^i(G, A^*)$ (on commencera par le cas $i = 0$).

2. Étendre le lemme de Shapiro à la cohomologie modifiée $\widehat{H}^n$ pour tout $n \in \mathbf{Z}$.

3. Soit G un groupe fini cyclique. Soit A un G-module. Lorsque $\widehat{H}^0(G, A)$ et $\widehat{H}^1(G, A)$ sont des groupes finis, on note $h_0(A)$ et $h_1(A)$ leurs ordres respectifs et on appelle $h(A) := h_0(A)/h_1(A)$ le *quotient d'Herbrand* du G-module A.

a) Soit $0 \to A \to B \to C \to 0$ une suite exacte de G-modules. Montrer que si deux des quotients d'Herbrand $h(A)$, $h(B)$, $h(C)$ sont définis, alors il en va de même du troisième et on a $h(B) = h(A)h(C)$.

b) Montrer que si A est un G-module fini, alors $h(A) = 1$ (on regardera le noyau et le conoyau de la multiplication par $D = s - 1$ dans A, ainsi que le noyau et le conoyau de la norme de A_G dans A^G, où s est un générateur de G).

c) Soient A et B deux G-modules. Soit $f : A \to B$ un G-homomorphisme dont le noyau et le conoyau sont finis. Montrer que si l'un des deux quotients d'Herbrand $h(A)$, $h(B)$ est défini, l'autre l'est aussi et $h(A) = h(B)$.

4. Soit G un groupe fini. Soit p un nombre premier. Pour tout groupe abélien A, on note $A\{p\}$ sa *composante p-primaire*, i.e. le sous-groupe des $x \in A$ tels qu'il existe $m \in \mathbf{N}$ avec $p^m x = 0$. Le groupe A est dit p-primaire si $A = A\{p\}$.

a) Soit H un sous-groupe de G d'indice premier à p. Soit A un G-module. Montrer que pour tout $n \in \mathbf{Z}$, l'application

$$\text{Res} : \widehat{H}^n(G, A)\{p\} \to \widehat{H}^n(H, A)$$

est injective et l'application

$$\text{Cores} : \widehat{H}^n(H, A)\{p\} \to \widehat{H}^n(G, A)\{p\}$$

est surjective.

b) Soit G un p-groupe fini. On suppose que A est un G-module p-primaire. Montrer que si $H^0(G, A) = 0$ ou $H_0(G, A) = 0$, alors $A = 0$ (on se ramènera au cas où A est fini et on montrera qu'alors A et A^G ont même cardinal modulo p ; pour traiter le cas où $H_0(G, A) = 0$, on utilisera l'exercice 1. de ce chapitre).

3. Cohomologie d'un groupe profini

Quand on étudie la cohomologie galoisienne d'un corps k, on est souvent amené à travailler avec le groupe de Galois absolu $\Gamma_k := \text{Gal}\,(\bar{k}/k)$ (où $\bar{k}$ est une clôture séparable de k) et pas avec une extension finie. Nous allons voir que plus généralement on peut définir la cohomologie d'un groupe profini par un procédé de limite à partir de celle de certains de ses quotients finis (qui dans le cas de Γ_k correspondent aux groupes de Galois des extensions finies galoisiennes de k).

3.1. Notions de base sur les groupes profinis

Définition 3.1 *Un groupe topologique G est dit profini s'il est limite projective de groupes finis (munis chacun de la topologie discrète).*

Un groupe profini admet une base $\{G_i\}$ de voisinages du neutre constitué de sous-groupes ouverts[7] distingués d'indice fini, et G s'identifie alors à la limite projective des G/G_i. Un groupe topologique est profini si et seulement s'il est compact[8] et totalement discontinu ([12], proposition 1.1.3)[9]. Les groupes profinis forment une catégorie, les morphismes étant les morphismes *continus* de groupes.

Exemples de groupes profinis :

a) Les groupes finis sont profinis (!).

b) Le groupe de Galois absolu $\Gamma_k = \mathrm{Gal}\,(\bar{k}/k)$ d'un corps k est profini : c'est par définition la limite projective des $\mathrm{Gal}\,(L/k)$ quand L parcourt les extensions finies galoisiennes de k incluses dans $\bar{k}$.

c) Si M est un groupe abélien discret de torsion, son *dual de Pontryagin* $M^* := \mathrm{Hom}(M, \mathbf{Q}/\mathbf{Z})$ est un groupe profini quand on le munit de la topologie de la convergence simple (c'est-à-dire la topologie "compacte-ouverte") . En effet M est la limite inductive de ses sous-groupes finis N, donc M^* est la limite projective des groupes finis N^*. On peut montrer que $M \mapsto M^*$ induit une anti-équivalence de catégorie entre groupes discrets de torsion et groupes profinis, cas particulier de la dualité de Pontryagin pour les groupes abéliens localement compacts ; cf. [12], Th. 1.1.11. Noter que de même le dual d'un groupe abélien profini G est le groupe discret de torsion constitué des homomorphismes *continus* $\mathrm{Hom}_c(G, \mathbf{Q}/\mathbf{Z})$ de G dans $\mathbf{Q}/\mathbf{Z}$. Cette dualité ne marche pas bien pour un groupe discret qui n'est pas de torsion, par exemple pour $M = \mathbf{Z}$ on trouve $M^* = \mathbf{Q}/\mathbf{Z}$ et $M^{**} = \widehat{\mathbf{Z}}$, complété profini de $\mathbf{Z}$ (c'est la limite projective des $\mathbf{Z}/n\mathbf{Z}$).

d) Tout sous-groupe *fermé* d'un groupe profini est profini. De même tout quotient par un sous-groupe distingué fermé est profini.

e) Le groupe additif de l'anneau des entiers $\mathcal{O}_K$ d'un corps local (=corps complet pour une valuation discrète à corps résiduel fini) K (ex. : $\mathbf{Z}_p$) et son groupe multiplicatif $\mathcal{O}_K^*$ sont profinis.

7. Noter que pour un sous-groupe d'indice fini, fermé équivaut à ouvert ; rappelons aussi que tout sous-groupe ouvert d'un groupe topologique est fermé.

8. On demandera toujours la condition d'être séparé (au sens de Hausdorff) pour être compact.

9. En particulier la structure profinie de G ne dépend que de sa topologie, et pas du système projectif choisi pour définir G.

f) Le groupe $A(K)$ des points sur un corps local K d'une variété abélienne A (par exemple une courbe elliptique) est profini.

Dans les trois derniers exemples, c'est la caractérisation "compact+ totalement discontinu" qui permet le plus facilement de voir qu'on a affaire à des groupes profinis. Rappelons qu'une variété abélienne sur un corps est un groupe algébrique lisse, connexe et *projectif* sur ce corps, le cas de la dimension 1 correspondant aux courbes elliptiques.

Remarque : Attention dans un groupe profini G, les sous-groupes ouverts sont donc d'indice fini, mais la réciproque est en général fausse, même si G est abélien. Par exemple le groupe de Galois de l'extension abélienne maximale d'un corps de nombres a des sous-groupes d'indice fini qui ne sont pas ouverts. Un autre exemple est fourni par $\mathcal{O}_K^*$ quand K est le corps des séries de Laurent sur un corps fini ; voir [10], remarque en bas de la page 26.

Il se trouve que pour un groupe profini, on peut définir l'indice d'un sous-groupe même si ce sous-groupe n'est pas d'indice fini, via la notion de *nombre surnaturel*. Par définition, un tel nombre est un produit formel $\prod_p p^{n_p}$, où p parcourt l'ensemble des nombres premiers et $n_p \in \mathbf{N} \cup \{+\infty\}$. On définit de manière évidente le pgcd, le ppcm et le produit d'une famille quelconque de nombres surnaturels.

Définition 3.2 Soit G un groupe profini. Soit H un sous-groupe fermé de G. L'*indice* de H dans G (noté $[G : H]$) est le nombre surnaturel défini comme le ppcm des indices $[G/U : H/(H \cap U)]$ (qui sont des entiers naturels) quand U parcourt l'ensemble des sous-groupes ouverts distingués de G. L'*ordre* d'un groupe profini est le nombre surnaturel $[G : \{1\}]$.

Il n'est pas complètement évident [10] que "d'indice fini" au sens usuel soit la même chose que d'indice fini au sens de la définition précédente. Voici un lemme qui montre que c'est bien le cas.

Lemme 3.3 *Soit H un sous-groupe fermé d'un groupe profini G. Alors H est d'indice fini (au sens usuel) si et seulement si $[G : H]$ (défini comme dans la définition 3.2) est un entier naturel. De plus dans ce cas $[G : H]$ est l'indice de H au sens usuel.* [11] *En particulier H est ouvert si et seulement si le nombre surnaturel $[G : H]$ est un entier naturel.*

10. La plupart des auteurs semblent avoir totalement ignoré ce point...

11. Merci a Miaofen Chen pour avoir attiré mon attention sur le fait que ce point est aussi à vérifier.

Démonstration : Soit U un sous-groupe ouvert distingué de G. Soit p_U la surjection canonique $G \to G/U$. Alors $p_U(H) = (H/H \cap U)$. On a une surjection

$$\tilde{p}_U : G/H \to (G/U)/p_U(H)$$

de l'ensemble des classes à gauche de G selon H sur l'ensemble des classes à gauche de G/U selon $p_U(H)$. Si maintenant g_1 et g_2 sont deux éléments de G, on observe que $\tilde{p}_U(g_1H) = \tilde{p}_U(g_2H)$ si et seulement s'il existe $h \in H$ tel que $g_1 = g_2h$ modulo U (rappelons que U est distingué dans G), ou encore si et seulement si $(g_2^{-1}g_1U) \cap H \neq \emptyset$

On en déduit que toutes les fibres de la surjection $\tilde{p}_U$ ont le même cardinal car pour tout g de G, la fibre de $\tilde{p}_U(gH)$ est la double classe UgH. En particulier si l'ensemble G/H est fini de cardinal m, alors l'indice $[G : H]$ de la définition 3.2 est fini et divise m.

Pour conclure, il nous suffit de montrer que si n est un entier naturel tel que G/H contienne au moins n éléments distincts, alors il existe un sous-groupe ouvert U tel que $(G/U)/p_U(H)$ contienne au moins n éléments distincts (cela montrera à la fois que si G/H est infini, alors le nombre surnaturel $[G : H]$ n'est pas dans $\mathbf{N}$, et que si G/H est fini, alors ce nombre surnaturel est fini et au moins égal au cardinal de G/H). Soient donc $g_1, ..., g_n$ dans G telles que les classes $g_1H, ..., g_nH$ soient deux à deux distinctes. Alors aucun des $g_j^{-1}g_i$ pour i, j distincts n'est dans H. Comme le complémentaire de H dans G est ouvert et que les sous-groupes ouverts distingués forment une base de voisinages de 1, on peut trouver U ouvert distingué tel qu'aucun des $(g_j^{-1}g_i)U$ ne rencontre H, d'où on déduit que les images par $\tilde{p}_U$ de $g_1H, ..., g_nH$ sont deux à deux distinctes, d'où le résultat.

□

Définition 3.4 On dit que G est un *pro-p-groupe* si son ordre est une puissance de p (cela revient à dire que G est limite projective de p-groupes finis). Un *p-groupe de Sylow* (ou p-Sylow en abrégé) d'un groupe profini G est un sous-groupe fermé H de G qui est un pro-p-groupe et tel que l'indice $[G : H]$ soit premier à p.

La proposition ci-dessous (dont la preuve se déduit des résultats analogues pour les groupes finis [12], cf. [14], paragraphes I.1.3. et I.1.4.) résume les propriétés des indices et des sous-groupes de Sylow.

Proposition 3.5 *a) Soient $K \subset H \subset G$ des groupes profinis. Alors*

$$[G : K] = [G : H].[H : K]$$

12. Plus le fait classique qu'une limite projective d'ensembles finis non vides est non vide.

b) Soit G un groupe profini. Pour tout nombre premier p, le groupe G possède des p-Sylow, et ceux-ci sont conjugués.

c) Soit G un groupe profini. Alors tout pro-p-sous-groupe de G est contenu dans un p-Sylow.

Exemples : a) Le groupe $\mathbf{Z}_p$ est un pro-p-groupe. C'est le p-Sylow de $\widehat{\mathbf{Z}} := \varprojlim_{n\in\mathbf{N}^*} \mathbf{Z}/n = \prod_{p\in\mathcal{P}} \mathbf{Z}_p$, où $\mathcal{P}$ désigne l'ensemble des nombres premiers.

b) Soit G un groupe discret. Le *complété profini* $\widehat{G}$ de G est la limite projective des quotients finis de G. Le *p-complété* $\widehat{G}_p$ de G est la limite projective des quotients de G qui sont des p-groupes finis ; c'est le plus grand quotient de $\widehat{G}$ qui est un pro-p-groupe.

c) Soit K un corps p-adique (c'est-à-dire une extension finie de $\mathbf{Q}_p$) ; soit K_{nr} son extension maximale non ramifiée et K^{mr} l'extension maximale modérément ramifiée de K_{nr}. Soit $U = \mathrm{Gal}\,(\overline{K}/K_{\mathrm{nr}})$ le groupe d'inertie. La théorie des groupes de ramification (cf. [13], paragraphe IV.2) donne que $U_p := \mathrm{Gal}\,(\overline{K}/K^{\mathrm{mr}})$ est l'unique p-Sylow de U, et le quotient U/U_p est isomorphe au produit des $\mathbf{Z}_l$ pour $l \neq p$.

3.2. G-modules discrets

Dans toute la suite, G désignera un groupe profini. Soit A un groupe abélien discret muni d'une action de G. On dira que G opère *continûment* sur A si pour tout x de A, l'application $g \mapsto g.x$ est continue de G dans A, ou encore (A étant discret) [13] si le fixateur de tout élément de A est un sous-groupe ouvert de A.

Définition 3.6 Un G-module discret (ou plus simplement G-module si aucune confusion n'est possible) est un groupe abélien A muni d'une action de G telle que G opère continûment sur A.

On demande donc, en plus de la définition habituelle d'un G-module, que le fixateur de tout point soit ouvert. Bien entendu pour G fini ceci coïncide avec la notion habituelle de G-module. On notera C_G la catégorie des G-modules discrets (c'est une sous-catégorie abélienne pleine de $\mathcal{M}od_G$). Si A est un G-module discret, on a $A = \bigcup_U A^U$, où U parcourt l'ensemble des sous-groupes ouverts de G.

Exemples : Le cas qui va principalement nous intéresser est celui où $G = \Gamma_k = \mathrm{Gal}\,(\bar{k}/k)$ est le groupe de Galois absolu d'un corps k, ou encore

13. On pourrait considérer des groupes A munis d'une autre topologie, pour obtenir de la "cohomologie continue", mais dans ce cours on se limitera au cas A discret.

un quotient d'un tel groupe. Le théorème principal de la "théorie de Galois infinie" dit que l'application $\Gamma \mapsto L^\Gamma$ induit une correspondance bijective entre les sous-groupes *fermés* Γ de Γ_k et les extensions de corps L de k incluses dans $\bar{k}$. Les sous-groupes ouverts (=fermés d'indice fini) sont ceux qui correspondent aux extensions finies de k (ce qui n'empêche pas qu'il puisse exister des sous-groupes d'indice fini qui ne sont pas fermés ; ceux-ci ne correspondent à aucune extension de k).

a) On peut prendre l'action triviale $\gamma.x = x$ pour tous $\gamma \in \Gamma_k$, $x \in M$. On l'utilisera beaucoup pour $M = \mathbf{Z}$, $M = \mathbf{Z}/n\mathbf{Z}$.

b) Soit n un entier non divisible par la caractéristique de k. On obtient un Γ_k-module discret en prenant l'action du groupe de Galois sur le groupe multiplicatif $\bar{k}^*$, ou encore sur les racines n-ièmes de l'unité dans $\bar{k}$ (on notera ce dernier Γ_k-module μ_n).

c) Plus généralement, si S est un *groupe algébrique commutatif* sur k, on peut faire agir Γ_k sur l'ensemble $S(\bar{k})$ de ses $\bar{k}$-points. Si $\operatorname{Car} k = 0$, le cas d'un groupe fini sur k (au sens des schémas) correspond à $S(\bar{k})$ fini ; c'est le cas par exemple pour $\mathbf{Z}/n\mathbf{Z}$ et μ_n. L'action triviale correspond en plus au fait que tous les $\bar{k}$-points de S sont définis sur k. Le cas du module $\bar{k}^*$ correspond au *groupe multiplicatif* $\mathbf{G}_m$. On peut aussi prendre pour S une variété abélienne.

d) Supposons $\operatorname{Car} k = 0$. Si M est un Γ_k-module fini (correspondant à un k-groupe algébrique noté encore M par abus), on peut définir son *dual* M' via le groupe algébrique fini $\operatorname{Hom}(M, \mathbf{G}_m)$ ("dual de Cartier"). Cela signifie que le Γ-module M' est constitué des morphismes φ de M dans $\bar{k}^*$ (ou dans μ_n si M est de n-torsion), l'action de Γ sur M' étant donnée par $(\gamma.\varphi)(x) := \gamma(\varphi(\gamma^{-1}.x))$ pour $\gamma \in \Gamma$, $\varphi \in M'$, $x \in M$.[14] Par exemple $\mathbf{Z}/n\mathbf{Z}$ et μ_n sont des Γ-modules duaux l'un de l'autre.

3.3. Cohomologie d'un G-module discret

Il y a plusieurs façons de définir les groupes de cohomologie $H^n(G, A)$ quand G est un groupe profini et A un G-module discret. Comme C_G possède assez d'injectifs[15] (voir [16], lemme 6.11.10), on peut utiliser les foncteurs dérivés du foncteur $A \mapsto A^G$ de C_G dans A*b*. Toutefois, une petite difficulté pour les calculer est que contrairement à $\mathcal{M}od_G$, la catégorie C_G ne possède

14. Cette formule peut paraître compliquée, mais elle est nécessaire pour envoyer par exemple $M \otimes M'$ dans $\bar{k}^*$, voir plus loin.

15. Le point est que si A est un G-module discret, il se plonge dans un G-module I qui est injectif dans $\mathcal{M}od_G$; il est facile de voir qu'alors A se plonge aussi dans $\bigcup_U I^U$ (où U décrit les sous-groupes ouverts de G) et que ce dernier est injectif dans C_G.

en général pas suffisamment de projectifs. Comme le but est de se ramener à la cohomologie des groupes finis, il est plus simple d'adopter la définition par cochaînes :

Définition 3.7 Soit $A \in C_G$. Pour $q \geq 0$, on note $K^q(G, A)$ l'ensemble des applications *continues* (i.e. localement constantes) de G^q dans A. Soit $d : K^q(G, A) \to K^{q+1}(G, A)$ le cobord défini par la formule usuelle (cf. Theorème 1.17). On définit alors les groupes de cohomologie $H^q(G, A)$ comme les groupes de cohomologie du complexe $(K^q(G, A))$.

On a alors :

Proposition 3.8 *Soit (G_i) un système projectif de groupes profinis ; soit (A_i) un système inductif de G_i-modules discrets, les flèches de transition étant compatibles avec celles de (G_i). Soit $G = \varprojlim G_i$ et $A = \varinjlim A_i$. Alors pour tout $q \in \mathbf{N}$:*

$$H^q(G, A) = \varinjlim H^q(G_i, A_i)$$

Démonstration : Il suffit de vérifier que les homomorphismes canoniques

$$\varinjlim K^q(G_i, A_i) \to K^q(G, A)$$

sont des isomorphismes. L'injectivité résulte de ce que si φ est une fonction continue de G_i^q dans A_i qui induit une fonction nulle de G^q dans A, alors les valeurs de φ (qui sont en nombre fini par continuité) s'annulent toutes dans A_j pour un certain $j \geq i$; de ce fait, l'image de φ dans $K^q(G_j, A_j)$ est nulle, donc aussi son image dans la limite inductive.

Montrons la surjectivité. Soit f une fonction continue de G dans A, alors f est localement constante ; comme G est compact et possède une base de voisinages de 1 constituée de sous groupes ouverts distingués, la fonction f se factorise par un quotient fini G/U qui est un quotient G_j/U_j de l'un des G_j. En particulier l'application induite $\bar{f} : G/U \to A$ provient d'un homomorphisme $f_j : G_j/U_j \to A_i$ pour un certain i (par finitude de G_j/U_j). On peut supposer $i \geq j$ (quitte à augmenter i, vu qu'on travaille toujours avec des ensembles ordonnés filtrants d'indices), auquel cas on obtient que f provient de $f_i : G_i \to A_i$ obtenu en composant l'application de transition $G_i \to G_j$ avec $f_j : G_j/U_j \to A_i$. On conclut en appliquant cela à G^q pour tout $q \in \mathbf{N}^*$.

□

On en déduit immédiatement les corollaires suivants (dont le premier aurait pu être pris comme définition des groupes $H^q(G, A)$).

Corollaire 3.9 *Soit A un G-module discret. Alors*

$$H^q(G, A) = \varinjlim_U H^q(G/U, A^U)$$

où U parcourt l'ensemble des sous-groupes ouverts distingués de G.

On a en effet $G = \varprojlim_U (G/U)$ et $A = \varinjlim_U A^U$.

Corollaire 3.10 *Soit A un G-module discret. Alors*

$$H^q(G, A) = \varinjlim H^q(G, B)$$

où B parcourt l'ensemble des sous G-modules de type fini[16] *de A.*

Cela résulte de ce que A est la réunion (et donc la limite inductive) de tels B.

Corollaire 3.11 *Pour $q \geq 1$, les groupes $H^q(G, A)$ sont de torsion.*

Cela résulte du corollaire 3.9 et du corollaire 1.26.

Noter aussi que si A est injectif dans C_G, les A^U sont injectifs dans $C_{G/U}$ pour tout sous-groupe ouvert distingué U de G. On déduit alors facilement du corollaire 3.9 que les $H^q(G, A)$ s'obtiennent bien comme foncteurs dérivés de $A \mapsto A^G$ de C_G dans Ab.

Remarque : Il pourrait a priori y avoir une ambigüité dans la notation $H^q(G, A)$ quand G est un groupe profini, suivant qu'on considère A comme un G-module discret (en travaillant dans la catégorie C_G, ou encore avec des cochaînes continues) ou simplement comme un G-module (en travaillant dans la catégorie $\mathcal{M}od_G$, ou encore avec des cochaînes non nécessairement continues comme au chapitre 1). Sauf mention expresse du contraire, nous considérerons toujours qu'on travaille dans C_G, et donc que le groupe $H^q(G, A)$ est celui de la définition 3.7. Quand on parlera sans précision d'un G-module (pour un groupe profini G), on sous-entendera également que ce G-module est discret.

Les propriétés de la cohomologie d'un groupe profini G se déduisent immédiatement de celle d'un groupe fini via le corollaire 3.9. Il faut juste faire attention, pour les propriétés faisant intervenir un sous-groupe H de G, à se restreindre aux sous-groupes *fermés* de G, de manière à rester dans la catégorie des groupes profinis (pour les modules définis par des fonctions de G ou G^n dans un G-module A, il faut aussi prendre des fonctions *continues*). En particulier :

16. Noter que comme A est discret, un sous G-module de A est de type fini sur $\mathbf{Z}[G]$ si et seulement s'il est de type fini sur $\mathbf{Z}$.

1. Pour tous sous-groupe fermé H de G et tout G-module discret A, on dispose du G-module $I_G^H(A)$ (la définition est la même à condition de se restreindre à des fonctions continues de G dans A). En particulier tout G-module induit $I_G(A)$ est acyclique (ce qui permet les raisonnements habituels par décalage). [17]
2. Pour tout sous-groupe fermé H de G, les homomorphismes de restriction et d'inflation sont définis comme dans le paragraphe 1.5., et le lemme de Shapiro reste vrai. Il en va de même de la proposition 1.21 et de la suite spectrale de Hochschild-Serre (ainsi que ses conséquences) lorsque H est un sous-groupe distingué fermé de G.
3. Lorsque H est un sous-groupe fermé d'indice fini (i.e. un sous-groupe ouvert) de G, la corestriction $H^q(H, A) \to H^q(G, A)$ est bien définie. Le théorème 1.25 et le corollaire 1.28 restent valables dans ce contexte.
4. Si p et q sont deux entiers naturels, le cup-produit

$$H^p(G, A) \times H^q(G, B) \to H^{p+q}(G, A \otimes B)$$

est défini comme au paragraphe 2.4. (si ce n'est que dans la définition il faut prendre des cochaînes continues), et jouit des mêmes propriétés.

Nous verrons au chapitre suivant des exemples de calculs de groupes de cohomologie quand $G = \Gamma_k$ est le groupe de Galois absolu d'un corps.

On peut également avoir besoin parfois d'utiliser le groupe $\widehat{H}^0(G, A)$. Pour cela, considérons des sous-groupes ouverts distingués U et V de G avec $V \subset U$. On définit une flèche de *déflation* :

$$\text{Def} : \widehat{H}^0(G/V, A^V) \to \widehat{H}^0(G/U, A^U)$$

en passant au quotient l'identité, vu qu'on a

$$\widehat{H}^0(G/V, A^V) = A^G/N_{G/V}A^V, \quad \widehat{H}^0(G/U, A^U) = A^G/N_{G/U}A^U$$

et $N_{G/V}A^V \subset N_{G/U}A^U$ (regrouper les éléments de G/V en classes selon U/V).

Définition 3.12 Soit G un groupe profini. Soit A un G-module discret. On définit le groupe de cohomologie modifié $\widehat{H}^0(G, A)$ comme la limite *projective* des $\widehat{H}^0(G/U, A^U)$ pour U sous-groupe ouvert distingué de G, les flèches de transition étant les flèches de *déflation*.

17. Par contre il n'y a plus de bonne notion de module co-induit dans C_G car $\mathbf{Z}[G]$ n'est pas un G-module discret si G est infini.

Alors la restriction et la corestriction sont encore bien définies (sous les hypothèses habituelles) pour le $\widehat{H}^0$, avec la formule $\mathrm{Cor} \circ \mathrm{Res} = .[G : H]$ (on peut également définir les groupes $\widehat{H}^q(G, A)$ pour $q < 0$ par un procédé analogue de limite projective, cf. [12], def. 1.9.3., mais nous ne nous en servirons pas).

3.4. Dimension cohomologique

Rappelons qu'un groupe abélien de torsion A est dit *p-primaire* si tout élément de A est d'ordre une puissance de p. Tout groupe abélien de torsion A est somme directe (pour p premier) de ses *composantes p-primaires* $A\{p\}$, où $A\{p\}$ est le sous-groupe de A constitué des éléments d'ordre une puissance de p. Un G-module discret est *simple* s'il est non nul et n'admet pas de sous G-module autre que $\{0\}$ et lui-même.

La notion de p-dimension cohomologique d'un groupe profini est très importante. L'exercice 1 de ce chapitre montre qu'elle est surtout intéressante pour un groupe *infini* car la p-dimension cohomologique d'un groupe fini est soit nulle (si p ne divise pas son cardinal) soit infinie (dans le cas contraire).

Définition 3.13 Soit G un groupe profini. Pour tout nombre premier p, la *p-dimension cohomologique de* G (notée $\mathrm{cd}_p(G)$) est la borne inférieure (dans $\mathbf{N} \cup \{+\infty\}$) des entiers $n \in \mathbf{N}$ vérifiant :

Pour tout G-module discret *de torsion* A et tout $q > n$, la composante p-primaire de $H^q(G, A)$ est nulle (ce qui équivaut au fait que le sous-groupe de p-torsion $H^q(G, A)[p]$ soit nul).

La *dimension cohomologique de* G est $\mathrm{cd}(G) = \sup_p \mathrm{cd}_p(G)$.

Par exemple, le groupe fini $G = \mathbf{Z}/2 = \mathrm{Gal}\,(\mathbf{C}/\mathbf{R})$ est de p-dimension cohomologique 0 si $p \neq 2$ (via le corollaire 1.26), mais infinie si $p = 2$ vu le théorème 2.10 et le fait que $\widehat{H}^0(G, \mathbf{Z}/2) = \widehat{H}^1(G, \mathbf{Z}/2) = \mathbf{Z}/2$ par un calcul immédiat. Si p ne divise pas l'ordre de G, on a $\mathrm{cd}_p(G) = 0$ via les corollaires 3.9 et 1.26.

Theorème 3.14 *Soit G un groupe profini. Soit p un nombre premier et soit $n \in \mathbf{N}$. Les conditions suivantes sont équivalentes :*

1. $\mathrm{cd}_p(G) \leq n$.
2. *Pour tout $q > n$ et tout G-module discret A qui est un groupe abélien de torsion p-primaire, on a $H^q(G, A) = 0$.*
3. *On a $H^{n+1}(G, A) = 0$ pour tout G-module discret A qui est simple et de p-torsion.*

Noter au passage qu'un G module A simple et p-primaire est forcément de p-torsion vu que $A[p]$ est un sous G-module non trivial de A.

Démonstration : Écrivons A comme somme directe des $A\{p\}$. Alors pour $q \geq 1$ le groupe $H^q(G, A\{p\})$ est la composante p-primaire de $H^q(G, A)$ (via la proposition 3.8), d'où l'équivalence de 1. et 2. Il est immédiat que 2. implique 3. Supposons donc 3. Montrons d'abord par récurrence sur le cardinal de A que $H^{n+1}(G, A) = 0$ lorsque A est fini et p-primaire. C'est évident si $A = 0$, supposons donc $A \neq 0$. Si A est simple, alors $A[p]$ (qui est non nul vu que A est p-primaire) est égal à A et l'hypothèse 3. donne que $H^{n+1}(G, A) = 0$. Sinon on a une suite exacte de G-modules

$$0 \to A_1 \to A \to A_2 \to 0$$

avec A_1 et A_2 de cardinaux strictement plus petits que celui de A, d'où encore $H^{n+1}(G, A) = 0$ via la suite exacte longue et l'hypothèse de récurrence.

Maintenant on a encore $H^{n+1}(G, A) = 0$ (via le corollaire 3.10), pour tout G-module discret A qui est p-primaire car un sous G-module de type fini de A est alors fini (il est de type fini sur $\mathbf{Z}$ et de torsion). On montre alors 2. par récurrence sur q en plongeant A dans le module induit $I_G(A)$ (qui est bien p-primaire vu que toute fonction continue de G dans A est localement constante, donc ne prend qu'un nombre fini de valeurs par compacité de G), puis en appliquant l'hypothèse de récurrence au module de torsion p-primaire $I_G(A)/A$.

□

Le lemme suivant va souvent être utile :

Lemme 3.15 *Soit p un nombre premier. Soient G un p-groupe fini et A un G-module de torsion p-primaire. Alors si $A^G = 0$ on a $A = 0$.*

Démonstration : Supposons $A \neq 0$. On se ramène immédiatement à A fini en considérant le G-module engendré par un élément non nul de A, qui est fini car de type fini sur $\mathbf{Z}$ et de torsion. Alors l'équation aux classes donne que A et A^G ont même cardinal modulo p, et leurs cardinaux sont des puissances de p, donc A^G ne peut pas être de cardinal 1.

□

On déduit du théorème 3.14 l'important critère suivant pour majorer la p-dimension cohomologique d'un pro-p-groupe :

Theorème 3.16 *Soient G un pro-p-groupe et $n \in \mathbf{N}$. Alors $\mathrm{cd}_p(G) \leq n$ si et seulement si $H^{n+1}(G, \mathbf{Z}/p) = 0$.*

Démonstration : Si $\mathrm{cd}_p(G) \leq n$, alors $H^{n+1}(G, \mathbf{Z}/p) = 0$ par définition de la p-dimension cohomologique. Supposons donc $H^{n+1}(G, \mathbf{Z}/p) = 0$. D'après le théorème 3.14, on est ramené à montrer que si A est un G-module discret simple de p-torsion, alors $H^{n+1}(G, A) = 0$. Pour cela, on va en fait montrer qu'un tel A est forcément isomorphe à $\mathbf{Z}/p$.

On a déjà que A est fini : en effet le G-module M engendré par un élément a non nul de A est fini vu qu'il est de type fini sur $\mathbf{Z}$ et de torsion ; or $M = A$ par simplicité de A. On peut donc considérer A comme un G/U-module, avec U sous-groupe ouvert distingué de G. Quitte à appliquer le résultat à G/U et au G/U-module simple A, on est donc ramené au cas où G est un p-groupe fini. Comme $A \neq 0$, le lemme 3.15 dit alors que $A^G \neq 0$ et par simplicité de A, on obtient $A^G = A$, autrement dit l'action de G sur A est triviale. Maintenant on a forcément $A = \mathbf{Z}/p$, car le groupe abélien engendré par un élément non nul de A est un sous G-module de A, donc il est égal à A (par simplicié de A) et isomorphe à $\mathbf{Z}/p$ (car A est de p-torsion).

□

Exemple. Prenons $G = \mathbf{Z}_p = \varprojlim_n (\mathbf{Z}/p^n)$. On a $H^2(G, \mathbf{Z}/p) = 0$ via la proposition 3.8 : en effet d'après le théorème 2.10, on a $H^2(\mathbf{Z}/p^n, \mathbf{Z}/p) = \widehat{H}^0(\mathbf{Z}/p^n, \mathbf{Z}/p) = \mathbf{Z}/p$, où les applications de transition entre les différents groupes $H^2(\mathbf{Z}/p^n, \mathbf{Z}/p)$ correspondent [18] à la multiplication par p ; ainsi on a bien $\varinjlim_n H^2(\mathbf{Z}/p^n, \mathbf{Z}/p) = 0$. Le théorème 3.16 dit alors que $\mathrm{cd}_p(\mathbf{Z}_p) \leq 1$, et l'égalité vient de ce que

$$H^1(\mathbf{Z}_p, \mathbf{Z}/p) = \mathrm{Hom}_c(\mathbf{Z}_p, \mathbf{Z}/p) = \mathrm{Hom}_c(\mathbf{Z}_p/p\mathbf{Z}_p) = \mathbf{Z}/p \neq 0$$

Quand on travaille avec des G-modules qui ne sont plus forcément de torsion, on obtient la notion de dimension cohomologique stricte :

Définition 3.17 Soient G un groupe profini, p un nombre premier, et $n \in \mathbf{N}$. La *p-dimension cohomologique stricte* de G est la borne inférieure des $n \in \mathbf{N}$ tels que pour tout G-module discret A et tout entier $q > n$, on ait $H^q(G, A)\{p\} = 0$. On la note $\mathrm{scd}_p(G)$. La *dimension cohomologique stricte* de G est $\mathrm{scd}(G) = \sup_p \mathrm{scd}_p(G)$.

On va maintenant comparer cd_p et scd_p, ainsi que leur comportement par passage à un sous-groupe ou un quotient :

18. Une subtilité ici : si U et V sont des sous-groupes ouverts distingués d'un groupe profini G avec $V \subset U$, la flèche d'inflation $\widehat{H}^0(G/U, A^U) \to \widehat{H}^0(G/V, A^V)$ (qui permet de faire la limite inductive) est obtenue via l'application norme ; comparer avec la situation inverse quand on définit la flèche de déflation.

Proposition 3.18 *Soit G un groupe profini. Alors* $\mathrm{scd}_p(G) \leq \mathrm{cd}_p(G) + 1$ *pour tout nombre premier p. En particulier* $\mathrm{scd}(G) \leq \mathrm{cd}(G) + 1$.

Preuve de la proposition 3.18 : Soit M un G-module, posons $N = M[p]$ (le sous-module de p-torsion) et $Q = M/pM$. Notons n la p-dimension cohomologique de G. Soit $I = pM$. La multiplication par p induit deux suites exactes

$$0 \to N \to M \to I \to 0$$

$$0 \to I \to M \to Q \to 0$$

Soit alors $q > n + 1$. Comme N et Q sont de torsion p-primaire, on a $H^q(G, N) = H^{q-1}(G, Q) = 0$. Alors les applications $H^q(G, M) \to H^q(G, I)$ et $H^q(G, I) \to H^q(G, M)$ respectivement induites par les suites exactes ci-dessus sont injectives, donc aussi leur composée qui est la multiplication par p dans $H^q(G, M)$. Finalement $H^q(G, M)[p] = 0$ pour tout M, i.e. $\mathrm{scd}_p(G) \leq n + 1$.

□

Proposition 3.19 *Soit G un groupe profini et soit H un sous-groupe fermé de G. Alors pour tout nombre premier p, on a*

$$\mathrm{cd}_p(H) \leq \mathrm{cd}_p(G)\,; \quad \mathrm{scd}_p(H) \leq \mathrm{scd}_p(G)$$

Il y a égalité si l'indice $[G : H]$ est premier à p, ou encore si H est ouvert et $\mathrm{cd}_p(G) < +\infty$.

Bien entendu on a des résultats analogues pour $\mathrm{cd}(G)$ et $\mathrm{scd}(G)$. Par contre il n'y a pas d'inégalité analogue pour le quotient : par exemple le groupe $\mathbf{Z}_2$ est de 2-dimension cohomologique 1, mais il possède un quotient isomorphe à $\mathbf{Z}/2$, dont la 2-dimension cohomologique est infinie. Noter aussi que la dernière assertion de la proposition est en général fausse si $\mathrm{cd}_p(G)$ n'est pas supposée finie (prendre par exemple $G = \mathbf{Z}/2$, $H = 0$ et $p = 2$).

Démonstration : On commence par un lemme (utile en lui-même) :

Lemme 3.20 *Soient G un groupe profini et A un G-module discret. Soient p un nombre premier et H un sous-groupe fermé de G.*

a) Si p ne divise pas le nombre surnaturel $[G : H]$, l'application Res : $H^q(G, A)\{p\} \to H^q(H, A)$ *est injective pour tout $q > 0$.*

b) Si de plus H est ouvert et $n = \mathrm{cd}_p(G)$) (resp. $n = \mathrm{scd}_p(G)$)) est fini, alors Cor : $H^n(H, A)\{p\} \to H^n(G, A)\{p\}$ *est surjective pour tout G-module discret de torsion A (resp. pour tout G-module discret A).*

Démonstration : a) Si $[G : H]$ est fini cela vient de la formule $\mathrm{Cor} \circ \mathrm{Res} = .[G : H]$; le cas général s'y ramène via le corollaire 3.9 et la définition de l'indice d'un sous-groupe fermé.

b) Posons $I = I_G^H(A)$, on dispose d'un homomorphisme $\pi : I \to A$ défini par

$$f \mapsto \pi(f) := \sum_{g \in G/H} g.f(g^{-1})$$

Cet homomorphisme est surjectif car si $a \in A$, on définit un antécédent f de a par π en posant $f(h) = h.a$ pour $h \in H$ et $f(g) = 0$ si $g \notin H$. Si A est de torsion, I (et donc aussi le noyau B de π) est de torsion ; d'autre part l'homomorphisme induit

$$H^n(G, I) = H^n(H, A) \to H^n(G, A)$$

s'identifie à la corestriction (voir l'exercice 1. du chapitre 1. : cela résulte comme d'habitude de ce qu'on obtient deux foncteurs cohomologiques qui coïncident en degré 0). Comme pour B de torsion, on a $H^{n+1}(G, B)\{p\} = 0$ vu que $\mathrm{cd}_p(G) = n$, on conclut avec la longue suite exacte de cohomologie (noter qu'une suite exacte de groupes abéliens *de torsion* reste exacte quand on applique le foncteur $\{p\}$). Le raisonnement avec scd_p est identique.

□

On peut maintenant démontrer la proposition 3.19. Traitons le cas de cd_p (le raisonnement est le même pour scd_p). Soit $A \in C_H$, alors $I_G^H(A)$ (qui est p-primaire si A est p-primaire) est dans C_G et par le lemme de Shapiro $H^q(G, I_G^H(A)) = H^q(H, A)$, ce qui donne $\mathrm{cd}_p(H) \leq \mathrm{cd}_p(G)$. Si maintenant $[G : H]$ est premier à p, alors on a égalité via le lemme 3.20 a).

Supposons maintenant que H est ouvert et que $\mathrm{cd}_p(G) = n$ est finie. On peut alors trouver un G-module discret de torsion A tel que $H^n(G, A)\{p\} \neq 0$. Il suffit alors de montrer que $H^n(H, A)\{p\} \neq 0$, ce qui résulte du lemme 3.20 b).

□

Corollaire 3.21 *Soit G_p un p-Sylow de G. Alors* $\mathrm{cd}_p(G) = \mathrm{cd}_p(G_p) = \mathrm{cd}(G_p)$ *et* $\mathrm{scd}_p(G) = \mathrm{scd}_p(G_p) = \mathrm{scd}(G_p)$.

Exemples : a) D'après le corollaire précédent, $\mathrm{cd}_p(\widehat{\mathbf{Z}}) = \mathrm{cd}_p(\mathbf{Z}_p) = 1$. D'autre part $H^2(\mathbf{Z}_p, \mathbf{Z}) \neq 0$ (en effet $H^2(\mathbf{Z}_p, \mathbf{Z}) = \mathrm{Hom}_c(\mathbf{Z}_p, \mathbf{Q}/\mathbf{Z}) = \mathbf{Q}_p/\mathbf{Z}_p$), d'où on déduit que $\mathrm{scd}_p(\mathbf{Z}) = \mathrm{scd}_p(\mathbf{Z}_p) = 2$.

b) On verra plus tard dans le cours que si k est un corps p-adique et $G = \mathrm{Gal}\,(\bar{k}/k)$, alors $\mathrm{cd}(G) = \mathrm{scd}(G) = 2$.

Proposition 3.22 *Soit H un sous-groupe distingué fermé de G. Alors pour tout nombre premier p, on a*

$$\mathrm{cd}_p(G) \leq \mathrm{cd}_p(G/H) + \mathrm{cd}_p(H)$$

(et de même pour scd_p, $\mathrm{cd}(G)$ *etc.).*

Démonstration : On utilise la suite spectrale de Hochschild-Serre. Soit A un G-module discret de torsion p-primaire. Soit $n > \mathrm{cd}_p(G/H) + \mathrm{cd}_p(H)$. Alors si $i + j = n$, on a soit $i > \mathrm{cd}_p(G/H)$, soit $j > \mathrm{cd}_p(H)$; dans les deux cas le groupe $E_2^{ij} = H^i(G/H, H^j(H, A))$ est nul. Finalement $H^n(G, A)$ (qui admet une filtration dont les quotients successifs sont des sous-quotients des E_2^{ij} pour $i + j = n$) est nul.

□

On a enfin le critère général suivant (dû à Serre) :

Proposition 3.23 *Soit G un groupe profini de dimension cohomologique n. Alors G est de dimension cohomologique*[19] *stricte n si et seulement si : pour tout sous-groupe ouvert U de G, on a $H^{n+1}(U, \mathbf{Z}) = 0$*

Preuve de la proposition : La condition est clairement nécessaire. En sens inverse, si elle est vérifiée on a (par le lemme de Shapiro) $H^{n+1}(G, A) = 0$ pour tout G-module A qui est de la forme $A = I_G^U(\mathbf{Z}^r) = \mathbf{Z}[G/U]^r$ avec $r \geq 0$ et U sous-groupe ouvert distingué de G. Soit alors M un G-module discret de type fini. Alors il existe un sous-groupe ouvert distingué U de G qui opère trivialement sur M, d'où une suite exacte

$$0 \to B \to \mathbf{Z}[G/U]^r \to M \to 0$$

ce qui implique $H^{n+1}(G, M) = 0$ vu que $H^{n+2}(G, B) = 0$ d'après la proposition 3.18. Comme tout G-module discret A est réunion de G-modules discrets de type fini, on obtient $H^{n+1}(G, A) = 0$, d'où le résultat (toujours avec la proposition 3.18).

□

Le calcul de la dimension cohomologique du groupe de Galois absolu $\mathrm{Gal}\,(\bar{k}/k)$ d'un corps k est un problème en général difficile. On a déjà vu que pour $k = \mathbf{R}$, la p-dimension cohomologique est 0 si $p \neq 2$ et infinie si $p = 2$. Pour un corps fini, le groupe de Galois est isomorphe à $\widehat{\mathbf{Z}}$, dont la dimension

19. Bien entendu on a l'analogue avec la p-dimension cohomologique en se limitant à la torsion p-primaire de $H^{n+1}(U, \mathbf{Z})$ dans l'énoncé.

cohomologique est 1. On verra que pour une extension finie de $\mathbf{Q}_p$, cette dimension est 2, ainsi que pour une extension finie totalement imaginaire de $\mathbf{Q}$.

3.5. Exercices

1. Soient G un groupe profini et p un nombre premier.

a) Montrer que $\mathrm{cd}_p(G) = 0$ si et seulement si l'ordre de G (en tant que nombre surnaturel) est premier à p.

b) Montrer que si $\mathrm{cd}_p(G)$ n'est ni nul ni infini, alors l'exposant de p dans l'ordre de G est infini.

2. Soient G un groupe profini et p un nombre premier tel que $\mathrm{cd}_p(G) \leq n$ avec $n \in \mathbf{N}$.

a) Montrer que si A est un G-module discret *p-divisible* (i.e. la multiplication par p est surjective dans A), alors pour tout $q > n$ la composante p-primaire $H^q(G, A)\{p\}$ est nulle.

b) En déduire que si A est un G-module discret divisible et $\mathrm{cd}(G) \leq n$, alors $H^q(G, A) = 0$ pour tout $q > n$.

3. Soit G le groupe profini $\widehat{\mathbf{Z}} = \varprojlim_{n \in \mathbf{N}^*} \mathbf{Z}/n$.

a) Soit A un G-module discret. On note F l'automorphisme de A induit par le générateur topologique canonique s de G (correspondant à $1 \in \widehat{\mathbf{Z}}$) et A' le sous groupe de A constitué des a tels qu'il existe $n \in \mathbf{N}^*$ avec

$$(1 + F + ... + F^{n-1})a = 0$$

. Montrer que $(F - 1)A$ est un sous-groupe de A' et qu'on a $H^1(G, A) = A'/(F - 1)A$.

b) Calculer le dual $\mathrm{Hom}_c(G, \mathbf{Q}/\mathbf{Z})$ de G.

c) Montrer que si A est fini, alors $H^2(G, A) = 0$ et retrouver le fait que $\mathrm{cd}(\widehat{\mathbf{Z}}) = 1$ (comparer avec l'exercice 3).

4. Reprendre l'exercice 2. du chapitre 1 en supposant cette fois que G est un groupe profini et H un sous-groupe ouvert de G.

5. Soit G un groupe profini de dimension cohomologique finie. Montrer que G est sans torsion (c'est-à-dire que tout élément de G autre que le neutre est d'ordre infini).

6. Soit G un groupe profini. Soit $(A_n)_{n\in\mathbf{N}}$ un système projectif de G-modules finis.

a) Montrer que si G est fini, on a

$$H^q(G, \varprojlim_n A_n) = \varprojlim_n H^q(G, A_n)$$

pour tout $q \in \mathbf{N}$ (on pourra procéder par décalage).

b) On prend $G = \mathbf{Z}_p$ et $A_n = \mathbf{Z}/p^n\mathbf{Z}$ (muni de l'action triviale de G). Montrer que l'égalité de a) ne vaut plus (On comparera avec l'exercice 3 du chapitre 1, et aussi avec la proposition 3.8).

7. Soit G un groupe abélien profini. On suppose que pour tout entier $n > 0$, le groupe G/nG est fini.

a) Montrer que nG est un sous-groupe ouvert de G.

b) Soit U un sous-groupe ouvert de G. Montrer que nU est un sous-groupe ouvert de G (on pourra comparer G/U et nG/nU).

c) En déduire que si A est un G-module discret fini, alors $H^1(G, A)$ est fini.

8. Soient n un entier > 0 et p un nombre premier. Soit G un groupe profini avec $\mathrm{cd}_p(G) = n$. Montrer que $\mathrm{scd}_p(G) = n + 1$ si et seulement s'il existe un sous-groupe ouvert H de G tel que $H^n(H, \mathbf{Q}_p/\mathbf{Z}_p) \neq 0$.

4. Premières notions de cohomologie galoisienne

Dans tout ce chapitre on désigne par k un corps de clôture séparable $\bar{k}$ et on note Γ_k le groupe profini $\Gamma_k := \mathrm{Gal}\,(\bar{k}/k)$.

4.1. Généralités

Soit M un Γ_k-module discret. Les groupes de cohomologie $H^q(\Gamma_k, M)$ pour $q \geq 0$ (ainsi que $\widehat{H}^0(\Gamma_k, M)$) ont été définis au chapitre précédent. Si maintenant k_1 est une extension de corps de k de clôture algébrique $\bar{k}_1$ et $j : \bar{k} \to \bar{k}_1$ est un morphisme de corps prolongeant l'inclusion $i : k \to k_1$, alors j définit un homomorphisme continu $f : \Gamma_{k_1} \to \Gamma_k$; on obtient donc (cf. début du paragraphe 1.5.) des homomorphismes

$$H^q(\Gamma_k, M) \to H^q(\Gamma_{k_1}, M)$$

Si on change j, on change f par un automorphisme intérieur de Γ_k, ce qui fait que ces homomorphismes sont en fait indépendants du choix de j d'après la proposition 1.21. En particulier deux clôtures séparables de k définissent des $H^q(\Gamma_k, M)$ canoniquement isomorphes, ce qui permet de noter $H^q(k, M)$ au lieu de $H^q(\Gamma_k, M)$. Pour toute extension de corps k_1 de k, on a alors des homomorphismes canoniques $H^q(k, M) \to H^q(k_1, M)$. [20]

Le groupe additif $\bar{k}$ est un Γ_k-module pour l'action naturelle de Γ_k. La proposition suivante et son corollaire montrent que sa cohomologie est triviale.

Proposition 4.1 *Soit L une extension finie galoisienne de k. Alors*

$$\widehat{H}^q(\mathrm{Gal}\,(L/k), L) = 0$$

pour tout $q \in \mathbf{Z}$.

Corollaire 4.2 *On a $H^q(k, \bar{k}) = 0$ pour tout $q > 0$.*

Démonstration : Le corollaire se déduit de la proposition via le corollaire 3.9. La proposition résulte de ce que d'après le théorème de la base normale (cf. [1], paragraphe 10), le $\mathrm{Gal}\,(L/k)$-module L est co-induit (isomorphe à $\mathbf{Z}[\mathrm{Gal}\,(L/k)] \otimes_{\mathbf{Z}} k$), donc induit puisque $\mathrm{Gal}\,(L/k)$ est fini.

□

Proposition 4.3 (Artin-Schreier) *Soit k un corps de caractéristique p. Soit Φ l'application de $\bar{k}$ dans $\bar{k}$ définie par $\Phi(x) = x^p - x$. Alors $H^1(k, \mathbf{Z}/p) = k/\Phi(k)$ et $H^q(k, \mathbf{Z}/p) = 0$ pour $q \geq 2$.*

Démonstration : Comme $\bar{k}$ est de caractéristique p, l'application Φ est un morphisme de Γ_k-modules. Il est surjectif car $\bar{k}$ est séparablement clos et pour tout $a \in \bar{k}$, le polynôme $X^p - X - a$ est séparable (sa dérivée est -1). Le noyau de Φ est le sous-corps premier de $\bar{k}$, il est donc isomorphe au Γ_k-module $\mathbf{Z}/p$ (avec action triviale de Γ_k) et on a une suite exacte de Γ_k-modules :

$$0 \to \mathbf{Z}/p \to \bar{k} \xrightarrow{\Phi} \bar{k} \to 0$$

On conclut avec le corollaire 4.2 et la suite exacte longue de cohomologie.

□

20. Plus généralement, si A est un schéma en groupes commutatif sur k, ce procédé fournit des homomorphismes canoniques $H^q(k, A(\bar{k})) \to H^q(k_1, A(\bar{k}_1))$.

4.2. Théorème de Hilbert 90 et applications

On considère ici l'action naturelle du groupe de Galois Γ_k sur le groupe abélien $\bar{k}^*$, qui fait de $\bar{k}^*$ un Γ_k-module discret.

Theorème 4.4 (Hilbert 90) *Soit L une extension finie galoisienne de k. Soit G le groupe de Galois $G = \mathrm{Gal}\,(L/k)$. Alors*

$$H^1(G, L^*) = 0$$

et

$$H^1(k, \bar{k}^*) = 0$$

Démonstration : La seconde assertion se déduit de la première via le corollaire 3.9. Soit $s \mapsto a_s$ un cocycle dans $Z^1(G, L^*)$. D'après le théorème d'indépendance linéaire des morphismes de Dedekind ([1], paragraphe 7, no 5), on peut trouver un élément c de L^* tel que l'élément

$$b := \sum_{t \in G} a_t t(c)$$

soit non nul. On a alors, pour tout s de G :

$$s(b) = \sum_{t \in G} s(a_t).(st)(c) = \sum_{t \in G} a_s^{-1} a_{st}.(st)(c) = a_s^{-1} b$$

d'où $a_s = s(b^{-1})/b^{-1}$, ce qui montre que $s \mapsto a_s$ est un cobord.

□

Corollaire 4.5 *Soit n un entier inversible dans k. Alors*

$$H^1(k, \mu_n) = k^*/{k^*}^n$$

Démonstration : Ceci résulte de la suite exacte longue de cohomologie associée à

$$1 \to \mu_n \to \bar{k}^* \xrightarrow{.n} \bar{k}^* \to 1$$

et du théorème de Hilbert 90.

□

Contrairement au Γ_k-module k, on va voir dans le prochain paragraphe que $\bar{k}^*$ n'a pas toujours une cohomologie triviale.

4.3. Groupe de Brauer d'un corps, corps de dimension cohomologique ≤ 1

Définition 4.6 Soit k un corps de groupe de Galois absolu $\Gamma_k = \mathrm{Gal}\,(\bar{k}/k)$. Le *groupe de Brauer* de k est le groupe de cohomologie $H^2(\Gamma_k, \bar{k}^*)$. On le note $\mathrm{Br}\,k$.

Ainsi $\mathrm{Br}\,k$ est la limite inductive (pour L/k finie galoisienne) des groupes $\mathrm{Br}\,(L/k) := H^2(\mathrm{Gal}\,(L/k), L^*)$. Notons aussi que si K est une extension de k, on a un homomorphisme $\mathrm{Br}\,k \to \mathrm{Br}\,K$ induit par le morphisme [21] naturel $\Gamma_K \to \Gamma_k$ et l'inclusion $\bar{k}^* \to \overline{K}^*$.

Proposition 4.7 *Soit L une extension finie galoisienne de k. Alors*

$$\mathrm{Br}\,(L/k) = \ker[\mathrm{Br}\,k \to \mathrm{Br}\,L]$$

Ainsi $\mathrm{Br}\,k$ est la réunion des $\mathrm{Br}\,(L/k)$ pour L/k finie galoisienne.

Démonstration : Ceci résulte du théorème 4.4 (Hilbert 90) et du corollaire 1.24, dans sa version où le groupe G est profini et H est un sous-groupe fermé de G : on prend $q = 2$, $G = \Gamma_k$ et $H = \Gamma_L = \mathrm{Gal}\,(\bar{k}/L)$, ainsi que $A = \bar{k}^*$.

□

Remarques : 1. La proposition précédente s'étend immédiatement au cas où L est une extension galoisienne (non nécessairement finie) de k.

2. Il existe une autre définition du groupe de Brauer, basée sur les algèbres centrales simples, voir par exemple [13], chapitre X, paragraphe 5.

Proposition 4.8 *Soit n un entier inversible dans k. Alors*

$$H^2(k, \mu_n) = (\mathrm{Br}\,k)[n]$$

En particulier si on a de plus $\mu_n \subset k$, alors $H^2(k, \mathbf{Z}/n) = (\mathrm{Br}\,k)[n]$

Démonstration : Ceci résulte de la suite exacte longue de cohomologie associée à la suite exacte

$$1 \to \mu_n \to \bar{k}^* \xrightarrow{.n} \bar{k}^* \to 1$$

compte tenu de ce que $H^1(k, \bar{k}^*) = 0$ (Hilbert 90).

□

21. Ce morphisme n'est bien défini qu'à conjugaison près, mais le même raisonnement qu'au paragraphe 4.1. montre que l'homomorphisme $\mathrm{Br}\,k \to \mathrm{Br}\,K$ est bien défini.

Exemples. 1. Par définition, un corps séparablement clos a un groupe de Brauer nul. Comme on le verra un peu plus loin, il en va de même d'un corps fini.

2. Le groupe de Brauer du corps $\mathbf{R}$ est $\mathbf{Z}/2$ car $H^2(\Gamma_{\mathbf{R}}, \mathbf{C}^*)$ est isomorphe à $\widehat{H}^0(\Gamma_{\mathbf{R}}, \mathbf{C}^*) = \mathbf{R}^*/\mathbf{R}_+^*$ via le théorème 2.10 vu que $\Gamma_{\mathbf{R}}$ est cyclique.

3. On verra au prochain chapitre que le groupe de Brauer d'un corps p-adique est $\mathbf{Q}/\mathbf{Z}$.

Définition 4.9 Soient k un corps et p un nombre premier. La p-dimension cohomologique (resp. la dimension cohomologique) de k est par définition celle du groupe de Galois absolu Γ_k. On la note $\mathrm{cd}_p(k)$ (resp. $\mathrm{cd}(k)$).

Bien entendu on a aussi une définition analogue pour la dimension cohomologique stricte.

Le cas où k est de dimension cohomologique ≤ 1 est particulièrement important. [22]

Proposition 4.10 *Soit k un corps de caractéristique $p > 0$. Alors on a $\mathrm{cd}_p(k) \leq 1$.*

Démonstration : Soit G_p un p-Sylow de Γ_k. Par la théorie de Galois, on a $G_p = \mathrm{Gal}\,(\bar{k}/K)$, où K est une extension de k incluse dans $\bar{k}$. Le corollaire 3.21 dit que $\mathrm{cd}_p(\Gamma_k) = \mathrm{cd}_p(G_p)$. D'après le théorème 3.16, il suffit donc de montrer que $H^2(K, \mathbf{Z}/p) = 0$. Mais ceci résulte de la proposition 4.3 vu que K est de caractéristique p.

□

Il est remarquable que les corps de p-dimension cohomologique au plus 1 puissent être caractérisés en utilisant le groupe de Brauer :

Theorème 4.11 *Soit k un corps et soit p un nombre premier différent de la caractéristique de k. Alors les trois propriétés suivantes sont équivalentes :*

1. *On a $\mathrm{cd}_p(k) \leq 1$.*
2. *Pour toute extension algébrique séparable K de k, on a $(\mathrm{Br}\,K)\{p\} = 0$.*

22. Nous adoptons ici pour ces corps la définition de [6] ; celle de [14] est légèrement différente dans le cas d'un corps de caractéristique p imparfait, en ce qu'elle requiert de plus que la condition 2. du théorème 4.11 ci-dessous soit satisfaite. Plus généralement, la notion de p-dimension cohomologique donnée ici n'est pas "la bonne" pour un corps imparfait de caractéristique p.

3. *Pour toute extension algébrique séparable K de k et toute extension finie galoisienne L/K telle que* $\mathrm{Gal}\,(L/K) \simeq \mathbf{Z}/p$, *la norme* $N_{L/K} : L^* \to K^*$ *est surjective.*

Ces assertions sont également équivalentes aux assertions 2bis et 3bis, obtenues respectivement à partir de 2. et 3. en remplaçant "Pour toute extension algébrique séparable K de k..." par "Pour toute extension algébrique finie séparable K de k..."

Noter que la norme (au sens usuel des extensions de corps) correspond bien à la norme au sens de l'action du groupe $\mathrm{Gal}\,(L/K)$ sur le groupe multiplicatif L^*.

On déduit du théorème 4.11 le critère suivant pour caractériser les corps k tels que $\mathrm{cd}(k) \leq 1$; il montre notamment que pour un corps parfait, la notion de corps de dimension cohomologique ≤ 1 définie dans [14] est la même que celle de [6] (que nous avons adoptée dans ce cours).

Theorème 4.12 *Soit k un corps parfait (par exemple de caractéristique zéro). Alors les trois propriétés suivantes sont équivalentes :*

1. *On a* $\mathrm{cd}(k) \leq 1$.
2. *Pour toute extension algébrique (resp. finie) K de k, on a* $\mathrm{Br}\,K = 0$.
3. *Pour toute extension algébrique (resp. finie) K de k et toute extension cyclique L/K de degré premier, la norme $N_{L/K} : L^* \to K^*$ est surjective.*

De plus 2. et 3. (en supposant de plus dans ces assertions que K/k est séparable) impliquent 1. même si k n'est pas supposé parfait.

Démonstration : (à partir du théorème 4.11) Si k est de caractéristique zéro c'est un corollaire immédiat vu que $\mathrm{cd}(k)$ est le sup des $\mathrm{cd}_p(k)$ pour p premier. Si k est de caractéristique $p > 0$, on a automatiquement $\mathrm{cd}_p(k) \leq 1$ d'après la proposition 4.10, et il s'agit donc juste de vérifier en plus :

-dans 2. que si k est parfait, on a $(\mathrm{Br}\,K)[p] = 0$ quand K est une extension algébrique de k. Ceci résulte de ce que $x \mapsto x^p$ est un morphisme bijectif du Γ_K-module $\overline{K}^*$ sur lui-même (parce que K est parfait).

-Dans 3. que si L/K est cyclique de degré p, la norme $N_{L/K} : L^* \to K^*$ est surjective. Or on a

$$\widehat{H}^0(\mathrm{Gal}\,(L/K), L^*) = H^2(\mathrm{Gal}\,(L/K), L^*) \subset \mathrm{Br}\,(L/K)[p] = 0$$

donc 3. est bien vérifiée aussi dans ce cas.

□

Remarques : 1. Si k est imparfait de caractéristique $p > 0$, on a toujours $\mathrm{cd}_p(\Gamma_k) \leq 1$ mais la condition $(\mathrm{Br}\, K)[p] = 0$ (imposée dans [14] pour avoir $\mathrm{cd}_p(k) \leq 1$) ne vaut pas toujours pour les extensions finies séparables K de k (voir l'exercice 2 du chapitre 5).

2. La condition $\mathrm{Br}\, k = 0$ ne suffit pas à assurer $\mathrm{cd}(k) \leq 1$, voir l'exercice 1 du chapitre 5.

3. Si $\mathrm{cd}(k) \leq 1$ et k est parfait, la propriété 3. du théorème 4.12 vaut pour toute extension finie galoisienne L de K. C'est clair par dévissage si $\mathrm{Gal}\,(L/K)$ est résoluble ; dans le cas général il faut utiliser le fait (un peu plus compliqué à démontrer) que le $\mathrm{Gal}\,(L/K)$-module L^* est *cohomologiquement trivial*, voir paragraphe 6.1. En pratique c'est plutôt l'implication 3. $\Rightarrow$ 1. qui est utile dans le théorème 4.12.

Preuve du théorème 4.11 : Commençons par un lemme.

Lemme 4.13 *L'assertion 2. (resp. 3) est équivalente à 2bis (resp. 3bis).*

Démonstration : Supposons 2bis ; soit K une extension algébrique séparable de k, qu'on peut supposer incluse dans $\bar{k}$. Alors $\Gamma_K = \mathrm{Gal}\,(\bar{k}/K)$ est la limite projective (ici l'intersection) des $\mathrm{Gal}\,(\bar{k}/L)$ pour L extension finie galoisienne de k incluse dans K. D'après la proposition 3.8, le groupe $\mathrm{Br}\, K$ est la limite inductive des $\mathrm{Br}\, L$ pour de telles L, et on a donc $(\mathrm{Br}\, K)\{p\} = 0$ via 2bis. Ainsi 2. est bien vérifiée.

Supposons 3bis. Soit K une extension algébrique séparable de k incluse dans $\bar{k}$. Soit K_1 une extension cyclique de K de groupe $\mathbf{Z}/p$, on peut écrire (d'après le théorème de l'élément primitif) $K_1 = K(\alpha)$, avec $\alpha \in \bar{k}$. On peut alors trouver une extension finie F de k incluse dans K qui contient les coefficients du polynôme minimal de α sur k, et tels que tous les conjugués de α sur k soient dans $F[\alpha]$. Alors $F(\alpha)$ est une extension cyclique de degré p de F, linéairement disjointe de K au-dessus de F puisque $F(\alpha) \otimes_F K = K(\alpha)$ est un corps. Soit alors x dans K^*. Alors $L := F(x, \alpha)$ est une extension cyclique de degré p de $F(x)$ (qui est finie séparable sur k) donc d'après 3bis il existe y dans L^* tel que $N_{L/F(x)}(y) = x$. Alors $y \in K_1^*$ et $N_{K_1/K}(y) = x$ comme on voulait.

□

Reprenons la preuve du théorème 4.11. Supposons 1. Soit $\bar{k}$ une clôture séparable de k contenant K. Comme $\mathrm{Gal}\,(\bar{k}/K)$ est un sous-groupe fermé de Γ_k, on a $\mathrm{cd}_p(K) \leq \mathrm{cd}_p(k)$ par la proposition 3.19. Ainsi $\mathrm{cd}_p(K) \leq 1$, d'où $H^2(K, \mu_p) = 0$ et donc $(\mathrm{Br}\, K)[p] = 0$ par la proposition 4.8 (noter ici l'importance de la condition $p \neq \mathrm{Car}\, k$), ce qui donne 2.

Supposons 2. et soient K et L comme dans 3. Alors

$$\mathrm{Br}\,(L/K) = K^*/N_{L/K}L^*$$

par le théorème 2.10. D'autre part $\mathrm{Br}\,(L/K)$ est annulé par p d'après le corollaire 1.26. L'hypothèse 2. implique alors que $\mathrm{Br}\,(L/K) \subset (\mathrm{Br}\,K)[p] = 0$, d'où $K^* = N_{L/K}L^*$.

La partie difficile consiste à montrer 1. quand on suppose que 3. est vérifiée. Soit G_p un p-Sylow de Γ_k, il suffit de montrer que $H^2(G_p, \mathbf{Z}/p) = 0$ grâce au théorème 3.16 et au corollaire 3.21. Comme une racine primitive p-ième de l'unité ζ_p annule le polynôme $1 + X + ... + X^{p-1}$, le degré de l'extension $k(\zeta_p)/k$ est au plus $p-1$, ce qui fait que le corps fixe k_p de G_p contient les racines p-ièmes de l'unité. Ainsi

$$H^2(G_p, \mathbf{Z}/p) \simeq H^2(k_p, \mu_p) \simeq (\mathrm{Br}\,k_p)[p]$$

Tout revient donc à montrer que si K_p est une extension finie galoisienne de k_p de groupe $P := \mathrm{Gal}\,(K_p/k_p)$ (incluse dans $\bar{k}$), on a $\mathrm{Br}\,(K_p/k_p)[p] = 0$.

Comme P est un p-groupe fini, il est résoluble et par la théorie de Galois on peut trouver une tour

$$k_p = K_0 \subset K_1 \subset ... \subset K_n = K_p$$

de corps tels que chaque extension K_{i+1}/K_i soit cyclique de degré p. Montrons alors par récurrence sur i que $\mathrm{Br}\,(K_i/k_p)[p] = 0$. C'est clair pour $i = 0$. Supposons le résultat vrai pour $i-1$. Alors comme $H^1(\mathrm{Gal}\,(K_i/K_{i-1}), K_i^*) = 0$ par Hilbert 90, le corollaire 1.24 donne une suite exacte

$$0 \to \mathrm{Br}\,(K_{i-1}/k_p) \to \mathrm{Br}\,(K_i/k_p) \to \mathrm{Br}\,(K_i/K_{i-1})$$

Maintenant $\mathrm{Br}\,(K_{i-1}/k_p)[p] = 0$ par hypothèse de récurrence et on a d'autre part $\mathrm{Br}\,(K_i/K_{i-1}) = H^2(\mathrm{Gal}\,(K_i/K_{i-1}), K_i^*) = 0$ via 3. et le théorème 2.10 vu que K_i/K_{i-1} est cyclique de degré p. Finalement $\mathrm{Br}\,(K_i/k_p)[p] = 0$ ce qui conclut la preuve.

□

4.4. Corps C_1

Les exemples les plus fréquents de corps de dimension cohomologique 1 sont les corps C_1, qui sont définis par la propriété très concrète suivante.

Définition 4.14 *On dit qu'un corps k est C_1 si tout polynôme homogène $f \in k[X_1, ...X_n]$ de degré $d < n$ possède au moins un zéro non trivial.*

Exemples. 1. Un corps fini est C_1 (théorème de Chevalley, [6], Th. 6.2.6.).

2. Si k est un corps algébriquement clos, alors $k(t)$ est C_1, ainsi plus généralement que toute extension de k de degré de transcendance 1 (théorème de Tsen, [6], Th. 6.2.8.). Il en va de même de $k((t))$ (résultat dû à Lang, [6], Th. 6.2.1.)

3. Lang ([7]) a également démontré que l'extension maximale non ramifiée d'un corps p-adique[23] est C_1.

Lemme 4.15 *Soit k un corps C_1 et soit k_1 une extension algébrique de k. Alors k_1 est C_1.*

Démonstration : Soit F un polynôme homogène de degré d en n variables à coefficients dans k_1, avec $d < n$, dont on veut montrer qu'il a un zéro non trivial. Comme les coefficients de F sont algébriques sur k, il existe une extension finie de k qui les contient et on peut donc supposer que k_1 est une extension finie de k, dont on note m le degré. Posons alors $f(x) = N_{k_1/k}(F(x))$, alors f est un polynôme homogène de degré dm en nm variables à coefficients dans k (prendre une base $(e_1, ..., e_m)$ de k_1 sur k, et décomposer $x \in k_1^n$ sur cette base). Comme k est C_1, le polynôme f a un zéro non trivial, d'où un $x \in k_1^n$ tel que $f(x) = 0$, ce qui implique $F(x) = 0$.

□

Theorème 4.16 *Soit k un corps C_1. Alors* $\mathrm{cd}(k) \leq 1$.

(La réciproque est fausse : Ax a construit un corps de dimension cohomologique 1 qui n'est pas C_1, cf. [14], exercice p.90).

Démonstration : Soit K une extension algébrique de k. Soit L une extension finie de degré d de K. Soit $a \in K^*$. Soit N l'application norme de L dans K. Comme K est C_1 d'après le lemme précédent, l'équation

$$N(x) = ax_0^d$$

pour $x \in L$, $x_0 \in K$, possède une solution non triviale (x, x_0) car c'est une équation polynomiale de degré d en $d+1$ variables sur K. On a $x_0 \neq 0$ (sinon $N(x) = 0$ d'où $x = 0$), ce qui fait que $N(x/x_0) = a$. Finalement la norme $N_{L/K} : L^* \to K^*$ est surjective, et $\mathrm{cd}(k) \leq 1$ d'après le théorème 4.12.

Corollaire 4.17 *Soit k un corps C_1. Alors pour toute extension algébrique K de k, on a* $\mathrm{Br}\, K = 0$.

Noter qu'ici l'extension K/k n'est pas supposée séparable.

23. Le résultat de Lang vaut plus généralement pour le corps des fractions K d'un anneau de valuation discrète hensélien excellent (cette dernière condition est automatique si $\mathrm{Car}\, K = 0$) à corps résiduel algébriquement clos.

Démonstration : Comme on l'a vu K est également C_1, donc $\mathrm{cd}(K) \leq 1$ d'après le théorème 4.16. Si K est parfait on en déduit $\mathrm{Br}\, K = 0$ via le théorème 4.12. Le cas où K est imparfait est un peu plus compliqué : on peut soit utiliser la caractérisation de $\mathrm{Br}\, K$ en termes d'algèbres simples centrales (cf. [6], preuve de la proposition 6.2.3.), soit utiliser le fait que pour toute extension finie galoisienne L de K, le $\mathrm{Gal}\,(L/K)$-module L^* est *cohomologiquement trivial*, ce qui résulte d'un théorème que nous verrons un peu plus loin (joint au fait que K est C_1 et à Hilbert 90) ; voir les exemples après le théorème 6.6.

□

En particulier un corps fini a un groupe de Brauer nul. De même pour une extension de k de degré de transcendance 1 et pour $k((t))$ si k est algébriquement clos.

4.5. Exercices

1. Soient k un corps et p un nombre premier. Soit k' une extension algébrique de k. Comparer $\mathrm{cd}_p(k)$ et $\mathrm{cd}_p(k')$. Que peut-on dire si on suppose de plus que $[k' : k]$ est premier à p ? Que $[k' : k]$ est fini ?

2. Soit k un corps parfait. Soit p un nombre premier.

a) Montrer que $\mathrm{cd}_p(k(t)) \leq \mathrm{cd}_p(k) + 1$.

b) En déduire, en utilisant l'exercice 1., que si K est une extension de k de degré de transcendance N, alors

$$\mathrm{cd}_p(K) \leq N + \mathrm{cd}_p(k)$$

3. Soient p un nombre premier et k un corps de caractéristique $\neq p$, de clôture séparable $\bar{k}$. Soit $n \in \mathbf{N}^*$. Montrer l'équivalence des propriétés :

i) $\mathrm{cd}_p(k) \leq n$;

ii) Pour toute extension algébrique séparable $K \subset \bar{k}$ de k, on a

$$H^{n+1}(K, \bar{k}^*)\{p\} = 0$$

et $H^n(K, \bar{k}^*)\{p\}$ est p-divisible ;

iii) Même énoncé que dans ii) mais en se limitant aux extensions K/k qui sont de plus finies et de degré premier à p.

(On pourra d'abord traduire ii) en utilisant le module galoisien μ_p).

4. Soit k un corps C_1 de caractéristique $p > 0$. Montrer que $[k : k^p]$ vaut 1 ou p.

5. Cohomologie d'un corps p-adique (I)

Dans ce chapitre, nous commençons à appliquer les résultats généraux des chapitres précédents à des situations de nature arithmétique. On va commencer par déterminer le groupe de Brauer d'un corps p-adique, ce qui peut être considéré comme la première étape de la *théorie du corps de classes local*, puis on en déduira un théorème de finitude pour la cohomologie.

5.1. Le groupe de Brauer d'un corps local

Dans tout ce paragraphe, on désigne par K un corps complet pour une valuation discrète v, à corps résiduel parfait κ. Par exemple K peut être un corps p-adique (extension finie de $\mathbf{Q}_p$) ou le corps des séries de Laurent $k((t))$ sur un corps parfait k, par exemple quand $k = \mathbf{F}_q$ est le corps fini à q éléments.

Theorème 5.1 *Soit K_{nr} l'extension maximale non ramifiée*[24] *de K. Alors K_{nr} est de dimension cohomologique ≤ 1 et on a $\mathrm{Br}\, K_{\mathrm{nr}} = 0$.*

Démonstration (esquisse): Plusieurs approches sont possibles. On peut utiliser l'interprétation du groupe de Brauer en termes d'algèbres simples centrales (cf. [13], paragraphe 12.2). Le résultat découle également du théorème de Lang (qui dit que K_{nr} est C_1) et du théorème 4.16.

Enfin, on peut utiliser le théorème 4.12 pour voir que $\mathrm{cd}(K_{\mathrm{nr}}) \leq 1$. Il suffit alors de vérifier que si K_1 est une extension finie séparable de K_{nr} et L une extension finie cyclique d'ordre premier de K_1, alors la norme $N_{L/K_1} : L^* \to K_1^*$ est surjective, ce qui résulte de la théorie des groupes de ramification (voir [13], chapitre V, Prop. 7). Ceci implique immédiatement $\mathrm{Br}\, K_{\mathrm{nr}} = 0$ si K est parfait, sinon le même raisonnement que dans la preuve du corollaire 4.17 fonctionne.

□

Corollaire 5.2 *Soit K_{nr} l'extension maximale non ramifiée de K. Alors $\mathrm{Br}\, K = \mathrm{Br}\,(K_{\mathrm{nr}}/K) = H^2(\mathrm{Gal}\,(K_{\mathrm{nr}}/K), K_{\mathrm{nr}}^*)$. Si $a \in \mathrm{Br}\, K$, alors il existe une extension finie galoisienne non ramifiée L de K telle que $a \in \mathrm{Br}\,(L/K) = \ker[\mathrm{Br}\, K \to \mathrm{Br}\, L]$.*

24. Merci à Alena Pirutka et Yongqi Liang qui m'ont fait observer que K^{nr} n'est pas complet par exemple si $K = \mathbf{Q}_p$.

Démonstration : D'après le théorème 5.1, on a $\mathrm{Br}\, K_{\mathrm{nr}} = 0$ d'où le premier point. Le deuxième point résulte du corollaire 3.9 vu que K_{nr} est la réunion (dans une clôture séparable $\overline{K}$ de K) des extensions finies galoisiennes non ramifiées de K.

□

Le corollaire ci-dessus dit que $\mathrm{Br}\, K$ est la réunion des $H^2(\mathrm{Gal}\,(L/K), L^*)$ pour L extension finie galoisienne non ramifiée de K. On va maintenant déterminer la structure de ces groupes de cohomologie. On note U_L le groupe des unités de l'anneau des entiers $\mathcal{O}_L$ de L, et (pour tout $n > 0$) U_L^n le sous-groupe de U_L constitué des éléments x tels que $v(1-x) \geq n$. Ainsi si $\mathcal{O}_L$ est l'anneau des entiers de L et π une uniformisante de L, le groupe U_L^n est constitué des éléments de L de la forme $1 + \pi^n x$ avec $x \in \mathcal{O}_L$.

Proposition 5.3 *Soit L une extension finie galoisienne non ramifiée de K. On pose $G = \mathrm{Gal}\,(L/K)$. Alors $H^q(G, U_L^1) = 0$ pour tout $q \geq 1$.*

Démonstration : Soit κ_L le corps résiduel de L. Comme L/K est non ramifiée, le groupe de Galois $\mathrm{Gal}\,(\kappa_L/\kappa)$ est isomorphe à G. D'autre part pour tout $n \geq 1$, le G-module U_L^n/U_L^{n+1} est isomorphe à κ_L ([13], chapitre IV, Proposition 6), dont la cohomologie est triviale d'après la proposition 4.1. On en déduit par récurrence sur n que la même propriété vaut pour les U_L^1/U_L^n pour tout $n \geq 1$. Maintenant le groupe U_L^1 est la limite projective des U_L^1/U_L^n ; on en déduit pour tout $q \geq 1$ que $H^q(G, U_L^1) = 0$ via le lemme suivant.[25] :

Lemme 5.4 *Soit G un groupe fini. Soit M un G-module filtré par une suite décroissante $(M_n)_{n\geq 1}$ de sous-modules*

$$M = M_1 \supset M_2 \supset \ldots \supset M_n \supset \ldots$$

tels que l'application canonique $M \to \varprojlim_n (M/M_n)$ soit un isomorphisme.

Soit q un entier naturel tel que $H^q(G, M_n/M_{n+1}) = 0$ pour tout $n \geq 1$. Alors $H^q(G, M) = 0$.

Démonstration : Soit $\varphi : G^q \to M$ un q-cocycle à valeurs dans $M = M_1$. Comme $H^q(G, M_1/M_2) = 0$, il existe une $(q-1)$-cochaîne ψ_1 de G à valeurs dans M_1 telle que $\varphi = \delta\psi_1 + \varphi_1$, où φ_1 est un q-cocycle à valeurs dans M_2. De proche en proche, on construit ainsi (en utilisant l'hypothèse $H^q(G, M_n/M_{n+1}) = 0$) une

25. Dans le cas particulier où le corps résiduel κ_L est fini, on peut aussi utiliser l'exercice 6 du chapitre 3.

suite (φ_n, ψ_n), où ψ_n est une $(q-1)$-cochaîne à valeurs dans M_n et φ_n un q-cocycle à valeurs dans M_{n+1}, telle que

$$\varphi_n = \delta\psi_{n+1} + \varphi_{n+1}$$

pour tout n. On définit alors une $(q-1)$-cochaîne ψ à valeurs dans $\varprojlim_n (M/M_n)$ (qui par hypothèse n'est autre que M) en considérant pour tout n la cochaîne

$$(\psi_1 + ... + \psi_n) \in M/M_{n+1}$$

Par construction on a alors $\varphi = \delta\psi$ donc φ est bien un cobord.

□

Corollaire 5.5 *Soit K un corps complet pour une valuation discrète, à corps résiduel fini. Soit L une extension finie galoisienne non ramifiée de K, on pose $G = \mathrm{Gal}\,(L/K)$. Alors $H^q(G, U_L) = 0$ pour tout $q \geq 1$.*

Démonstration : Cela résulte de la proposition 5.3, de la suite exacte

$$0 \to U_L^1 \to U_L \to \kappa_L^* \to 0$$

(où κ_L est le corps résiduel de L) et du fait qu'on a $H^q(G, \kappa_L^*) = 0$ pour tout $q \geq 1$ via Hilbert 90, la nullité de $\mathrm{Br}\,\kappa$, et le fait que la cohomologie (modifiée) du groupe cyclique $G \simeq \mathrm{Gal}\,(\kappa_L/\kappa)$ est 2-périodique.

Theorème 5.6 *Soit K un corps complet pour une valuation discrète à corps résiduel parfait κ. Soit $\bar{\kappa}$ une clôture algébrique de κ et $\Gamma = \mathrm{Gal}\,(\bar{\kappa}/\kappa) = \mathrm{Gal}\,(K_{\mathrm{nr}}/K)$. Alors pour tout $q \geq 1$ on a une suite exacte scindée*

$$0 \to H^q(\Gamma, \bar{\kappa}^*) \to H^q(\Gamma, K_{\mathrm{nr}}^*) \to H^q(\Gamma, \mathbf{Z}) \to 0$$

et une suite exacte scindée

$$0 \to \mathrm{Br}\,\kappa \to \mathrm{Br}\,K \to \chi(\Gamma) \to 0$$

où $\chi(\Gamma) = \mathrm{Hom}_c(\Gamma, \mathbf{Q}/\mathbf{Z})$ est le groupe des caractères du groupe de Galois absolu Γ de κ.

Démonstration : Soit L une extension finie galoisienne non ramifiée de K. Posons $G = \mathrm{Gal}\,(L/K)$. On a une suite exacte, scindée par le choix d'une uniformisante (noter qu'une uniformisante de K reste une uniformisante dans L vu que L/K est non ramifiée)

$$0 \to U_L \to L^* \xrightarrow{v} \mathbf{Z} \to 0$$

et une suite exacte

$$0 \to U_L^1 \to U_L \to \kappa_L^* \to 0$$

où κ_L est le corps résiduel de L. Cette dernière suite jointe à la proposition 5.3 donne

$$H^q(G, U_L) = H^q(G, \kappa_L^*)$$

et comme la première suite est scindée, on obtient une suite exacte scindée

$$0 \to H^q(G, \kappa_L^*) \to H^q(G, L^*) \to H^q(G, \mathbf{Z}) \to 0$$

En passant sur la limite sur L, on obtient alors une suite exacte scindée

$$0 \to H^q(\Gamma, \bar{\kappa}^*) \to H^q(\Gamma, K_{\mathrm{nr}}^*) \to H^q(\Gamma, \mathbf{Z}) \to 0$$

comme on voulait.

Faisons maintenant $q = 2$. Alors $H^2(\Gamma, \bar{\kappa}^*) = \operatorname{Br} \kappa$ par définition et $H^2(\Gamma, K_{\mathrm{nr}}^*) = \operatorname{Br} K$ d'après le corollaire 5.2. Enfin le groupe $H^2(\Gamma, \mathbf{Z}) = H^1(\Gamma, \mathbf{Q}/\mathbf{Z})$ est bien le groupe des caractères de Γ.

□

Corollaire 5.7 *On suppose que K est un corps p-adique. Alors* $\operatorname{Br} K$ *est isomorphe à* $\mathbf{Q}/\mathbf{Z}$.

En effet dans ce cas $\operatorname{Br} \kappa = 0$ car κ est fini, et $H^1(\kappa, \mathbf{Q}/\mathbf{Z})$ est isomorphe à $\mathbf{Q}/\mathbf{Z}$ vu que le groupe de Galois absolu de κ est isomorphe à $\widehat{\mathbf{Z}}$.

□

On peut préciser un peu l'énoncé précédent. Notons encore Γ le groupe $\operatorname{Gal}(K_{\mathrm{nr}}/K) = \operatorname{Gal}(\bar{\kappa}/\kappa)$. On a obtenu un isomorphisme $j_K : \operatorname{Br} K \to \mathbf{Q}/\mathbf{Z}$ via la chaîne d'isomorphismes suivante :

$$\operatorname{Br} K \xleftarrow{\alpha} H^2(\Gamma, K_{\mathrm{nr}}^*) \xrightarrow{\beta} H^2(\Gamma, \mathbf{Z}) \xleftarrow{\delta} H^1(\Gamma, \mathbf{Q}/\mathbf{Z}) \xrightarrow{\gamma} \mathbf{Q}/\mathbf{Z}$$

On a $j_K = \gamma \circ \delta^{-1} \circ \beta \circ \alpha^{-1}$.

Proposition 5.8 *Soit L une extension finie de degré n d'un corps p-adique K. Soit* $\operatorname{Res}_{L/K}$ *l'homomorphisme de restriction* $\operatorname{Br} K \to \operatorname{Br} L$. *Alors on a un diagramme commutatif :*

$$\begin{array}{ccc} \operatorname{Br} K & \xrightarrow{\operatorname{Res}_{L/K}} & \operatorname{Br} L \\ {\scriptstyle j_K}\downarrow & & {\scriptstyle j_L}\downarrow \\ \mathbf{Q}/\mathbf{Z} & \xrightarrow{.n} & \mathbf{Q}/\mathbf{Z} \end{array}$$

Démonstration : Par dévissage, on se ramène à traiter les deux cas extrêmes : L/K non ramifiée et L/K totalement ramifiée.

Supposons d'abord que L/K est non ramifiée. On peut alors supposer $L \subset K_{\mathrm{nr}}$ et on a donc $L_{\mathrm{nr}} = K_{\mathrm{nr}}$. Soit $\Gamma_n = \mathrm{Gal}\,(K_{\mathrm{nr}}/L) = \mathrm{Gal}\,(\bar{\kappa}/\kappa_L)$ (c'est l'unique sous-groupe d'indice n de Γ). Par fonctorialité de la restriction en cohomologie, on est ramené à montrer que le diagramme

$$\begin{array}{ccc} H^1(\Gamma, \mathbf{Q}/\mathbf{Z}) & \xrightarrow{\mathrm{Res}} & H^1(\Gamma_n, \mathbf{Q}/\mathbf{Z}) \\ {\scriptstyle\gamma}\downarrow & & {\scriptstyle\gamma_n}\downarrow \\ \mathbf{Q}/\mathbf{Z} & \xrightarrow{.n} & \mathbf{Q}/\mathbf{Z} \end{array}$$

est commutatif. Soit F le Frobenius (générateur topologique de Γ), alors on a $\gamma(\chi) = \chi(F)$ pour tout caractère $\chi : \Gamma \to \mathbf{Q}/\mathbf{Z}$. Le résultat découle alors de ce que le Frobenius de Γ_n est F^n, d'où

$$\gamma_n(\mathrm{Res}(\chi)) = \chi(F^n) = n\gamma(\chi)$$

Supposons maintenant que L/K est totalement ramifiée. Alors K_{nr} et L sont linéairement disjointes sur K et $L_{\mathrm{nr}} = K_{\mathrm{nr}}L$, ce qui fait que $\Gamma = \mathrm{Gal}\,(K_{\mathrm{nr}}/K)$ est aussi $\mathrm{Gal}\,(L_{\mathrm{nr}}/L)$. Via les fonctorialités habituelles, on est ramené à montrer la commutativité du diagramme

$$\begin{array}{ccc} H^2(\Gamma, K_{\mathrm{nr}}^*) & \xrightarrow{i} & H^2(\Gamma, L_{\mathrm{nr}}^*) \\ {\scriptstyle\beta}\downarrow & & {\scriptstyle\beta_L}\downarrow \\ H^2(\Gamma, \mathbf{Z}) & \xrightarrow{.n} & H^2(\Gamma, \mathbf{Z}) \end{array}$$

où i est induite par l'inclusion $K_{\mathrm{nr}}^* \to L_{\mathrm{nr}}^*$ et β (resp. β_L) est induite par la valuation $v_K : K_{\mathrm{nr}}^* \to \mathbf{Z}$ (resp. $v_L : L_{\mathrm{nr}}^* \to \mathbf{Z}$). Cette commutativité résulte de ce que pour x dans K_{nr}^*, on a $v_L(x) = nv_K(x)$ vu que n est l'indice de ramification de L/K.

□

Corollaire 5.9 *Sous les hypothèses et notations de la proposition 5.8, un élément a de* $\mathrm{Br}\,K$ *a une image nulle dans* $\mathrm{Br}\,L$ *si et seulement si $na = 0$.*

Si de plus L/K est galoisienne, l'image de $H^2(\mathrm{Gal}\,(L/K), L^*)$ par j_K est le sous-groupe $(\frac{1}{n}\mathbf{Z})/\mathbf{Z}$ de $\mathbf{Q}/\mathbf{Z}$.

La première assertion vient de la proposition précédente et du fait que j_K et j_L sont des isomorphismes. La deuxième vient de l'identification de $H^2(\mathrm{Gal}\,(L/K), L^*)$ avec le noyau de la restriction $\mathrm{Br}\,K \to \mathrm{Br}\,L$.

□

Corollaire 5.10 *Sous les hypothèses et notations de la proposition 5.8, on a un diagramme commutatif :*

$$\begin{array}{ccc} \operatorname{Br} L & \xrightarrow{\text{Cor}} & \operatorname{Br} K \\ {\scriptstyle j_L}\downarrow & & {\scriptstyle j_K}\downarrow \\ \mathbf{Q}/\mathbf{Z} & \xrightarrow{\text{Id}} & \mathbf{Q}/\mathbf{Z} \end{array}$$

Démonstration : Soit $\alpha_L \in \operatorname{Br} L$. Comme j_K et j_L sont des isomorphismes et $\mathbf{Q}/\mathbf{Z}$ est divisible, il existe d'après la proposition 5.8 un élément $\alpha \in \operatorname{Br} K$ tel que $\operatorname{Res}(\alpha) = \alpha_L$. Comme l'indice de Γ_L dans Γ_K est n, on a alors :

$$\operatorname{Cor}(\alpha_L) = \operatorname{Cor}(\operatorname{Res}(\alpha)) = n\alpha$$

d'où

$$j_K(\operatorname{Cor}(\alpha_L)) = nj_K(\alpha) = j_L(\alpha_L)$$

d'après la proposition 5.8.

□

Remarque : Les mêmes résultats (avec des démonstrations identiques) valent pour un corps local de caractéristique $p > 0$, i.e. pour une extension finie de $\mathbf{F}_p((t))$, à condition de toujours faire l'hypothèse supplémentaire que l'extension L/K est *séparable*.

5.2. Le théorème de finitude pour un corps p-adique

Dans tout ce paragraphe, K désigne une extension finie du corps $\mathbf{Q}_p$ pour p premier. On note $\Gamma_K = \operatorname{Gal}(\overline{K}/K)$ le groupe de Galois absolu de K. On appelle $\mathcal{O}_K$ l'anneau des entiers de K, et $U_K = \mathcal{O}_K^*$ le groupe multiplicatif de ses inversibles ; ce sont des groupes profinis. Enfin on note $\mathcal{M}_K$ l'idéal maximal de $\mathcal{O}_K$ et $\mathbf{F}_K = \mathcal{O}_K/\mathcal{M}_K$ son corps résiduel.

On commence par calculer la cohomologie de μ_n.

Proposition 5.11 *1. Le groupe $H^1(K, \mu_n) = K^*/K^{*n}$ est fini.*

2. On a $H^2(K, \mu_n) = \mathbf{Z}/n\mathbf{Z}$.

Démonstration : 1. On a déjà vu (via la suite exacte de Kummer et Hilbert 90) l'égalité $H^1(K, \mu_n) = K^*/K^{*n}$. Le fait que ces groupes soient finis est classique et résulte par exemple de la filtration du groupe des unités U_K par les U_K^i, $i \geq 1$ ([13], IV.2). On peut aussi utiliser le fait que U_K est

un *groupe de Lie p-adique* commutatif compact, donc isomorphe au produit direct d'un groupe fini et de $\mathbf{Z}_p^r$ avec $r \geq 0$.

2. Le corollaire 5.7 dit que $\mathrm{Br}\, K \simeq \mathbf{Q}/\mathbf{Z}$. On a donc $H^2(K, \mu_n) = (\mathrm{Br}\, K)[n] \simeq \mathbf{Z}/n\mathbf{Z}$.

□

Remarque : Si K est une extension finie de $k((t))$, avec k fini de caractéristique $p > 0$, il n'est plus vrai que K^*/K^{*p} est fini, ni que $H^1(K, \mathbf{Z}/p)$ est fini.

Theorème 5.12 *Un corps p-adique K est de dimension cohomologique 2.* [26]

Démonstration : La dimension cohomologique de K est au moins 2 vu que $H^2(K, \mu_n)$ est non nul. Soit K_{nr} l'extension maximale non ramifiée de K. Le groupe Γ_K est extension

$$1 \to \Gamma_{K_{\mathrm{nr}}} \to \Gamma_K \to \Gamma_{\mathbf{F}_K} \to 1$$

du groupe de Galois absolu $\Gamma_{\mathbf{F}_K}$ du corps résiduel $\mathbf{F}_K$ par le sous-groupe d'inertie $\Gamma_{K_{\mathrm{nr}}}$. Or $\mathbf{F}_K$ est C_1 (théorème de Chevalley), donc de dimension cohomologique ≤ 1, et K_{nr} est de dimension cohomologique ≤ 1 d'après le théorème 5.1. Il suffit alors d'appliquer la proposition 3.22.

□

Corollaire 5.13 *Soient K un corps p-adique et M un Γ_K-module fini. Alors $H^r(\Gamma_K, M)$ est fini pour tout $r \geq 0$.*

Démonstration : Soit n l'ordre de M. D'après ce qu'on a déjà vu, $H^r(K, \mu_n)$ est fini pour $r = 0, 1, 2$, et nul pour $r \geq 3$. Comme M est fini, on peut trouver une extension finie galoisienne L/K telle que l'action de Γ_L sur μ_n et sur M soit triviale ; en particulier le Γ_L-module M est isomorphe à une somme directe de μ_{n_i}. Comme on a alors $H^q(\Gamma_L, M)$ fini pour tout $q \geq 0$ d'après l'étude de la cohomologie de μ_n, la suite spectrale

$$H^p(\mathrm{Gal}\,(L/K), H^q(\Gamma_L, M)) \Rightarrow H^{p+q}(\Gamma_K, M)$$

permet de conclure que tous les $H^r(\Gamma_K, M)$ sont finis.

□

26. Ce résultat sera raffiné un peu plus tard.

5.3. Exercices

1. Soit k_0 un corps de caractéristique 0 qui n'est pas algébriquement clos, n'a aucune extension abélienne non triviale, et vérifie $\mathrm{cd}(k_0) \leq 1$ (exemple [27] : le composé de toutes les extensions galoisiennes finies résolubles de $\mathbf{Q}$). Soit $k = k_0((t))$. Montrer que $\mathrm{Br}\, k = 0$ mais que k n'est pas de dimension cohomologique ≤ 1.

2. a) Soit p un nombre premier. Soient $K = \mathbf{F}_p((t))$ et Γ_K le groupe de Galois absolu de K. Que vaut $(\mathrm{Br}\, K)\{p\}$?

b) Trouver un corps k de caractéristique p (imparfait) tel que $\mathrm{cd}(\Gamma_k) \leq 1$ mais $\mathrm{Br}\, k \neq 0$.

3. Soit K un corps p-adique. Soit L une extension finie non ramifiée de K de groupe de Galois G. Montrer que $H^q(G, U_L) = 0$ pour tout $q \geq 1$.

4. Soit ℓ un nombre premier. Soit K une extension finie de $\mathbf{Q}_l$ de groupe de Galois $G = \mathrm{Gal}\,(\overline{K}/K)$. On fixe un nombre premier p (qui peut être égal à ℓ).

a) Soit L une extension algébrique de K dont le degré (en tant que nombre surnaturel) est divisible par p^∞. Montrer que $(\mathrm{Br}\, L)\{p\} = 0$ (on pourra écrire $(\mathrm{Br}\, L)\{p\}$ comme limite inductive de certains groupes $(\mathrm{Br}\, F)\{p\}$ pour F extension de K).

b) Soit $G_K(p) = G/I$ le plus grand quotient de G qui soit un pro-p-groupe : on a donc $G_K(p) = \mathrm{Gal}\,(K(p)/K)$, où $K(p)$ est une extension algébrique de K et $I = \mathrm{Gal}\,(\overline{K}/K(p))$. Montrer que $\mathrm{cd}_p(I) \leq 1$.

c) Montrer que tout homomorphisme de I dans un pro-p-groupe est trivial. En déduire que si A est un $G_K(p)$-module de torsion p-primaire, on a $H^1(I, A) = 0$.

d) Soit A un $G_K(p)$-module de torsion p-primaire. Montrer que pour tout entier $i \geq 0$, l'homomorphisme d'inflation $H^i(G_K(p), A) \to H^i(G, A)$ est un isomorphisme.

5. Soit K un corps p-adique de groupe de Galois absolu Γ_K. Soit M un Γ_K-module de type fini. Montrer que $H^1(K, M)$ est fini.

27. Pour vérifier que $\mathrm{cd}(k_0) \leq 1$, il faut connaître le groupe de Brauer d'un corps de nombres afin d'appliquer le théorème 4.12, cf. [14], Prop. 9 p. 91.

6. Théorème de Tate-Nakayama, application aux formations de classes

La notion générale de *formation* de classes est très utile pour mieux comprendre la structure du groupe de Galois abélien d'un corps p-adique ou d'un corps de nombres (théorie du corps de classes), et aussi pour démontrer des théorèmes de dualité en arithmétique. On regroupe dans ce chapitre des résultats techniques qui seront ensuite notamment appliqués aux situations arithmétiques. On aura d'abord besoin de compléments sur la cohomologie des groupes finis, qui font l'objet du prochain paragraphe.

6.1. Modules cohomologiquement triviaux

Le but de ce paragraphe (qui aurait pu figurer dans le chapitre 2.) est de donner quelques compléments sur la cohomologie des groupes finis. On commence par un lemme.

Lemme 6.1 *Soit G un groupe fini. Soient A et B des G-modules. Supposons B induit. Alors le G-module* $\mathrm{Hom}(A,B) := \mathrm{Hom}_{\mathbf{Z}}(A,B)$ *est induit.*

Notons que par définition, l'action de G sur $\mathrm{Hom}_{\mathbf{Z}}(A,B)$ est donnée par $(g.f)(x) = g.f(g^{-1}.x)$ pour tous $g \in G$, $f \in \mathrm{Hom}_{\mathbf{Z}}(A,B)$, $x \in A$; voir l'exercice 1 du chapitre 2 pour le cas particulier $B = \mathbf{Q}/\mathbf{Z}$.

Démonstration : (Voir aussi [13], Prop. 1. p. 149 pour un énoncé un peu plus général). Comme G est fini, les notions de G-module induits et co-induits coïncident. Or si B est co-induit, il est somme directe des $g.X$ pour $g \in G$, où X est un sous-groupe fixé de B. Alors $\mathrm{Hom}(A,B)$ est somme directe des $\mathrm{Hom}(A, g.X) = g.\mathrm{Hom}(A,X)$ (en effet $\mathrm{Hom}(A,g.X)$ est simplement le sous-groupe de $\mathrm{Hom}(A,B)$ constitué des f dont l'image est incluse dans $g.X$, ce qui équivaut à $\mathrm{Im}\,(g^{-1}.f \subset X)$, donc est co-induit.

□

Nous aurons aussi besoin de la notation suivante : soit G un groupe fini et soit A un G-module. Alors comme on l'a vu on a un plongement naturel $A \hookrightarrow I_G(A)$; on notera A_1 le quotient $I_G(A)/A$, et plus généralement par récurrence on définit $A_q = (A_{q-1})_1$ pour tout $q > 0$. De même on peut écrire A comme un quotient de $I_G(A)$ via l'homomorphisme surjectif (que nous avons déjà rencontré dans la preuve du lemme 3.20) $f \mapsto \sum_{g\in G} g.f(g^{-1})$; on appelle alors A_{-1} le noyau de $I_G(A) \to A$ et on pose $A_q = (A_{q+1})_{-1}$ si $q < 0$.

Alors on a par décalage

$$\widehat{H}^q(G, A) = \widehat{H}^{q-r}(G, A_r)$$

pour tous $q, r \in \mathbf{Z}$ via le corollaire 2.7.

Définition 6.2 Soit G un groupe profini. On dit qu'un G-module discret A est *cohomologiquement trivial* si pour tout $n > 0$ et tout sous-groupe fermé H de G, on a $H^n(H, A) = 0$.

En particulier un tel G-module est aussi un H-module cohomologiquement trivial pour tout sous-groupe fermé H de G.

Proposition 6.3 *Un G-module A est cohomologiquement trivial si et seulement si pour tout sous-groupe ouvert distingué U de G, le G/U-module A^U est cohomologiquement trivial.*

Démonstration : Si pour tout sous-groupe ouvert distingué U de G, le G/U-module A^U est cohomologiquement trivial, on a pour tout sous-groupe fermé H de G et tout $n > 0$:

$$H^n(H, A) = \varinjlim_{U} H^n(HU/U, A^U) = 0$$

(via la proposition 3.8) donc A est cohomologiquement trivial. En sens inverse supposons que A soit cohomologiquement trivial et soit U un sous-groupe ouvert distingué de G. Alors tout sous-groupe fermé de G/U est de la forme H/U, où H est un sous-groupe fermé de G contenant U, et comme par hypothèse $H^i(U, A) = 0$ pour $1 \leq i \leq n-1$, le corollaire 1.24 s'applique et donne que $H^n(H/U, A^U)$ s'injecte dans $H^n(H, A)$, donc est nul.

□

Par exemple un G-module induit est cohomologiquement trivial : cela résulte de ce que A est aussi induit en tant que H-module, fait qu'on a déjà vu quand G est fini. Cela marche aussi dans le cas général en utilisant le fait que l'espace topologique G est homéomorphe à $G/H \times H$ ([14], Prop. 1. p. 3). On peut également utiliser la proposition 6.3 ci-dessus pour se ramener au cas où G est fini, vu que pour tout groupe abélien X le G/U-module $(I_G(X))^U$ est isomorphe à $I_{G/U}(X)$.

Lemme 6.4 *Soit G_p un p-Sylow de G. Un G-module A est cohomologiquement trivial si et seulement si A est un G_p-module cohomologiquement trivial pour tout nombre premier p.*

Noter que si G'_p est un autre p-Sylow de G, alors A est cohomologiquement trivial comme G_p-module si et seulement s'il est cohomologiquement trivial comme G'_p-module. En effet G_p et G'_p sont conjugués (disons par $t \in G$), ce qui permet pour tout sous-groupe fermé H' de G'_p d'avoir un homomorphisme bijectif de A dans A (défini par $x \mapsto t^{-1}.x$) compatible avec l'isomorphisme $g \mapsto tgt^{-1}$ de H' dans $H := tH't^{-1}$, d'où un isomorphisme de $H^n(H, A)$ sur $H^n(H', A)$.

Démonstration : Soit H un sous-groupe fermé de G. Soit H_p un p-Sylow de H. Alors H_p est contenu dans un p-Sylow de G, qu'on peut supposer être G_p via la remarque ci-dessus. Le résultat découle alors de ce que pour $n \geq 1$, la restriction $H^n(H, A)\{p\} \to H^n(H_p, A)$ est injective (lemme 3.20, a)) vu que l'indice $[H : H_p]$ est premier à p.

□

Theorème 6.5 *Soit p un nombre premier. Soient G un p-groupe fini et A un G-module de p-torsion. On suppose qu'il existe $q \in \mathbf{Z}$ tel que $\widehat{H}^q(G, A) = 0$. Alors A est un G-module induit (en particulier cohomologiquement trivial).*

(La preuve va même montrer que A est un $\mathbf{F}_p[G]$-module libre).

Démonstration : On va commencer par trouver un G-module induit V tel que V^G soit isomorphe à A^G. Pour cela, posons $\Lambda = \mathbf{F}_p[G]$, et choisissons une base I du $\mathbf{F}_p$-espace vectoriel A^G. Posons $V = \bigoplus_I \Lambda$, alors V est un G-module co-induit, donc induit puisque G est fini. Comme $\Lambda^G = \mathbf{F}_p$, on obtient un isomorphisme $j_G : A^G \simeq V^G$. On va maintenant essayer d'étendre cet isomorphisme en un G-morphisme de A dans V.

Comme le foncteur $\mathrm{Hom}(., V)$ est exact dans la catégorie des $\mathbf{F}_p$-espaces vectoriels, on a une suite exacte de G-modules

$$0 \to \mathrm{Hom}(A/A^G, V) \to \mathrm{Hom}(A, V) \to \mathrm{Hom}(A^G, V) \to 0$$

et d'autre part le fait que V soit induit implique via le lemme 6.1 que le G-module $B := \mathrm{Hom}(A/A^G, V)$ est induit. On a donc $H^1(G, B) = 0$ d'où une surjection :

$$u : \mathrm{Hom}_G(A, V) \to \mathrm{Hom}_G(A^G, V) = \mathrm{Hom}_G(A^G, V^G)$$

De ce fait j_G s'étend bien en un G-homomorphisme $j : A \to V$.

On observe que le G-module $\ker j$ vérifie $(\ker j)^G = 0$ car la restriction de j à A^G est un isomorphisme de A^G sur V^G. Comme G est un p-groupe,

ceci implique $\ker j = 0$ par le lemme 3.15. Ainsi j est injective. Soit C son conoyau, la longue suite exacte de cohomologie

$$0 \to A^G \to V^G \to C^G \to H^1(G, A)$$

donne alors les implications

$$H^1(G, A) = 0 \Rightarrow C^G = 0 \Rightarrow C = 0$$

vu que j induit un isomorphisme $A^G \simeq V^G$ (la dernière implication vient encore du lemme 3.15). On a donc montré que si $H^1(G, A) = 0$, alors $A \simeq V$ est un G-module induit.

Soit alors $q \in \mathbf{Z}$ tel que $\widehat{H}^q(G, A) = 0$. On va se ramener au cas $q = 1$ par décalage. On a

$$\widehat{H}^q(G, A) = H^1(G, A_{q-1})$$

ce qui montre que $H^1(G, A_{q-1}) = 0$. D'après ce qui précède, ceci implique que A_{q-1} (qui est encore de p-torsion) est induit, mais alors on a

$$H^1(G, A) = \widehat{H}^{2-q}(G, A_{q-1}) = 0$$

et A est induit d'après le cas $q = 1$.

□

Theorème 6.6 *Soit G un groupe fini. Soit A un G-module.*

a) On suppose que pour tout nombre premier p, il existe un entier $q \in \mathbf{Z}$ (pouvant dépendre de p) tel que

$$\widehat{H}^q(G_p, A) = \widehat{H}^{q+1}(G_p, A) = 0$$

où G_p est un p-Sylow de G. Alors A est cohomologiquement trivial. Si on suppose de plus que A est un $\mathbf{Z}$-module libre, alors A est un $\mathbf{Z}[G]$-module projectif (donc relativement injectif).

b) On suppose que A est cohomologiquement trivial ; alors $\widehat{H}^q(H, A) = 0$ pour tout sous-groupe H de G et tout $q \in \mathbf{Z}$. De plus il existe une suite exacte

$$0 \to R \to F \to A \to 0$$

de G-modules avec F libre sur $\mathbf{Z}[G]$ et R projectif sur $\mathbf{Z}[G]$.

Démonstration : On commence par écrire A comme quotient d'un $\mathbf{Z}[G]$-module libre F, d'où une suite exacte de G-modules

$$0 \to R \to F \to A \to 0$$

Fixons un nombre premier p et plaçons nous d'abord sous l'hypothèse de a), i.e. $\widehat{H}^q(G_p, A) = \widehat{H}^{q+1}(G_p, A) = 0$. Alors comme F est en particulier relativement injectif, on obtient

$$\widehat{H}^{q+1}(G_p, R) = \widehat{H}^{q+2}(G_p, R) = 0 \tag{2}$$

ce qui, via la suite exacte,

$$0 \to R \xrightarrow{.p} R \to R/pR \to 0 \tag{3}$$

(noter que R est sans torsion car c'est un sous-module de F) donne l'égalité $\widehat{H}^{q+1}(G_p, R/pR) = 0$. Le théorème 6.5 donne alors que R/pR est un G_p-module induit.

On commence par le cas où A est supposé libre sur $\mathbf{Z}$; on va alors démontrer que A est un facteur direct de F (donc est un $\mathbf{Z}[G]$-module projectif). Soit M le G-module $M := \mathrm{Hom}(A, R)$.

Lemme 6.7 *On a $H^1(G, M) = 0$.*

Démonstration : La suite exacte (3) et le fait que A soit libre sur $\mathbf{Z}$ donne un isomorphisme de G-modules

$$M/pM \simeq \mathrm{Hom}(A, R/pR)$$

ce qui montre que M/pM est un G_p-module induit par le lemme 6.1 puisque R/pR est un G_p-module induit. De ce fait $H^1(G_p, M)[p] = 0$ via la longue suite exacte de cohomologie modifiée associée à la suite exacte

$$0 \to M \xrightarrow{.p} M \to M/pM \to 0$$

Ainsi on a $H^1(G, M)\{p\} = 0$ (rappelons que la restriction $H^1(G, M)\{p\} \to H^1(G_p, M)$ est injective par le lemme 3.20, a)). Ceci étant valable pour tout p, on obtient bien $H^1(G, M) = 0$.

□

Reprenons alors la preuve que A est un facteur direct de F, toujours sous l'hypothèse que A est libre sur $\mathbf{Z}$. Cette hypothèse implique qu'on a une suite exacte de G-modules

$$0 \to M = \mathrm{Hom}(A, R) \to \mathrm{Hom}(A, F) \to \mathrm{Hom}(A, A) \to 0$$

et $H^1(G,M) = 0$ donne que $\mathrm{Hom}_G(A,F)$ se surjecte sur $\mathrm{Hom}_G(A,A)$, ce qui permet (en considérant Id_A) d'obtenir une section de l'homomorphisme surjectif de G-modules $F \to A$. Ainsi F est isomorphe *comme G-module* à la somme directe $A \oplus R$ comme on voulait. On a ainsi démontré a) dans le cas particulier où A est libre sur $\mathbf{Z}$.

Démontrons maintenant a) dans le cas général. Ce qui précède s'applique à R d'après (2) car R est libre sur $\mathbf{Z}$ en tant que sous-module de F. On obtient donc que R est projectif (en particulier relativement injectif), donc cohomologiquement trivial. Comme c'est aussi le cas de F (qui est induit), le G-module $A = F/R$ est également cohomologiquement trivial (via la longue suite exacte). D'où a).

Montrons enfin b). Soit A un G-module cohomologiquement trivial. A fortiori A vérifie les hypothèses de a) (par exemple pour $q = 1$). Choisissons une surjection $F \to A$ de noyau R avec F libre sur $\mathbf{Z}[G]$. On vient de voir que R était alors projectif (en tant que G-module, donc aussi en tant que H-module pour tous sous-groupe H de G) donc pour tout $q \in \mathbf{Z}$, on obtient

$$\widehat{H}^q(H,A) = \widehat{H}^{q+1}(H,R) = 0$$

pour tout sous-groupe H de G, ce qui prouve a).

□

Exemples. 1. Soit k un corps parfait avec $\mathrm{cd}(k) \leq 1$. Soit K une extension algébrique séparable de k et soit L une extension finie galoisienne de K. Posons $G = \mathrm{Gal}\,(L/K)$ et soit $G_p = \mathrm{Gal}\,(L/K_p)$ un p-Sylow de G. Alors le G-module L^* est cohomologiquement trivial. En effet on a $H^1(G_p, L^*) = 0$ par Hilbert 90 et $H^2(G_p, L^*) \subset \mathrm{Br}\, K_p = 0$ par le théorème 4.12. Il suffit alors d'appliquer le théorème précédent. En particulier $\widehat{H}^0(G, L^*) = 0$, ce qui donne que la norme $N_{L/K} : L^* \to K^*$ est surjective sans avoir besoin de supposer l'extension L/K résoluble.

2. Soient maintenant k un corps (éventuellement imparfait) C_1, K une extension algébrique de k, et L une extension finie galoisienne de K de groupe G. Soit comme ci-dessus $G_p := \mathrm{Gal}\,(L/K_p)$ un p-Sylow de G. Comme K_p est C_1 (lemme 4.15), on obtient encore que la norme $N_{L/K_p} : L^* \to K_p^*$ est surjective (cf. preuve du théorème 4.16) d'où $\widehat{H}^0(G_p, L^*) = 0$; comme $H^1(G_p, L^*) = 0$ par Hilbert 90, le G-module L^* est cohomologiquement trivial et on obtient $\mathrm{Br}\,(L/K) = H^2(G, L^*) = 0$. Ceci étant vrai pour toute extension finie galoisienne L de K, on en déduit $\mathrm{Br}\, K = 0$ *sans faire l'hypothèse que k est parfait* (ni que K est une extension séparable de k).

6.2. Théorème de Tate-Nakayama

Avant d'introduire le formalisme des formations de classes et de démontrer un théorème de dualité abstrait pour ces structures, nous allons dans ce paragraphe démontrer l'important théorème de Tate-Nakayama, qui utilise de façon essentielle les résultats du paragraphe précédent. Dans tout ce paragraphe, on désigne par G un groupe fini et pour tout nombre premier p, on fixe un p-sous-groupe de Sylow G_p de G.

Lemme 6.8 *Soit A un G-module cohomologiquement trivial. Soit B un G-module sans torsion. Alors le G-module $A \otimes B := A \otimes_{\mathbf{Z}} B$ est cohomologiquement trivial.*

Démonstration : D'après le théorème 6.6, on a une suite exacte

$$0 \to R \to F \to A \to 0$$

avec F libre sur $\mathbf{Z}[G]$ et R facteur direct d'un $\mathbf{Z}[G]$-module libre. Alors les G-modules $F \otimes B$ et $R \otimes B$ sont tous deux facteur direct d'un G-module coinduit, ils sont donc cohomologiquement triviaux. Comme B est sans torsion, la suite

$$0 \to R \otimes B \to F \otimes B \to A \otimes B \to 0$$

reste exacte, d'où on déduit immédiatement via la longue suite exacte que le G-module $A \otimes B$ est aussi cohomologiquement trivial.

□

Remarque : La même preuve montre qu'il est suffisant de supposer $\mathrm{Tor}_{\mathbf{Z}}(A, B) = 0$, où $\mathrm{Tor}_{\mathbf{Z}}(., B)$ est le premier foncteur dérivé à gauche du foncteur $. \otimes_{\mathbf{Z}} B$ dans la catégorie des modules sur l'anneau $\mathbf{Z}$.

Proposition 6.9 *Soient A et A' deux G-modules. Soit $f : A' \to A$ un G-homomorphisme. On suppose que pour tout p premier, il existe un entier n_p tel que l'homomorphisme*

$$f_*^i : \widehat{H}^i(G_p, A') \to \widehat{H}^i(G_p, A)$$

soit surjectif pour $i = n_p$, bijectif pour $i = n_p + 1$, et injectif pour $i = n_p + 2$. Soit B un G-module sans torsion[28] *sur $\mathbf{Z}$. Alors pour tout sous-groupe H de G, l'homomorphisme*

$$\widehat{H}^i(H, A' \otimes B) \to \widehat{H}^i(H, A \otimes B)$$

induit par $f \otimes 1$ est bijectif pour tout $i \in \mathbf{Z}$. En particulier l'homomorphisme $\widehat{H}^i(H, A') \to \widehat{H}^i(H, A)$ induit par f est bijectif pour tout $i \in \mathbf{Z}$.

28. Là encore, cela fonctionne dès que $\mathrm{Tor}_{\mathbf{Z}}(A, B) = \mathrm{Tor}_{\mathbf{Z}}(A', B) = 0$.

Démonstration : On commence par le cas où f est injectif. Soit A'' son conoyau. La suite exacte longue associée à la suite exacte

$$0 \to A' \to A \to A'' \to 0$$

jointe à l'hypothèse sur les f_*^i donne alors

$$\widehat{H}^{n_p}(G_p, A'') = \widehat{H}^{n_p+1}(G_p, A'') = 0$$

pour tout nombre premier p. D'après le théorème 6.6, le G-module A'' est cohomologiquement trivial. D'après le lemme 6.8, le G-module $A'' \otimes B$ est aussi cohomologiquement trivial. Comme B est sans torsion, la suite

$$0 \to A' \otimes B \to A \otimes B \to A'' \otimes B \to 0$$

est exacte, ce qui implique que $\widehat{H}^q(H, A' \otimes B) \to \widehat{H}^q(H, A \otimes B)$ est bijectif pour tout $q \in \mathbf{Z}$ et tout sous-groupe H de G comme on voulait.

Le cas général se ramène au cas particulier f injectif par le procédé suivant : on plonge A' dans le module induit $\overline{A}' := I_G(A')$ et on pose $A^* = A \oplus \overline{A}'$. On obtient alors (via f et le plongement $j : A' \to \overline{A}'$) une injection $\theta = (f, j) : A' \to A^*$. Comme $\overline{A}'$ et $\overline{A}' \otimes B$ sont cohomologiquement triviaux, on a $\widehat{H}^q(H, A) = \widehat{H}^q(H, A^*)$ et $\widehat{H}^q(H, A \otimes B) = \widehat{H}^q(H, A^* \otimes B)$, ce qui permet de se ramener au cas précédent en remplaçant f par θ.

□

Proposition 6.10 *Soient A, B, C trois G-modules. Soit $\varphi : A \times B \to C$ une application bilinéaire compatible avec l'action de G. Soient $q \in \mathbf{Z}$ et $a \in \widehat{H}^q(G, A)$; pour tout sous-groupe H de G et tout G-module D, on note a_H la restriction de a à H et*

$$f(n, H, D) : \widehat{H}^n(H, B \otimes D) \to \widehat{H}^{n+q}(H, C \otimes D)$$

l'homomorphisme défini par le cup-produit avec a_H (relativement à l'application bilinéaire induite par φ).

Supposons que pour tout nombre premier p, il existe un entier n_p tel que $f(n, G_p, \mathbf{Z})$ soit surjectif pour $n = n_p$, bijectif pour $n = n_p + 1$, et injectif pour $n = n_p + 2$. Alors $f(n, H, D)$ est bijectif pour tout $n \in \mathbf{Z}$, tout sous-groupe H de G, et tout G-module sans torsion D (là encore $\mathrm{Tor}(B, D) = \mathrm{Tor}(C, D) = 0$ suffit).

Démonstration : On commence par le cas $q = 0$. Alors $a \in \widehat{H}^0(G, A) = A^G/N_G A$ provient d'un élément (noté encore a) de A^G. Soit $f : B \to C$ le G-homomorphisme défini par $f(b) = \varphi(a, b)$. Alors $f_n^* : \widehat{H}^n(G_p, B) \to \widehat{H}^n(G_p, C)$ est simplement $f(n, G_p, \mathbf{Z})$ et la proposition 6.9 dit alors que $f(n, H, D)$ est bijective puisque $f(n, H, D)$ est alors l'homomorphisme induit par $f \otimes \mathrm{Id} : B \otimes D \to C \otimes D$.

Le cas q quelconque se traite par décalage. Montrons par exemple comment passer de $q - 1$ à q en plongeant A dans l'induit $\overline{A} = I_G(A)$ (pour aller dans l'autre sens, on écrit A comme quotient de l'induit $\overline{A}$). Posons $A_1 = \overline{A}/A$, et de même posons $C_1 = \overline{C}/C$, ce qui induit une application bilinéaire $\varphi_1 : A_1 \times B \to C_1$. On peut alors écrire $a = \delta(a_1)$ avec $a_1 \in \widehat{H}^{q-1}(G, A_1)$ et a_1 définit par cup-produit des homomorphismes

$$f_1(n, H, D) : \widehat{H}^n(H, B \otimes D) \to \widehat{H}^{n+q-1}(H, C_1 \otimes D)$$

Comme $\overline{C} \times D$ est encore cohomologiquement trivial (lemme 6.8), le cobord $\delta : \widehat{H}^{n+q-1}(H, C_1 \otimes D) \to \widehat{H}^{n+q}(H, C \otimes D)$ est un isomorphisme. Or $f(n, H, D)$ s'obtient (au signe près) en composant f_1 avec δ vu la compatiblité des cup-produits avec les cobords (proposition 2.12). Si le résultat voulu vaut pour a_1, il vaut donc également pour a d'où le résultat par récurrence sur q.

□

On en déduit :

Theorème 6.11 (Tate-Nakayama) *Soit A un G-module. On considère un élément a de $H^2(G, A)$. Supposons que pour tout nombre premier p, les hypothèses suivantes valent :*

a) On a $H^1(G_p, A) = 0$.

b) Le groupe $H^2(G_p, A)$ est d'ordre $m_p := \#G_p$ et est engendré par la restriction a_p de a à $H^2(G_p, A)$.

Alors pour tout G-module sans torsion D et pour tout sous-groupe H de G, le cup-produit par $a_H = \mathrm{Res}_H(a) \in H^2(H, A)$ induit des isomorphismes

$$\widehat{H}^n(H, D) \to \widehat{H}^{n+2}(H, A \otimes D)$$

pour tout $n \in \mathbf{Z}$. En particulier le cup-produit par a_H induit des isomorphismes

$$\widehat{H}^n(H, \mathbf{Z}) \to \widehat{H}^{n+2}(H, A)$$

Démonstration : On applique la proposition précédente avec $B = \mathbf{Z}$, $C = A$, $q = 2$, en prenant pour $\varphi : A \otimes \mathbf{Z} \to A$ l'application évidente. On choisit $n_p = -1$. Le cup-produit

$$\widehat{H}^n(G_p, \mathbf{Z}) \to \widehat{H}^{n+2}(G_p, A)$$

induit par a_p est surjectif pour $n = -1$ via l'hypothèse a). Pour $n = 0$, c'est l'application

$$\mathbf{Z}/m_p\mathbf{Z} \to H^2(G_p, A)$$

qui envoie le générateur canonique de $\mathbf{Z}/m_p\mathbf{Z}$ sur a_p, et l'hypothèse b) dit que cette application est bijective. Enfin pour $n = 1$ le groupe $H^1(G_p, \mathbf{Z})$ est nul donc le cup-produit est bien injectif.

□

6.3. Premières applications aux corps p-adiques

Dans ce paragraphe on désigne par K un corps p-adique. Nous allons voir que les résultats du chapitre 5. permettent de préciser la structure du groupe de Galois $\mathrm{Gal}\,(L/K)$ quand L est une extension finie de K. On va notamment utiliser le fait que pour un groupe fini G, le groupe $\widehat{H}^{-2}(G, \mathbf{Z}) = H_1(G, \mathbf{Z})$ s'identifie à l'abélianisé G^{ab} de G (proposition 2.4).

Définition 6.12 Soit L une extension finie galoisienne de groupe G d'un corps p-adique K. Soit $n := [L : K]$. On appelle *classe fondamentale* de l'extension L/K l'unique élément $u_{L/K}$ de $\mathrm{Br}\,(L/K) = H^2(G, L^*)$ tel que $j_K(u_{L/K}) = 1/n \in \mathbf{Q}/\mathbf{Z}$.

Rappelons qu'on a un isomorphisme $j_K : \mathrm{Br}\,K \to \mathbf{Q}/\mathbf{Z}$ (corollaire 5.7) et que le groupe $\mathrm{Br}\,(L/K)$ est précisément le sous-groupe de n-torsion de $\mathrm{Br}\,K$ (corollaire 5.9), ce qui justifie la définition ci-dessus. Nous pouvons alors appliquer le théorème de Tate-Nakayama au G-module $A = L^*$ et à l'élément $u_{L/K}$ de $H^2(G, L^*)$. Soit en effet $G_p = \mathrm{Gal}\,(L/K_p)$ un p-Sylow de G. On a bien $H^1(G_p, L^*) = 0$ par Hilbert 90, et $H^2(G_p, L^*) = \mathrm{Br}\,(L/K_p)$ est d'ordre $\#G_p$, engendré par la restriction u_{L/K_p} de u à $H^2(G_p, L^*)$ (d'après la proposition 5.8). En prenant $n = -2$ et en appliquant la proposition 2.4, on obtient

Theorème 6.13 *Soit L une extension finie galoisienne d'un corps p-adique K. Alors le cup-produit par $u_{L/K}$ définit un isomorphisme*

$$\theta_{L/K} : G^{\mathrm{ab}} \to K^*/NL^*$$

où $G := \mathrm{Gal}\,(L/K)$ et $N : L^* \to K^*$ désigne la norme de L à K.

Définition 6.14 Soit L une extension finie abélienne de K. L'isomorphisme

$$\omega_{L/K} := \theta_{L/K}^{-1} : K^*/NL^* \to \mathrm{Gal}\,(L/K)$$

s'appelle *isomorphisme de réciprocité* associé à l'extension L/K. L'homomorphisme

$$\omega : K^* \to \Gamma_K^{\mathrm{ab}}$$

obtenue à partir des $\omega_{L/K}$ par passage à la limite sur les extensions finies abéliennes L de K s'appelle *application de réciprocité*. Elle induit un isomorphisme de $\varprojlim_L K^*/NL^*$ sur Γ_K^{ab}.

Ici Γ_K^{ab} est l'abélianisé de Γ_K en tant que groupe profini (c'est le quotient de Γ_K par l'adhérence de son sous-groupe dérivé au sens usuel).

Nous verrons plus loin que Γ_K^{ab} est le complété profini de K^*, et donc que ce complété profini est isomorphe à $\varprojlim_L K^*/NL^*$ (la limite étant prise sur les extensions finies abéliennes L de K), mais ceci nécessite de connaître le *théorème d'existence* pour les corps p-adiques. Pour l'instant on déduit juste des résultats précédents que $\varprojlim_L K^*/NL^*$ est un quotient du complété profini $\widehat{K}^*$ de K^*.

La proposition suivante fait le lien entre application de réciprocité et cup-produit.

Proposition 6.15 *Soit L une extension finie abélienne d'un corps p-adique K. Soient $G = \mathrm{Gal}\,(L/K)$ et $\chi : G \to \mathbf{Q}/\mathbf{Z}$ un caractère de G, dont on note d_χ l'image dans $H^2(G, \mathbf{Z})$ via le cobord associé à la suite exacte*

$$0 \to \mathbf{Z} \to \mathbf{Q} \to \mathbf{Q}/\mathbf{Z} \to 0$$

Soit $a \in K^*$ d'image $\bar{a} \in \widehat{H}^0(G, L^*) = K^*/NL^*$. Alors[29]

$$\chi(\omega_{L/K}(\bar{a})) = j_K(\bar{a} \cup d_\chi)$$

où $j_K : \mathrm{Br}\,(L/K) \to \mathbf{Q}/\mathbf{Z}$ est l'invariant local.

Démonstration : Soit $u = u_{L/K} \in H^2(G, L^*)$ la classe fondamentale. Soit $s = \omega_{L/K}(\bar{a}) \in G = \widehat{H}^{-2}(G, \mathbf{Z})$ (rappelons que G est abélien). Notons $n := [L : K]$. Par définition de l'application de réciprocité, on a

$$u \cup s = \bar{a} \in \widehat{H}^0(G, L^*)$$

29. Notons qu'il n'y a pas ici à se préoccuper de l'ordre dans lequel on fait le cup-produit car $\bar{a} \cup d_\chi = d_\chi \cup \bar{a}$ vu que les classes de cohomologie considérées sont en degré pair.

d'où, par associativité du cup-produit (proposition 2.13) et compatibilité avec les cobords (proposition 2.12)

$$\bar{a} \cup d_\chi = u \cup (s \cup d_\chi) = u \cup (d(s \cup \chi))$$

où $s \cup \chi \in \widehat{H}^{-1}(G, \mathbf{Q}/\mathbf{Z})$. Comme l'action de G sur $\mathbf{Q}/\mathbf{Z}$ est triviale, le groupe $\widehat{H}^{-1}(G, \mathbf{Q}/\mathbf{Z})$ est simplement le sous-groupe $\frac{1}{n}\mathbf{Z}/\mathbf{Z}$ de $\mathbf{Q}/\mathbf{Z}$ et le cup-produit $s \cup \chi$ s'identifie à $\chi(s)$. Posons alors $\chi(s) = r/n$ avec $r \in \mathbf{Z}$. Il est immédiat que $d(r/n) = r \in \widehat{H}^0(G, \mathbf{Z}) = \mathbf{Z}/n\mathbf{Z}$ d'où

$$u \cup (d(s \cup \chi)) = u \cup r = r.u \in \mathbf{Q}/\mathbf{Z}$$

Or on a précisément $j_K(r.u) = r/n$ par définition de u donc finalement $j_K(r.u) = \chi(s)$, ou encore

$$j_K(\bar{a} \cup d_\chi) = \chi(s)$$

comme on voulait.

□

Corollaire 6.16 *Soit K un corps p-adique de groupe de Galois absolu $\Gamma = \mathrm{Gal}\,(\overline{K}/K)$. Soit χ un caractère de Γ^{ab} (ou de Γ, cela revient au même). Soit $b \in K^*$. Alors*

$$j_K(b \cup \chi) = \chi(\omega(b))$$

où, dans le cup-produit, χ est vu comme un élément de $H^2(\Gamma, \mathbf{Z})$ et b comme un élément de $H^0(\Gamma, \overline{K}^*)$.

Cela résulte de la proposition précédente par passage à la limite sur les extensions finies abéliennes L de K.

□

6.4. Notion de formation de classes

Soit G un groupe profini. Soit C un G-module discret. On considère une famille[30] d'isomorphismes $\mathrm{inv}_U : H^2(U, C) \simeq \mathbf{Q}/\mathbf{Z}$ indexés par les sous-groupes ouverts U de G.

Définition 6.17 On dit qu'un système $(C, \{\mathrm{inv}_U\})$ (qu'on pourra aussi noter (C, G)) comme ci-dessus est une *formation de classes* (associée à G) si les deux propriétés suivantes sont satisfaites :

a) Pour tout sous-groupe ouvert U de G, on a $H^1(U, C) = 0$.

30. La définition que nous adoptons ici est celle de [10], paragraphe I.1. Elle est légèrement moins générale que celle de [14], chapitre XI, mais elle sera suffisante pour les applications.

b) Pour tous sous-groupes ouverts U, V de G avec $V \subset U$, le diagramme suivant est commutatif

$$\begin{array}{ccc} H^2(U,C) & \xrightarrow{\mathrm{Res}} & H^2(V,C) \\ \downarrow{\scriptstyle \mathrm{inv}_U} & & \downarrow{\scriptstyle \mathrm{inv}_V} \\ \mathbf{Q}/\mathbf{Z} & \xrightarrow{.n} & \mathbf{Q}/\mathbf{Z} \end{array} \tag{4}$$

où $n := [U : V]$.

Soit $(C, \{\mathrm{inv}_U\})$ une formation de classes. La définition et le corollaire 1.24 donnent, pour toute paire de sous-groupes ouverts U et V de G avec V distingué d'indice n dans U, un diagramme commutatif à lignes exactes :

$$\begin{array}{ccccccccc} 0 & \longrightarrow & H^2(U/V, C^V) & \longrightarrow & H^2(U,C) & \xrightarrow{\mathrm{Res}} & H^2(V,C) & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \mathrm{inv}_{U/V}} & & \downarrow{\scriptstyle \mathrm{inv}_U} & & \downarrow{\scriptstyle \mathrm{inv}_V} & & \\ 0 & \longrightarrow & \frac{1}{n}\mathbf{Z}/\mathbf{Z} & \longrightarrow & \mathbf{Q}/\mathbf{Z} & \xrightarrow{.n} & \mathbf{Q}/\mathbf{Z} & \longrightarrow & 0 \end{array}$$

En particulier, si U est un sous-groupe ouvert distingué de G d'indice n, on a un isomorphisme $\mathrm{inv}_{G/U} : H^2(G/U, C^U) \simeq \frac{1}{n}\mathbf{Z}/\mathbf{Z}$.

Définition 6.18 On notera $u_{G/U}$ l'unique élément de $H^2(G/U, C^U)$ qui s'envoie sur $1/n$ par $\mathrm{inv}_{G/U}$; on dit que $u_{G/U}$ est la *classe fondamentale* de G/U.

Remarque : Avec notre définition, l'existence d'une formation de classes associée à G implique que l'ordre de G (en tant que nombre surnaturel) est divisible par tout élément de $\mathbf{N}^*$. Si en effet il existait un nombre premier p tel que cet ordre ne soit pas divisible par p^{r+1} avec $r \in \mathbf{N}$, alors pour U ouvert distingué dans G on aurait $H^2(G/U, C^U)\{p\}$ annulé par p^r (car tout élément de $H^2(G/U, C^U)\{p\}$ est annulé par l'ordre de G/U et par une puissance de p, donc par leur pgcd). Ainsi $H^2(G, C)\{p\}$ serait annulé par p^r et ne pourrait pas être isomorphe à $(\mathbf{Q}/\mathbf{Z})\{p\}$.

Proposition 6.19 *Soit $(C, \{\mathrm{inv}_U\})$ une formation de classes. Soient U, V des sous-groupes ouverts de G avec $V \subset U$. Alors :*

a) On a un diagramme commutatif

$$\begin{array}{ccc} H^2(V,C) & \xrightarrow{\mathrm{Cor}} & H^2(U,C) \\ \downarrow{\scriptstyle \mathrm{inv}_V} & & \downarrow{\scriptstyle \mathrm{inv}_U} \\ \mathbf{Q}/\mathbf{Z} & \xrightarrow{\mathrm{Id}} & \mathbf{Q}/\mathbf{Z} \end{array}$$

b) On suppose de plus U et V distingués dans G. Alors l'image de $u_{G/U} \in H^2(G/U, C^U)$ par l'inflation $H^2(G/U, C^U) \to H^2(G/V, C^V)$ est $[U : V].u_{G/V}$.

Démonstration : a) résulte immédiatement des axiomes d'une formation de classes et de la formule $\mathrm{Cor} \circ \mathrm{Res} = .[U : V]$. Pour b), on écrit un diagramme commutatif :

$$\begin{array}{ccccc} H^2(G/U, C^U) & \xrightarrow{\mathrm{Inf}} & H^2(G, C) & \xrightarrow{\mathrm{inv}_G} & \mathbf{Q}/\mathbf{Z} \\ \downarrow \mathrm{Inf} & & \downarrow = & & \downarrow = \\ H^2(G/V, C^V) & \xrightarrow{\mathrm{Inf}} & H^2(G, C) & \xrightarrow{\mathrm{inv}_G} & \mathbf{Q}/\mathbf{Z} \end{array}$$

et le résultat découle alors de la définition de $u_{G/U}$ et $u_{G/V}$, qui s'envoie respectivement sur $1/[G : U]$ et $1/[G : V]$ dans $\mathbf{Q}/\mathbf{Z}$.

□

Exemples 1. Soit $G = \mathrm{Gal}\,(\overline{K}/K)$ le groupe de Galois absolu d'un corps p-adique K. Posons $C = \overline{K}^*$. Alors d'après le théorème de Hilbert 90 et la proposition 5.8, les isomorphismes $\mathrm{Br}\, L \xrightarrow{j_L} \mathbf{Q}/\mathbf{Z}$ (définis pour tout sous-groupe ouvert $U = \mathrm{Gal}\,(\overline{K}/L)$ de G, i.e. pour toute extension finie L de K) définissent une formation de classes.

2. Soit $G = \widehat{\mathbf{Z}}$ (par exemple G peut être le groupe de Galois d'un corps fini). Prenons $C = \mathbf{Z}$, muni de l'action triviale de G. Soit σ un générateur topologique de G. Pour $m > 0$ l'unique sous-groupe U d'indice m de G est engendré par σ^m. On obtient alors une formation de classes en prenant pour $\mathrm{inv}_U : H^2(U, \mathbf{Z}) \to \mathbf{Q}/\mathbf{Z}$ la composée de $\delta^{-1} : H^2(U, \mathbf{Z}) \to H^1(U, \mathbf{Q}/\mathbf{Z})$ avec l'évaluation $\chi \mapsto \chi(\sigma^m)$ de $H^1(U, \mathbf{Q}/\mathbf{Z})$ dans $\mathbf{Q}/\mathbf{Z}$.

Proposition 6.20 *Soit $(C, \{\mathrm{inv}_U\})$ une formation de classes. soit U un sous-groupe ouvert distingué de G. Alors pour tout G/U-module M sans torsion, le cup-produit par $u_{G/U}$:*

$$\widehat{H}^r(G/U, M) \to \widehat{H}^{r+2}(G/U, M \otimes C^U)$$

est un isomorphisme pour tout $r \in \mathbf{Z}$.

Démonstration : C'est le théorème de Tate-Nakayama (théorème 6.11).

□

Proposition 6.21 *Soit $(C, \{\mathrm{inv}_U\})$ une formation de classes. Alors on a un homomorphisme canonique*

$$\omega_G : C^G \to G^{\mathrm{ab}}$$

d'image dense, et de noyau le groupe des normes universelles $\bigcap_U N_{G/U} C^U$ (l'intersection étant prise sur les sous-groupes ouverts distingués U de G). On dit que ω_G est l'application de réciprocité associée à la formation de classes $(C, \{\mathrm{inv}_U\})$.

Démonstration : C'est exactement le même argument qu'on a utilisé pour la définition 6.14. On prend $r = -2$ et $M = \mathbf{Z}$ dans la proposition précédente, et on passe à la limite sur U les isomorphismes $(G/U)^{\mathrm{ab}} \to C^G/N_{G/U}C^U$, ce qui donne un isomorphisme

$$\theta : \varprojlim_U (G/U)^{\mathrm{ab}} \to \varprojlim_U C^G/N_{G/U}C^U$$

On obtient alors ω_G en composant l'homomorphisme canonique

$$C^G \to \varprojlim_U C^G/N_{G/U}C^U$$

avec θ^{-1}. L'assertion sur le noyau de ω_G est alors évidente, et la densité de $\operatorname{Im}\omega_G$ vient de ce que sa composée avec la projection $G^{\mathrm{ab}} \to (G/U)^{\mathrm{ab}}$ est surjective pour tout U.

□

Remarque : Le même calcul que dans le corollaire 6.16 donne, pour tout c de C^G et pour tout caractère χ de G^{ab}, la formule

$$\mathrm{inv}_G(c \cup \chi) = \chi(\omega_G(c))$$

où, pour faire le cup-produit, c est vu dans $H^0(G, C)$ et χ dans $H^2(G, \mathbf{Z})$.

6.5. La suite spectrale des Ext

Dans ce paragraphe, nous allons rappeler quelques résultats standard d'algèbre homologique. On désigne toujours par G un groupe profini et par C_G la catégorie des G-modules discrets. Considérons des objets M et N de C_G. Une difficulté est que si M n'est pas supposé de type fini, le G-module $\mathrm{Hom}(M, N) = \mathrm{Hom}_{\mathbf{Z}}(M, N)$ (l'action de G étant définie par la formule habituelle) n'est en général pas discret (autrement dit le stabilisateur d'un élément n'est pas toujours ouvert).

Définition 6.22 Soient M et N des G-modules discrets. On définit alors le G-module discret $\mathcal{H}om(M, N)$ par la formule

$$\mathcal{H}om(M, N) = \bigcup_U \mathrm{Hom}(M, N)^U$$

où U décrit l'ensemble des sous-groupes ouverts de G. Pour tout sous-groupe fermé distingué H de G, on note de même

$$\mathcal{H}om_H(M, N) = \bigcup_{U \supset H} \mathrm{Hom}(M, N)^U$$

où la réunion est sur l'ensemble des sous-groupes ouverts de G contenant H. C'est un G/H-module discret.

Définition 6.23 Soit H un sous-groupe fermé distingué d'un groupe profini G. Soit M un G-module discret. Pour tout $r \geq 0$, on définit $\mathcal{E}xt^r_H(M,N)$ comme le r-ième foncteur dérivé à droite du foncteur

$$N \mapsto \mathcal{H}om_H(M,N) : C_G \to C_{G/H}$$

Ainsi $\mathcal{E}xt^r_H(M,N)$ est un G/H-module discret.[31] Quand $H = \{1\}$, on notera $\mathcal{E}xt^r(M,N)$ au lieu de $\mathcal{E}xt^r_{\{1\}}(M,N)$. Si M est de type fini, on a $\mathrm{Hom}_H(M,N) = \mathcal{H}om_H(M,N)$ pour tout $N \in C_G$ et il n'y a pas lieu de distinguer entre $\mathrm{Ext}^r_H(M,N)$ (obtenu comme foncteur dérivé de $\mathrm{Hom}_H(M,.)$ de C_G dans $C_{G/H}$ ou $\mathcal{A}b$) et $\mathcal{E}xt^r_H(M,N)$.

Theorème 6.24 *Soit H un sous-groupe fermé distingué d'un groupe profini G. Soient $N, P \in C_G$ et soit M un G/H-module discret sans torsion.*[32] *Alors on a une suite spectrale*

$$E_2^{r,s} = \mathrm{Ext}^r_{G/H}(M, \mathcal{E}xt^s_H(N,P)) \Rightarrow \mathrm{Ext}^{r+s}_G(M \otimes N, P)$$

Démonstration : On peut considérer M comme un G-module avec action triviale de H. On a alors

$$\mathrm{Hom}_{G/H}(M, \mathcal{H}om_H(N,P)) = \mathrm{Hom}_G(M, \mathcal{H}om_H(N,P)) = \mathrm{Hom}_G(M \otimes N, P) \quad (5)$$

car $\mathrm{Hom}_G(M, \mathcal{H}om_H(N,P)) = \mathrm{Hom}_G(M, \mathrm{Hom}(N,P))$ vu que M est un G/H-module discret. On en déduit que pour tout G-module injectif I et tout G-module sans torsion N, le G/H-module $Q := \mathcal{H}om_H(N,I)$ est injectif car $\mathrm{Hom}_{G/H}(.,Q)$ est le composé des deux foncteurs exacts $.\otimes_N$ et $\mathrm{Hom}_G(.,I)$.

Pour appliquer la suite spectrale des foncteurs composés de Grothendieck ([16], Th. 5.8.3.), il nous suffit maintenant de vérifier que $\mathcal{H}om_H(N,I)$ est acyclique pour le foncteur $\mathrm{Hom}_{G/H}(M,.)$. Pour cela on écrit une résolution de N par des G-modules N_1 et N_0 sans torsion

$$0 \to N_1 \to N_0 \to N \to 0$$

31. Le G/H-module $\mathcal{H}om_H(M,N)$ correspond au Hom interne dans la catégorie $C_{G/H}$, pour les G/H-modules M^H et N^H, et les $\mathcal{E}xt_H(M,N)$ aux Ext internes correspondant. Quand G est le groupe de Galois d'un corps k, on peut identifier M et N à des *faisceaux étales* sur $\mathrm{Spec}\, k$ et on retrouve la distinction entre Hom (resp. Ext) et $\mathcal{H}om$ (resp. $\mathcal{E}xt$) pour des faisceaux.

32. Comme d'habitude $\mathrm{Tor}_{\mathbf{Z}}(M,N) = 0$ serait suffisant.

et on vérifie immédiatement (en utilisant le fait que I est injectif en tant que U-module pour tout sous-groupe ouvert U de G, via le fait que $A \mapsto I_G^U(A)$ est un foncteur exact) qu'on obtient une suite exacte

$$0 \to \mathcal{H}om_H(N, I) \to \mathcal{H}om_H(N_0, I) \to \mathcal{H}om_H(N_1, I) \to 0$$

qui est donc (d'après ce qui a été vu plus haut à propos de Q) une résolution injective du G/H-module $\mathcal{H}om_H(N, I)$. Ceci implique déjà que si $r \geq 2$, on a $\mathrm{Ext}^r_{G/H}(M, \mathcal{H}om_H(N, I)) = 0$. Pour $r = 1$, il faut juste vérifier que la flèche

$$\mathrm{Hom}_{G/H}(M, \mathcal{H}om_H(N_0, I)) \to \mathrm{Hom}_{G/H}(M, \mathcal{H}om_H(N_1, I))$$

reste surjective. D'après (5), cette flèche s'identifie à la flèche naturelle

$$\mathrm{Hom}_G(M \otimes N_0, I) \to \mathrm{Hom}_G(M \otimes N_1, I)$$

qui est bien surjective vu que I est injectif et la flèche $M \otimes N_1 \to M \otimes N_0$ reste injective vu que M est sans torsion. Finalement on a bien vérifié

$$\mathrm{Ext}^r_{G/H}(M, \mathcal{H}om_H(N, I)) = 0$$

pour tout $r \geq 1$, i.e. $\mathcal{H}om_H(N, I)$ est acyclique pour le foncteur $\mathrm{Hom}_{G/H}(M, .)$.

□

Exemples : 1. Pour $M = N = \mathbf{Z}$, on retrouve la suite de Hochschild-Serre vu que $\mathcal{E}xt^r_H(\mathbf{Z}, .) = \mathrm{Ext}^r_H(\mathbf{Z}, .) = H^r(H, .)$ pour tout $r \geq 0$.

2. Prenons $M = \mathbf{Z}$ et $H = \{1\}$. On obtient alors une suite spectrale

$$H^r(G, \mathcal{E}xt^s(N, P)) \Rightarrow \mathrm{Ext}^{r+s}_G(N, P)$$

Proposition 6.25 *Soient N et G des G-modules discrets. On suppose N de type fini.*

a) On a une suite exacte

$$0 \to H^1(G, \mathrm{Hom}(N, P)) \to \mathrm{Ext}^1_G(N, P) \to H^0(G, \mathrm{Ext}^1_{\mathbf{Z}}(N, P)) \to H^2(G, \mathrm{Hom}(N, P)) \to ... \tag{6}$$

De plus les $\mathrm{Ext}^r_G(N, P)$ sont de torsion pour tout $r \geq 1$.

b) Si de plus N est sans torsion, on a

$$H^r(G, \mathrm{Hom}(N, P)) = \mathrm{Ext}^r_G(N, P)$$

pour tout $r \geq 0$.

Démonstration : a) Comme N est de type fini, la suite spectrale devient

$$H^r(G, \mathrm{Ext}^s(N, P)) \Rightarrow \mathrm{Ext}_G^{r+s}(N, P)$$

En utilisant le fait que $\mathrm{Ext}_{\mathbf{Z}}^s(N, P)$ est nul [33] pour $s \geq 2$, on obtient la suite exacte voulue.

Comme groupe abélien N est somme directe de copies de $\mathbf{Z}/n$ et de $\mathbf{Z}$, et $\mathrm{Ext}_{\mathbf{Z}}^1(\mathbf{Z}, P) = 0$; ceci implique que $\mathrm{Ext}_{\mathbf{Z}}^1(N, P)$ est de torsion, donc avec la suite exacte tous les $\mathrm{Ext}_G^r(N, P)$ le sont aussi pour $r \geq 1$.

b) Notons que $\mathrm{Ext}_{\mathbf{Z}}^1(N, P) = 0$ est nul si N est de plus sans torsion, car comme groupe abélien N est alors isomorphe à la somme directe d'un nombre fini de copies de $\mathbf{Z}$. Le a) donne alors

$$H^r(G, \mathrm{Hom}(N, P)) = \mathrm{Ext}_G^r(N, P)$$

pour tout $r \geq 0$.

□

Soient maintenant M, N et P des G-modules discrets. On a un accouplement (cf. [10], page 4)

$$\mathrm{Ext}_G^r(M, N) \times \mathrm{Ext}_G^s(P, M) \to \mathrm{Ext}_G^{r+s}(P, N)$$

Comme $H^s(G, .) = \mathrm{Ext}_G^s(\mathbf{Z}, .)$ pour tout entier s, on en déduit (en faisant $P = \mathbf{Z}$) un accouplement

$$\mathrm{Ext}_{M,N} : \mathrm{Ext}_G^r(M, N) \times H^s(G, M) \to H^{r+s}(G, N)$$

qui pour $r = 0$ est l'application $(f, a) \mapsto f_*(a)$ de $\mathrm{Hom}_G(M, N) \times H^s(G, M)$ dans $H^s(G, N)$. Cet accouplement admet la compatibilité suivante avec le cup-produit :

Proposition 6.26 *Soit M, N, P des G-modules discrets. Soit*

$$\varphi : M \times N \to P$$

une application bilinéaire compatible avec l'action de G. Notons $u : M \to \mathcal{H}om(N, P)$ l'homomorphisme de G-modules correspondant. Soit

$$v : H^r(G, M) \to \mathrm{Ext}_G^r(N, P)$$

33. Pour le voir, il suffit de plonger P dans un groupe abélien divisible D, et d'observer que le quotient D/P est encore divisible, donc injectif dans $\mathcal{A}b$.

la composée de $u_* : H^r(G,M) \to H^r(G, \mathcal{H}om(N,P))$ *avec la flèche*

$$H^r(G, \mathcal{H}om(N,P)) \to \mathrm{Ext}^r_G(N,P)$$

provenant de la suite spectrale du théorème 6.24. Alors le diagramme suivant est commutatif :

$$\begin{array}{ccc} H^r(G,M) \times H^s(G,N) & \xrightarrow{\cup} & H^{r+s}(G,P) \\ \downarrow{\scriptstyle (v,\mathrm{Id})} & & \downarrow{\scriptstyle \mathrm{Id}} \\ \mathrm{Ext}^r_G(N,P) \times H^s(G,N) & \xrightarrow{\mathrm{Ext}_{N,P}} & H^{r+s}(G,P) \end{array}$$

Pour une preuve[34] (dans un cadre plus général), voir [9], Prop. V.1.20.

6.6. Le théorème de dualité pour une formation de classes

Dans tout ce paragraphe on désigne par G un groupe profini et par $(C, \{\mathrm{inv}_U\})$ une formation de classes associée à G. L'expression "G-module" désignera comme d'habitude un G-module discret. Pour simplifier l'écriture, on conviendra que $H^i(G,...) = 0$ si i est un entier strictement négatif.

Pour tout G-module M, on a (pour $r \in \mathbf{N}$) un accouplement

$$\mathrm{Ext}^r_G(M,C) \times H^{2-r}(G,M) \to \mathbf{Q}/\mathbf{Z}$$

obtenu en composant $\mathrm{Ext}_{M,C} : \mathrm{Ext}^r_G(M,C) \times H^{2-r}(G,M) \to H^2(G,C)$ avec $\mathrm{inv}_G : H^2(G,C) \to \mathbf{Q}/\mathbf{Z}$. On en déduit, pour $r \in \mathbf{N}$, des homomorphismes de groupes abéliens (fonctoriels et compatibles avec les cobords associés aux suites exactes courtes) :

$$\alpha^r(G,M) : \mathrm{Ext}^r_G(M,C) \to H^{2-r}(G,M)^*$$

Pour $r = 0$ et $M = \mathbf{Z}$, l'homomorphisme $\alpha^0(G,\mathbf{Z})$ va simplement de C^G dans $G^{\mathrm{ab}} = H^2(G,\mathbf{Z})^*$. On a aussi $\mathrm{Ext}^1_G(\mathbf{Z}/m, C) = C^G/m$ via la suite exacte

$$0 \to \mathbf{Z} \xrightarrow{.m} \mathbf{Z} \to \mathbf{Z}/m \to 0 \tag{7}$$

et l'axiome $H^1(G,C) = 0$. De même $\mathrm{Ext}^2_G(\mathbf{Z}/m, C) = H^2(G,C)[m]$.

On commence par décrire explicitement les $\alpha^r(G,M)$ pour $M = \mathbf{Z}$ et $M = \mathbf{Z}/m$.

34. Ce genre de vérification est nettement plus simple quand on connaît le formalisme des catégories dérivées.

Lemme 6.27 *a) L'application $\alpha^0(G,\mathbf{Z})$ est l'application de réciprocité $\omega_G : C^G \to G^{\mathrm{ab}}$; La source et le but de l'homomorphisme $\alpha^1(G,\mathbf{Z})$ sont nuls et $\alpha^2(G,\mathbf{Z}) : H^2(G,C) \to \mathbf{Q}/\mathbf{Z}$ est égale à inv_G.*

b) La composée de l'application $\alpha^0(G,\mathbf{Z}/m) : (C^G)[m] \to H^2(G,\mathbf{Z}/m)^*$ avec l'application naturelle $H^2(G,\mathbf{Z}/m)^* \to H^2(G,\mathbf{Z})^*[m] = G^{\mathrm{ab}}[m]$ est la restriction $C^G[m] \to G^{\mathrm{ab}}[m]$ de l'application ω_G. L'application $\alpha^1(G,\mathbf{Z}/m) : C^G/m \to H^1(G,\mathbf{Z}/m)^* = G^{\mathrm{ab}}/m$ est induite par ω_G et l'application

$$\alpha^2(G,\mathbf{Z}/m) : H^2(G,C)[m] \to \frac{1}{m}\mathbf{Z}/\mathbf{Z}$$

est induite par inv_G.

Démonstration : Les assertions sur les applications $\alpha^1(G,\mathbf{Z})$ et $\alpha^2(G,\mathbf{Z})$ sont immédiates. La proposition 6.26 jointe au fait que l'homomorphisme $\omega_G : H^0(G,C) \to H^2(G,\mathbf{Z})^*$ soit induit par le cup-produit (remarque à la fin du paragraphe 6.4.) donne l'assertion sur $\alpha^0(G,\mathbf{Z})$. Les assertions sur les $\alpha^r(G,\mathbf{Z}/m)$ se déduisent alors immédiatement de celles sur les $\alpha^r(G,\mathbf{Z})$ à partir des identifications $\mathrm{Ext}^1_G(\mathbf{Z}/m,C) = C^G/m$ et $\mathrm{Ext}^2_G(\mathbf{Z}/m,C) = H^2(G,C)[m]$, qui proviennent des suites exactes longues associées à la suite exacte (7).

□

Lemme 6.28 *Soit M un G-module de type fini. Alors $\mathrm{Ext}^r_G(M,C) = 0$ si $r \geq 4$. Si on suppose de plus M sans torsion, alors $\mathrm{Ext}^3_G(M,C) = 0$.*

Démonstration : On peut trouver une suite exacte de G-modules

$$0 \to M_1 \to M_0 \to M \to 0$$

avec M_0 de type fini et sans torsion, et donc M_1 également de type fini (car c'est un sous-module d'un module de type fini sur $\mathbf{Z}$) et sans torsion. Via la longue suite exacte, on est donc ramené à montrer que si $r \geq 3$, on a $\mathrm{Ext}^r_G(M,C) = 0$ pour M de type fini et sans torsion. Soit alors N le G-module $N = \mathrm{Hom}(M,\mathbf{Z})$. Alors les G-modules $N \otimes C$ et $\mathrm{Hom}(M,C)$ sont isomorphes, d'où un isomorphisme

$$\mathrm{Ext}^r_G(M,C) \simeq H^r(G, N \otimes C)$$

via la proposition 6.25 b). Comme N est de type fini, on a $N = N^U$ (et donc le U-module N est isomorphe à $\mathbf{Z}^m$ avec $m \in \mathbf{N}$) pour U sous-groupe ouvert assez petit de G, ce qui fait qu'on a

$$H^r(G, N \otimes C) = \varinjlim_U H^r(G/U, N \otimes C^U)$$

où la limite est prise sur les sous-groupes ouverts distingués U de G tels que $N = N^U$. La proposition 6.20 (conséquence immédiate du théorème de Tate-Nakayama) dit alors que pour tout $r \geq 3$ (cette hypothèse est nécessaire pour assurer que les groupes modifiés de Tate coïncident avec les groupes de cohomologie usuels), le cup-produit par la classe fondamentale $u_{G/U}$ donne un isomorphisme

$$H^{r-2}(G/U, N) \simeq H^r(G/U, N \otimes C^U)$$

On a alors, pour V ouvert distingué inclus dans U, un diagramme commutatif, dont les flèches horizontales sont des isomorphismes :

$$\begin{array}{ccc} H^{r-2}(G/U, N) & \xrightarrow{\cup u_{G/U}} & H^r(G/U, N \otimes C^U) \\ \Big\downarrow{\scriptstyle [U:V].\mathrm{Inf}} & & \Big\downarrow{\scriptstyle \mathrm{Inf}} \\ H^{r-2}(G/V, N) & \xrightarrow{\cup u_{G/V}} & H^r(G/V, N \otimes C^V) \end{array}$$

Le fait que le diagramme commute découle des formules

$$\mathrm{Inf}(u_{G/U}) = [U : V].u_{G/V}$$

(proposition 6.19) et

$$\mathrm{Inf}(a \cup b) = \mathrm{Inf}(a) \cup \mathrm{Inf}(b)$$

(proposition 2.13). D'autre part pour $r \geq 3$, le groupe $H^{r-2}(G/U, N)$ est de torsion et l'ordre de U (en tant que nombre surnaturel) est divisible par tout entier n comme on l'a vu après la définition d'une formation de classes. De ce fait la limite inductive des $H^{r-2}(G/U, N)$ (pour les applications de transition $[U : V]$.Inf) est nulle : en effet si α est un élément de m-torsion (avec $m > 0$) dans un $H^{r-2}(G/U, N)$, on peut trouver un sous-groupe ouvert distingué V de G inclus dans U tel que l'indice $[U : V]$ soit divisible par m, et l'image de α dans $H^{r-2}(G/V, N)$ est alors nulle. Finalement $H^r(G, N \otimes C)$ est nul comme on voulait.

□

On arrive maintenant au théorème principal de cette section, qui est un théorème de dualité général pour les formations de classes.

Theorème 6.29 *Soit M un G-module de type fini.*

a) L'homomorphisme $\alpha^r(G, M)$ est bijectif pour tout $r \geq 2$, et si M est sans torsion $\alpha^1(G, M)$ est également bijectif. En particulier $\mathrm{Ext}^r_G(M, C) = 0$ pour tout $r \geq 3$.

b) Supposons $\alpha^1(U, \mathbf{Z}/m)$ bijectif pour tout $m > 0$ et tout sous-groupe ouvert (distingué) U de G. Alors $\alpha^1(G, M)$ est bijectif.

c) Gardons les hypothèses de b) et supposons de plus M fini. On fait en outre l'hypothèse que $\alpha^0(U, \mathbf{Z}/m)$ est surjectif (resp. bijectif) pour tout $m > 0$ et tout sous-groupe ouvert (distingué) U de G. Alors $\alpha^0(G, M)$ est surjectif (resp. bijectif).

Démonstration : D'après le lemme 6.28, on a bien le résultat si $r \geq 4$, on suppose donc $r \leq 3$. Montrons d'abord le théorème quand G agit trivialement sur M. Dans ce cas M est somme directe de G-modules isomorphes à $\mathbf{Z}$ ou à $\mathbf{Z}/n$ et il suffit donc de traiter ces deux cas. Pour $M = \mathbf{Z}$ (où on se limite à $1 \leq r \leq 3$ puisque $\mathbf{Z}$ n'est pas fini), c'est le lemme 6.27 a) et le lemme 6.28. Pour $M = \mathbf{Z}/n$, c'est le lemme 6.27 b) si $r = 2$ et l'hypothèse b) (resp. c)) du théorème si $r = 1$ (resp. $r = 0$). Enfin pour $r = 3$ on déduit $\mathrm{Ext}^3_G(\mathbf{Z}/m, C) = 0$ de $\mathrm{Ext}^3_G(\mathbf{Z}, C) = 0$ via la suite exacte

$$0 \to \mathrm{Ext}^2_G(\mathbf{Z}, C)/m \to \mathrm{Ext}^3_G(\mathbf{Z}/m, C) \to \mathrm{Ext}^3_G(\mathbf{Z}, C)$$

(laquelle provient de la suite exacte (7)) et le fait que $\mathrm{Ext}^2_G(\mathbf{Z}, C) \simeq \mathbf{Q}/\mathbf{Z}$ est divisible. On obtient donc que le théorème vaut dès que l'action de G sur M est triviale.

Passons au cas général. Comme M est de type fini, on peut trouver un sous-groupe ouvert distingué U de G qui agit trivialement sur M. On écrit alors une suite exacte

$$0 \to M \to M_* \to M_1 \to 0$$

avec $M_* = I^U_G(M) = \mathbf{Z}[G/U] \otimes M$. Le lemme de Shapiro donne $H^r(G, M_*) = H^r(U, M)$ et $\mathrm{Ext}^r_G(M_*, C) = \mathrm{Ext}^r_U(M, C)$ (en effet $\mathrm{Ext}^r_G(M_*, .)$ et $\mathrm{Ext}^r_U(M, .)$ s'obtiennent comme foncteurs dérivés des foncteurs isomorphes $\mathrm{Hom}_G(M_*,)$ et $\mathrm{Hom}_U(M, .)$, l'isomorphisme étant induit par l'homomorphisme d'augmentation $M \otimes \mathbf{Z}[G/U] \to M$). On obtient alors un diagramme commutatif (les commutativités non évidentes[35] viennent de ce que l'augmentation induit la corestriction au niveau de la cohomologie, et la corestriction $H^2(U, C) \to H^2(G, C)$ induit via inv_U et inv_G l'identité sur $\mathbf{Q}/\mathbf{Z}$ par la proposition 6.19 a)) à lignes exactes :

$$\begin{array}{ccccccccccc}
\ldots & \longrightarrow & \mathrm{Ext}^r_G(M_1, C) & \longrightarrow & \mathrm{Ext}^r_U(M, C) & \longrightarrow & \mathrm{Ext}^r_G(M, C) & \longrightarrow & \mathrm{Ext}^{r+1}_G(M_1, C) & \longrightarrow & \ldots \\
 & & \downarrow{\scriptstyle \alpha^r(G, M_1)} & & \downarrow{\scriptstyle \alpha^r(U, M)} & & \downarrow{\scriptstyle \alpha^r(G, M)} & & \downarrow{\scriptstyle \alpha^{r+1}(G, M_1)} & & \\
\ldots & \longrightarrow & H^{2-r}(G, M_1)^* & \longrightarrow & H^{2-r}(U, M)^* & \longrightarrow & H^{2-r}(G, M)^* & \longrightarrow & H^{1-r}(G, M_1)^* & \longrightarrow & \ldots
\end{array}$$

35. Merci à Clément Gomez d'avoir attiré mon attention sur ce point.

Pour $r = 3$, on sait déjà, par le lemme et le cas où l'action de G est triviale, que $\mathrm{Ext}^3_U(M, C)$ et $\mathrm{Ext}^4_G(M_1, C)$ sont nuls ; il en va donc de même de $\mathrm{Ext}^3_G(M, C)$. Comme ceci est vrai pour tout G-module de type fini M, cela s'applique aussi à M_1 d'où $\mathrm{Ext}^3_G(M_1, C) = 0$. Finalement tous les termes du diagramme sont nuls pour $r = 3$. Pour $r = 2$, on sait maintenant que $\alpha^3(G, M_1)$ a une source et un but nuls, et d'autre part $\alpha^2(U, M)$ est un isomorphisme (l'action de U sur M étant triviale). Ainsi $\alpha^2(G, M)$ est surjective (pour tout M), donc aussi $\alpha^2(G, M_1)$. Le lemme des cinq donne alors que $\alpha^2(G, M)$ est un isomorphisme. Si de plus M est sans torsion, c'est aussi le cas de M_* et M_1 et on montre de la même façon que $\alpha^1(G, M)$ est un isomorphisme. Enfin la preuve des assertions b) et c) suit exactement le même schéma.

□

Remarque : On vérifie facilement que dans les assertions b) et c), il suffit de supposer que pour m fixé, les hypothèses sur $\alpha^1(U, \mathbf{Z}/m)$ et $\alpha^0(U, \mathbf{Z}/m)$ valent *pour U suffisamment petit*. En effet dans la preuve du cas général on peut toujours remplacer le sous-groupe U qui intervient par n'importe quel sous-groupe ouvert inclus dans U.

Exemples. 1. Soit G un groupe isomorphe à $\widehat{\mathbf{Z}}$ (par exemple le groupe de Galois absolu d'un corps fini) et soit C la formation de classes associée à un générateur topologique σ de G (cf. exemple 2. avant la proposition 6.20). Ici l'application de réciprocité est l'inclusion $n \mapsto \sigma^n$ de $\mathbf{Z}$ dans G. D'après le lemme 6.27, la source et le but de l'application $\alpha^0(U, \mathbf{Z}/m)$ sont nuls pour tout entier m et tout sous-groupe ouvert U de G (en effet $\mathrm{cd}(G) = 1$). L'application $\alpha^1(U, \mathbf{Z}/m)$ est aussi un isomorphisme car c'est l'application naturelle $\mathbf{Z}/m \to \widehat{\mathbf{Z}}/m$. Le théorème implique alors que si $r \geq 1$, alors $\alpha^r(G, M)$ est un isomorphisme pour tout G-module de type fini M, et la même propriété vaut quand $r = 0$ si M est fini.

2. Soit K un corps de groupe de Galois absolu $G = \mathrm{Gal}\,(\overline{K}/K)$ et supposons qu'on ait une formation de classe (G, C) associée à G. Soit M un G-module de type fini et sans torsion, et soit N le G-module $N = \mathrm{Hom}(M, \mathbf{Z})$ (M peut être vu comme le module galoisien des *caractères* d'un *K-tore algébrique* T et N comme son module des *co-caractères*). D'après le théorème 6.29, on a pour tout $r \geq 1$ des isomorphismes

$$\mathrm{Ext}^r_G(M, C) \to H^{2-r}(G, M)^*$$

mais d'autre part $\mathrm{Ext}^r_G(M, C) = H^r(G, \mathrm{Hom}_{\mathbf{Z}}(M, C))$ (proposition 6.25).

Comme $\mathrm{Hom}_{\mathbf{Z}}(M, C) = N \otimes C$, la proposition 6.26 donne que le cup-produit

$$H^r(G, N \otimes C) \times H^{2-r}(G, M) \to H^2(G, C) \simeq \mathbf{Q}/\mathbf{Z}$$

induit un isomorphisme $H^r(G, N \otimes C) \to H^{2-r}(G, M)^*$. Pour $r = 1$ on obtient même une dualité parfaite de groupes finis (utiliser le fait que $H^1(U, \mathbf{Z}) = 0$ et donc $H^1(G, M) = H^1(G/U, M)$ où U est un sous-groupe ouvert distingué de G tel que $M = M^U$; puis appliquer le corollaire 1.27.). Pour $r = 0, 2$ il faut faire un peu attention car si par exemple on prend pour K un corps p-adique (avec la formation de classes habituelle associée à $C = \overline{K}^*$) et $M = \mathbf{Z}$, on obtient $N = \mathbf{Z}$ d'où

$$H^0(G, N \otimes C) = K^*; \quad H^2(G, M) = (G^{\mathrm{ab}})^*$$

or le dual du groupe discret $(G^{\mathrm{ab}})^*$ est le groupe profini $G^{\mathrm{ab}} = \widehat{K}^*$, complété profini de K^*. De même $H^2(G, N \otimes C) = \mathrm{Br}\, K \simeq \mathbf{Q}/\mathbf{Z}$, dont le dual est $\widehat{\mathbf{Z}}$, complété de $H^0(G, M) = \mathbf{Z}$. Le fait qu'il faille "compléter les H^0" pour avoir de bons théorèmes de dualité faisant intervenir ces groupes est un problème récurrent quand on ne travaille plus avec des modules finis.

Nous verrons dans les prochains chapitres comment le théorème 6.29 s'applique au groupe de Galois d'un corps local pour obtenir le théorème de dualité de Tate, et aux corps de nombres pour donner la dualité de Poitou-Tate.

6.7. P-formations de classes

Il est parfois utile de considérer une notion légèrement plus générale que celle de formation de classes telle que nous l'avons définie. Pour un groupe profini G et un ensemble P de nombres premiers, on définit une *P-formation de classes* $(C, \{\mathrm{inv}_U\})$ par les mêmes axiomes qu'une formation de classes à part qu'au lieu de demander que les inv_U soient des isomorphismes, on demande seulement que ce soient des injections satisfaisant les deux axiomes suivants :

a) Pour tout sous-groupes ouverts U et V de G avec V distingué dans U, la flèche

$$\mathrm{inv}_{U/V} : H^2(U/V, C^V) \to [U : V]^{-1}\mathbf{Z}/\mathbf{Z}$$

est un isomorphisme.

b) Pour tout sous-groupe ouvert U de G et tout $\ell \in P$, la restriction

$$\mathrm{inv}_U : H^2(U, C)\{\ell\} \to \mathbf{Q}_\ell/\mathbf{Z}_\ell$$

est un isomorphisme.

Si P est l'ensemble de tous les nombres premiers, une P-formation de classes est donc une formation de classes au sens où nous l'avons définie précédemment, et si $P = \emptyset$ une P-formation de classes est une formation de classes au sens d'Artin et Tate (cf. [13], chapitre XI). Si tous les autres axiomes sont satisfaits, l'axiome b) est équivalent au fait que l'ordre de G est divisible par ℓ^∞ pour tout $\ell \in P$. Notons aussi que si (G, C) est une formation de classes et H est un sous-groupe fermé distingué de G, alors $(G/H, C^H)$ est une P-formation de classes, où P est l'ensemble des nombres premiers ℓ tels que ℓ^∞ divise $[G : H]$.

Le théorème 6.29 s'étend immédiatement aux P-formations de classes pourvu qu'on se restreigne partout aux composantes ℓ-primaires des groupes considérés avec $\ell \in P$ (rappelons que pour $r \geq 1$, les groupes $\mathrm{Ext}^r_G(M, N)$ sont toujours de torsion quand M est un G-module de type fini et pour $r = 0$ on se limite de toute façon à M fini).

6.8. Exercices

1. Donner un exemple de groupe fini G et de G-module A tels qu'il existe $q \in \mathbf{Z}$ vérifiant $\widehat{H}^q(G, A) = \widehat{H}^{q+1}(G, A) = 0$, mais A ne soit pas cohomologiquement trivial.

2. Soit G un groupe fini. Soit

$$0 \to X_1 \to X_2 \to ... \to X_n \to 0$$

une suite exacte de G-modules. Soit $j \in \{1, ...n\}$. Montrer que si X_i est cohomologiquement trivial pour tout $i \neq j$, alors X_j l'est également.

3. Soit Γ un groupe profini et p un nombre premier. On suppose que la p-dimension cohomologique $\mathrm{cd}_p(\Gamma)$ est un entier $n > 0$. Soit U un sous-groupe ouvert normal de Γ ; on considère un Γ-module de torsion p-primaire A.

a) On considère une résolution

$$0 \to A \to X^0 \to ... \to X^n \to ...$$

par des Γ-modules induits p-primaires et on pose $A_n = \ker[X^n \to X^{n+1}]$. Montrer que A_n est un Γ-module cohomologiquement trivial.

b) Montrer qu'on a un diagramme commutatif à lignes exactes, où N désigne la norme $N_{\Gamma/U}$:

$$\begin{array}{ccccccc}
((X^{n-1})^U)_{\Gamma/U} & \longrightarrow & (A_n^U)_{\Gamma/U} & \longrightarrow & H^n(U, A)_{\Gamma/U} & \longrightarrow & 0 \\
{\scriptstyle N}\downarrow & & {\scriptstyle N}\downarrow & & {\scriptstyle \mathrm{Cor}}\downarrow & & \\
(X^{n-1})^\Gamma & \longrightarrow & A_n^\Gamma & \longrightarrow & H^n(\Gamma, A) & \longrightarrow & 0
\end{array}$$

c) Montrer que la flèche verticale de gauche du diagramme est surjective.

d) Montrer que la flèche verticale du milieu est injective, et en déduire que la corestriction $H^n(U,A)_{\Gamma/U} \to H^n(\Gamma,A)$ est un isomorphisme.

4. a) Soit A un groupe abélien fini. Montrer que $\mathrm{Ext}^r_{\mathbf{Z}}(A,\mathbf{Z}) = 0$ si $r \neq 1$ et $\mathrm{Ext}^1_{\mathbf{Z}}(A,\mathbf{Z}) = A^*$.

b) Soit $G = \widehat{\mathbf{Z}}$, muni de sa formation de classes habituelle. Montrer que pour $r = 0, 1$, le cup-produit

$$H^r(G,M) \times H^{1-r}(G,M^*) \to H^1(G,\mathbf{Q}/\mathbf{Z}) = \mathbf{Q}/\mathbf{Z}$$

est non dégénéré si M est un G-module fini.

7. Cohomologie des corps p-adiques (II) : les théorèmes de dualité

7.1. Le théorème d'existence pour une formation de classes

Dans ce paragraphe, nous donnons quelques compléments sur les formations de classes, en démontrant notamment un *théorème d'existence* qui permet, sous certaines hypothèses, d'identifier les sous-groupes ouverts d'un groupe profini à ses *groupes de normes*.

Dans toute la suite, on désignera par (C,G) une formation de classes (on vérifiera d'ailleurs que tous les résultats de ce paragraphe restent valables pour une P-formation de classes, où P est un ensemble quelconque de nombres premiers, par exemple $P = \emptyset$ qui est l'hypothèse minimale ; le point est que le corollaire 6.20 reste valable tel quel).

Pour toute paire (U,V) de sous-groupes ouverts de G avec $V \subset U$, on dispose d'un homomorphisme *norme*

$$N_{U/V} : C^V \to C^U \quad x \mapsto \sum_{s \in U/V} s.x$$

qui coïncide avec la définition habituelle quand V est distingué dans U. On a par ailleurs la transitivité des normes : si $W \subset V \subset U$, alors $N_{U/W}$ est la composée de $N_{V/W}$ et $N_{U/V}$.

Définition 7.1 Un *sous-groupe de normes* de C^U est un sous-groupe de la forme $N_{U/V}(C^V)$ pour un certain sous-groupe ouvert V de U.

Proposition 7.2 *Soit (C, G) une formation de classes. Soit (U, V) une paire de sous-groupes ouverts de G avec $V \subset U$.*

a) Supposons que V soit distingué dans U. Alors on a un isomorphisme (de réciprocité)

$$C^U/N_{U/V}C^V \to (U/V)^{\mathrm{ab}}$$

En particulier si U/V est abélien (i.e. : V contient le sous-groupe dérivé profini $D(U)$ de U), on obtient un isomorphisme de $C^U/N_{U/V}C^V$ sur U/V.

b) Dans le cas général, soit W le plus petit sous-groupe fermé de U contenant V, distingué dans U, et tel que U/W soit abélien (W est le sous-groupe engendré par V et $D(U)$). Alors on a

$$N_{U/V}(C^V) = N_{U/W}(C^W)$$

c) Le groupe des normes $N_{U/V}(C^V)$ est d'indice fini dans C^U. Cet indice divise $[U : V]$, et lui est égal si et seulement si V est distingué dans U avec U/V abélien.

Noter que si U est le groupe de Galois absolu d'un corps K et V correspond à une extension L de K, alors W correspond à la plus grande extension abélienne de K incluse dans L. Quand V est un sous-groupe distingué de U, on notera $(a, U/V)$ l'image d'un élément a de C^U par l'application de réciprocité $C^U \to (U/V)^{\mathrm{ab}}$ de a).

Démonstration : a) C'est la proposition 6.20 (qui est un corollaire de Tate-Nakayama) appliquée à la formation de classes (U, C) et au sous-groupe V de U, avec $r = -2$ et $M = \mathbf{Z}$.

b) L'inclusion $N_{U/V}(C^V) \subset N_{U/W}(C^W)$ résulte de la transitivité des normes. Soit $a \in N_{U/W}(C^W)$, montrons que $a \in N_{U/V}(C^V)$. Soit Z un sous-groupe ouvert de U inclus dans V et distingué dans U. Posons $J = U/Z$ et $H = V/Z$. Alors $W/Z = J'.H$, où J' est le sous-groupe dérivé de J. L'image $(a, U/W)$ de a dans $U/W = J/J'H$ est triviale, ce qui veut dire que $(a, U/Z) \in (J/J')$ provient de H/H'. On a un diagramme commutatif (qui résulte de la définition de l'application de réciprocité comme inverse de l'application "cup-produit par la classe fondamentale", du fait que les classes fondamentales sont compatibles aux restrictions, et de la formule de compatibilité de la proposition 2.13, b).

$$\begin{array}{ccc} C^V & \xrightarrow{N_{U/V}} & C^U \\ {\scriptstyle (.,V/Z)}\downarrow & & \downarrow{\scriptstyle (.,U/Z)} \\ H/H' & \longrightarrow & J/J' \end{array}$$

Comme C^V se surjecte sur H/H' par l'application de réciprocité, le diagramme donne alors l'existence d'un a' dans C^V tel que $(a, U/Z) = (N_{U/V}a', U/Z)$. Ainsi $N_{U/V}a' - a$ s'écrit $N_{U/Z}(a'')$ avec $a'' \in C^Z$, d'où

$$a = N_{U/V}(a' - N_{Z/V}(a''))$$

c) D'après b), on a $C^U/N_{U/V}(C^V) = C^U/N_{U/W}(C^W)$, qui est fini d'indice $[U : W]$ d'après a). Le résultat en découle via la transitivité des normes.

□

Proposition 7.3 *Soit U un sous-groupe ouvert de G. On note Ab_U l'ensemble des sous-groupes ouverts V de G tels que V soit distingué dans U et U/V soit abélien (i.e. V contienne le sous-groupe dérivé $D(U)$ de U). Pour V dans Ab_U, notons $I_V = N_{U/V}C^V$. Alors l'application $V \mapsto I_V$ est une bijection croissante de Ab_U sur l'ensemble des sous-groupes de normes de C^U. On a de plus, pour tous V, W de Ab_U :*

$$I_{V\cap W} = I_V \cap I_W$$

et tout sous-groupe de C^U qui contient un groupe de normes est un groupe de normes.

Démonstration : Notons déjà que si V et W sont dans Ab_U, alors $V \cap W$ l'est encore. Le fait que $V \mapsto I_V$ soit crossante résulte de la transitivité des normes, ce qui donne en particulier l'inclusion $I_{V\cap W} \subset I_V \cap I_W$. Réciproquement si $a \in I_V \cap I_W$, alors l'élément $(a, U/(V \cap W)$ de $U/(V \cap W)$ a une image triviale dans U/V et U/W, donc est trivial. Si maintenant $I_V \supset I_W$, alors $I_{V\cap W} = I_W$ donc $V \cap W$ et W ont même indice dans U, ce qui donne $V \supset W$. On obtient finalement bien que la correspondance est bijective.

Soit I un sous-groupe de C^U qui contient un sous-groupe de normes $N_{U/V}C^V$. On peut supposer (via la proposition 7.2, b) que U/V est un groupe abélien. Alors l'image de I par l'application de réciprocité $C^U \to U/V$ est un sous-groupe W/V, où W est un sous-groupe ouvert de U qui contient V. On en déduit que I est le noyau de l'application de réciprocité $C^U \to U/W$, d'où on déduit que $I = N_{U/W}C^W$ est un groupe de normes.

□

Pour obtenir un théorème d'existence lié aux sous-groupes de normes, il est nécessaire de faire des hypothèses supplémentaires sur la formation de classes (C, G). En particulier, on va supposer qu'on a une topologie sur

chaque C^U, telle que pour $V \subset U$ la topologie sur C^U soit celle induite par $C^V \supset C^U$, et pour tout s de G l'application $C^U \to C^{sus^{-1}}, a \mapsto s.a$ soit continue (ce qui implique que $N_{U/V} : C^V \to C^U$ est continue). L'exemple typique est celui où $G = \mathrm{Gal}\,(\overline{K}/K)$ est le groupe de Galois d'un corps p-adique K et $C = K^*$. Alors les sous-groupes ouverts U correspondant aux extensions finies galoisiennes L de K, et on munit $C^U = L^*$ de la topologie usuelle associée à sa valuation. L'application $N_{U/V}$ est la norme (au sens habituel) $N_{L/K} : L^* \to K^*$.

Hypothèse 1 (H1) : Pour toute paire $V \subset U$ de sous-groupes ouverts de G, la norme $N_{U/V} : C^V \to C^U$ a une image fermée et un noyau compact (si on travaille avec des groupes localement compacts et dénombrables à l'infini, cela signifie que $N_{U/V}$ est une application propre).

Il résulte de (H1) que $N_{U/V}C^V$ est un sous-groupe ouvert de C^U : en effet il est d'indice fini d'après la proposition 7.2, c).

Définition 7.4 Soit U un sous-groupe ouvert de G. On note D_U l'intersection de tous les sous-groupes de normes de U. C'est aussi le noyau de l'application de réciprocité $C^U \to U^{\mathrm{ab}}$.

Pour $U = G$, nous avions déjà rencontré D_G, groupe des normes universelles de C^G, au paragraphe 6.4.

Proposition 7.5 *Supposons (H1) vérifiée. Alors pour toute paire $V \subset U$ de sous-groupes ouverts de U, on a $N_{U/V}D^V = D^U$.*

Démonstration : L'inclusion $N_{U/V}D_V \subset D_U$ résulte de la transitivité des normes. Soit inversement $a \in D_U$. Pour tout sous-groupe ouvert W de V, notons $K(W)$ l'ensemble des b de C^V de norme a (dans E), et qui sont norme d'un élément de W. L'hypothèse (H1) dit que $K(W)$ est compact ; il est non vide car $a \in D_U$, donc a s'écrit comme norme d'un élément c de C^W et on peut prendre $b = N_{V/W}(c)$ via la transitivité des normes. Comme la famille des $K(W)$ est filtrante décroissante, son intersection sur tous les W est non vide. Or un élément b de cette intersection vérifie clairement $b \in D_V$ et $N_{U/V}(b) = a$.

□

Hypothèse 2 (H2) : Pour tout nombre premier p et tout sous-groupe[36] ouvert U de G, le noyau de la multiplication par p dans C^U est compact. De

36. Il semble que demander seulement (comme dans [13], paragraphe XI.5) cette propriété pour $U \subset U_p$ ne soit pas suffisant pour déduire la compacité de $L(V)$ dans la preuve de la proposition qui suit.

plus, il existe un sous-groupe ouvert U_p de G tel que pour tout sous-groupe ouvert $V \subset U_p$, l'application $\varphi_p : x \mapsto px$ de C^V dans C^V vérifie : l'image de φ_p contient D_V.

Proposition 7.6 *Supposons (H1) et (H2) vérifiées. Alors pour tout sous-groupe ouvert U de G, le groupe D_U est divisible et égal à $\bigcap_{n>0} nC^U$.*

Démonstration : Montrons d'abord que $D_U = pD_U$ pour tout p premier. Soit $a \in D_U$ et soit V un sous-groupe ouvert de U inclus dans U_p. Soit $L(V)$ l'ensemble des b de C^U tels que $pb = a$ et $b \in N_{U/V}C^V$. Alors $L(V)$ est non vide : en effet d'après la proposition 7.5, on peut écrire $a = N_{U/V}(a')$ avec $a' \in D_V$. Par (H2), on peut écrire $a' = pb'$ avec $b' \in C^V$ d'où $a = pb$ avec $b = N_{U/V}(b')$. De plus $L(V)$ est compact car il se déduit par translation de l'intersection du sous-groupe de p-torsion de C^U (qui est compact par (H2)) et de l'image de $N_{U/V}$ (qui est fermée par (H1)). Le même argument que dans la proposition 7.5 donne alors que l'intersection sur V des $L(V)$ est non vide, ce qui prouve l'assertion.

On en déduit déjà que D_U est divisible, donc inclus dans $\bigcap_{n>0} nC^U$. Réciproquement si a est dans cette intersection et si V est un sous-groupe fermé d'indice n de U, alors si $a = nb$ avec $b \in C^U$, on a $a = N_{U/V}b$ donc finalement $a \in D_U$.

□

Hypothèse 3 (H3) : Pour tout sous-groupe ouvert U de G, il existe un sous-groupe compact H de C^U tel que tout sous-groupe fermé d'indice fini de C^U qui contient H est un groupe de normes.

Theorème 7.7 *Supposons que (H1), (H2), et (H3) soient satisfaites. soit U un sous-groupe ouvert de G. Alors un sous-groupe de C^U est un sous-groupe de normes si et seulement s'il est fermé d'indice fini dans C^U.*

Démonstration : On sait déjà qu'un sous-groupe de normes est fermé d'indice fini. Soit réciproquement I un sous-groupe fermé d'indice fini n de C^U. Alors tout élément de C^U/I est annulé par n, on a $nC^U \subset I$ d'où $D_U \subset I$ d'après la proposition 7.6. Ainsi l'intersection des $N \cap H$ pour N sous-groupe de normes de C^U est incluse dans I (puisque c'est un sous-groupe de D_U). Comme tous les $N \cap H$ sont compacts et I est un sous-groupe ouvert de C^U, I contient l'un des $N \cap H$: en effet si I' désigne le complémentaire de I dans C^U, les $I' \cap N$ forment une famille filtrante décroissante de compacts dont l'intersection est vide, donc l'un de ces compacts est vide. On a alors

$$N \cap (H + (N \cap I)) \subset I$$

car si a est dans cette intersection, il s'écrit $a = a_1 + a_2$ avec $a_1 \in H$ et $a_2 \in N \cap I$; alors $a_1 = a - a_2$ est dans $N \cap H$, qui est inclus dans I par choix de N.

Maintenant $H + (N \cap I)$ est fermé [37] dans C^U, d'indice fini (il contient $N \cap I$), et contient H donc c'est un groupe de normes par l'hypothèse (H3). D'après la proposition 7.3, $N \cap (H + (N \cap I))$ est un groupe de normes, donc aussi I (qui le contient).

□

7.2. Application aux corps p-adiques

On commence par un lemme sur les *symboles*. Soit k un corps de groupe de Galois absolu Γ_k. Soit p un nombre premier différent de $\mathrm{Car}\, k$, et tel que k contienne une racine primitive p-ième ζ de l'unité. Soit $a \in k^*$; le choix de ζ permet de définir un caractère χ_a de $\Gamma_k = \mathrm{Gal}\,(\bar{k}/k)$ associé à a (en identifiant l'image $\bar{a}$ de a dans $k^*/k^{*p} = H^1(k, \mu_p)$ à un élément de $H^1(k, \mathbf{Z}/p)$). En particulier χ_a est un caractère de Γ_k dont le noyau est $\mathrm{Gal}\,(\bar{k}/k(a^{1/p}))$, et $\mathrm{Gal}\,(k(a^{1/p})/k)$ est un groupe cyclique trivial ou d'ordre p.

Définition 7.8 Soient a, b dans k^*. On définit le *symbole* $(a, b) \in (\mathrm{Br}\, k)[p]$ comme le cup-produit de $\chi_a \in H^2(k, \mathbf{Z}) = H^1(k, \mathbf{Q}/\mathbf{Z})$ avec $b \in H^0(k, \bar{k}^*) = k^*$. C'est une application bilinéaire du groupe multiplicatif $k^* \times k^*$ dans le groupe additif $\mathrm{Br}\, k$.

Lemme 7.9 *a) Si b est une norme de l'extension $k(a^{1/p})/k$, alors $(a, b) = 0$.*

b) On a $(a, -a) = 0$, $(a, 1 - a) = 0$, et $(a, b) = -(b, a)$ pour tous a, b de k^*.

c) Supposons que k soit un corps local de caractéristique zéro. Alors si un élément b de k^* vérifie $(a, b) = 0$ pour tout a de k^*, on a $b \in k^{*p}$.

Démonstration : a) Soit $L = k(a^{1/p})$. On peut supposer que L est une extension non triviale de K. Posons $G = \mathrm{Gal}\,(L/k)$. Alors χ_a s'identifie à un élément de $H^2(G, \mathbf{Z})$, de sorte que $\chi_a \cup b$ est aussi le cup-produit de χ_a avec l'image de b dans $\widehat{H}^0(G, L^*) = k^*/N_{L/k}L^*$. Le résultat en découle.

b) On observe que $N_{L/k}(-\zeta.a^{1/p})$ (qui est le produit des $-\zeta^i a^{1/p}$ pour $i = 0, ..., p-1$) vaut $-a$ donc $-a$ est une norme de L/k, d'où le premier

37. Plus généralement si A est un groupe topologique abélien et F, H sont respectivement un sous-groupe fermé et un sous-groupe compact de A, alors $F+H$ est fermé dans A comme image réciproque dans A du compact $H/(H \cap F)$ de A/F, lequel est fermé dans A/F parce que A/F est séparé.

point. Le deuxième point s'obtient de la même manière en observant que $N_{L/k}(1-\zeta.a^{1/p})=1-a$. Enfin, on a par le premier point

$$(a,b)+(b,a)=(a,-ab)+(b,-ba)=(ab,-ab)=0$$

d'où le troisième point.

c) D'après b), on a $(b,a)=0$, soit $\chi_b \cup a=0$. D'après le corollaire 6.16, on a $\chi_b(\omega_k(a))$ pour tout a de k^*. Ceci implique $\chi_b=0$ (par densité de l'image de l'application de réciprocité $\omega_k : k^* \to \Gamma_k^{\mathrm{ab}}$), ou encore que la classe de b dans $k^*/k^{*p} \simeq H^1(k,\mathbf{Z}/p)$ est nulle.

□

On va maintenant pouvoir déduire des résultats du paragraphe précédent le *théorème d'existence* pour les corps p-adiques :

Theorème 7.10 *Soit K un corps p-adique de clôture algébrique $\overline{K}$. Soit H un sous-groupe fermé d'indice fini de K^*. Alors il existe une unique extension abélienne finie $L \subset \overline{K}$ de K telle que $N_{L/K}L^*=H$.*

Démonstration : L'unicité résulte de ce que si L et F sont deux extensions abéliennes finies de K (incluses dans $\overline{K}$) avec $NL^*=NF^*$, les images réciproques de $\mathrm{Gal}\,(K^{\mathrm{ab}}/L)$ et $\mathrm{Gal}\,(K^{\mathrm{ab}}/F)$ par l'application de réciprocité $\omega : K^* \to \mathrm{Gal}\,(K^{\mathrm{ab}}/K)$ sont les mêmes, donc par la théorie de Galois on a $L=F$.

Pour l'existence, on va appliquer le théorème 7.7 à la formation de classes associée à $\Gamma=\mathrm{Gal}\,(\overline{K}/K)$ et $C=\overline{K}^*$, tous les groupes L^* (pour L extension finie de K) étant munis de la topologie associée à la valuation. Il faut vérifier les hypothèses (H1), (H2), et (H3). Pour cela on peut supposer que le groupe U qui intervient dans ces hypothèses est Γ (vu que tout sous-groupe ouvert de Γ est aussi le groupe de Galois d'un corps p-adique).

(H1) résulte du fait que la norme $L^* \to K^*$ est propre car tout sous-ensemble compact de K^* est contenu dans une union finie de translatés du groupe des unités U_K, et l'image réciproque de U_K par la norme est U_L (qui est compact), via le fait que si $x \in L^*$, alors $v_K(N_{L/K}(x))=f.N_L(x)$, où f est le degré résiduel de l'extension L/K ([13], chapitre II, corollaire 4 p. 39).

Pour (H2), on note déjà que pour tout corps p-adique K et tout nombre premier l (distinct ou non de p), le noyau de $x \mapsto x^l$ de K^* dans lui-même est fini, donc compact. On considère le corps K_l obtenu en adjoignant à K toutes les racines l-ièmes de l'unité, et on pose $U_l=\mathrm{Gal}\,(\overline{K}/K_l)$. Soit alors $V \subset U_l$ un sous-groupe ouvert de G, il correspond à une extension finie L de K qui contient K_l et l'application φ_l est l'application $x \mapsto x^l$ de L^* dans L^*.

Si $x \in L^*$ est une norme universelle, alors le symbole (a, x) est nul pour tout a de L^* d'après le lemme 7.9 a), donc $x \in L^{*^l}$ d'après le lemme 7.9, c).

Pour (H3), on prend pour H le groupe des unités U_K. Alors les sous-groupes d'indice fini I de K^* qui contiennent H sont les images réciproques par la valuation des sous-groupes $n\mathbf{Z}$ de $\mathbf{Z}$ pour $n \in \mathbf{N}$ (en effet si I est un tel sous-groupe, alors $v(I)$ est un sous-groupe de $\mathbf{Z}$, donc s'écrit $n\mathbf{Z}$; mais alors I contient l'image réciproque de $n\mathbf{Z}$ puisqu'il contient U_K et au moins un élément de valuation m pour tout entier m multiple de n). Montrons un lemme :

Lemme 7.11 *Soit K un corps p-adique de groupe de Galois absolu $\Gamma_K = \mathrm{Gal}\,(\overline{K}/K)$. Soit $\omega_K : K^* \to \Gamma_K^{\mathrm{ab}}$ l'application de réciprocité. Alors :*

a) Si K' est une extension finie non ramifiée (donc cyclique) de K, on a, pour tout x de K^*,

$$\omega_{K'/K}(x) = F_K^{v(x)} \tag{8}$$

où F_K est le générateur canonique de $\mathrm{Gal}\,(K'/K)$.

b) L'image par l'application de réciprocité ω_K du groupe des unités U_K de l'anneau des entiers $\mathcal{O}_K$ est exactement le sous-groupe d'inertie abélien $I_K^{\mathrm{ab}} = \mathrm{Gal}\,(\Gamma_K^{\mathrm{ab}}/K_{\mathrm{nr}})$ de Γ_K^{ab}.

Démonstration : a) résulte facilement du fait que pour tout caractère χ de $\mathrm{Gal}\,(K'/K)$, on a

$$\chi(\omega_{K'/K}(x)) = j_K(x \cup \chi)$$

(proposition 6.15) et de la définition de j_K donnée avant la proposition 5.8.

Pour b), il suffit de faire la vérification à niveau fini ; plus précisément soit L une extension finie abélienne de groupe G de K, il s'agit de montrer que l'image de U_K par l'application de réciprocité $\omega_{L/K} : K^* \to G$ est exactement le sous-groupe d'inertie I de G. Écrivons $I = \mathrm{Gal}\,(L/K')$, où K' est l'extension maximale non ramifiée de K incluse dans L. Identifiant $\mathrm{Gal}\,(K'/K)$ avec le groupe de Galois de l'extension résiduelle $\mathrm{Gal}\,(\kappa'/\kappa)$, on déduit de a) que pour $x \in U_K$, l'image de x par $\omega_{K'/K}$ est triviale, ce qui signifie que $\omega_{L/K}(x)$ est dans $I = \mathrm{Gal}\,(L/K')$.

Soit réciproquement $t \in I$; comme $\omega_{L/K}$ est surjective (de noyau $N_{L/K}L^*$), on peut écrire $t = \omega_{L/K}(a)$ avec $a \in K^*$. Posons $m = [K' : K] = [\kappa' : \kappa]$ (c'est le degré résiduel de l'extension L/K). Comme t est trivial sur K', la formule (8) donne que m divise $v(a)$. On sait que pour tout $b \in L^*$, on a $v(N_{L/K}(b)) = mv(b)$. Choisissons b dans L^* de valuation $v(a)/m$, on obtient alors que a et $N_{L/K}(b)$ ont même valuation. Posons alors $u = a/N_{L/K}(b)$,

alors $u \in U_K$ et $t = \omega_{L/K}(a) = \omega_{L/K}(u)$, ce qui montre bien que t est dans l'image de U_K par $\omega_{L/K}$.

□

On peut maintenant terminer la preuve du théorème 7.10. Soit $I \subset K^*$ l'image réciproque de $n\mathbf{Z}$ par la valuation. Soit K' l'extension non ramifiée de K de degré n. Alors d'après le lemme 7.11 a), le noyau de $\omega_{K'/K}$ est exactement I, puisque F_K engendre un groupe d'ordre n. Comme on sait que ce noyau est $N_{K'/K}(K'^*)$, on obtient bien que I est un groupe de normes comme on voulait.

□

On en déduit la structure de l'abélianisé du groupe de Galois d'un corps p-adique, résultat qui avait été annoncé après le théorème 6.13.

Corollaire 7.12 *a) L'intersection de tous les sous-groupes de normes de K^* est réduite à $\{1\}$ (autrement dit : il n'y a pas de norme universelle autre que 1).*

b) L'application de réciprocité induit un isomorphisme du groupe des unités U_K sur le "groupe d'inertie abélien" $\mathrm{Gal}\,(K^{\mathrm{ab}}/K_{\mathrm{nr}})$.

c) Le groupe $\mathrm{Gal}\,(K^{\mathrm{ab}}/K)$ *est isomorphe au complété profini de K^* : c'est une extension de $\widehat{\mathbf{Z}}$ par U_K.*

Remarque : La structure de K^* (qui est isomorphe au produit direct de U_K et de $\mathbf{Z}$ via le choix d'une uniformisante) implique que tous ses sous-groupes d'indice fini sont fermés. Il n'en va plus de même si K est un corps local de caractéristique p (pour lequel tous les énoncés précédents sont valables à condition de se limiter aux sous-groupes fermés d'indice fini).

Démonstration : a) Soit π une uniformisante de K^*. Pour m, n dans $\mathbf{N}^*$, notons $V_{m,n}$ le sous-groupe de K^* engendré par π^m et U_K^n (ce dernier groupe est l'ensemble des $1 + \pi^n x$ avec x dans U_K). Ce sont des sous-groupes fermés d'indice fini, et leur intersection est $\{1\}$, d'où le résultat avec le théorème d'existence.

b) On a déjà vu (lemme 7.11 b)) que l'application de réciprocité induit une surjection de U_K sur le groupe d'inertie abélien I_K^{ab}. L'injectivité résulte de a).

c) La première assertion résulte immédiatement du théorème d'existence et des propriétés de l'application de réciprocité vues en 6.3. La deuxième vient de b) et de ce que $\mathrm{Gal}\,(K_{\mathrm{nr}}/K)$ est isomorphe à $\widehat{\mathbf{Z}}$.

□

Ces résultats, combinés au théorème général de dualité pour une formation de classes, vont maintenant nous permettre de démontrer un théorème de dualité pour la cohomologie galoisienne d'un corps p-adique.

7.3. Le théorème de dualité pour un corps p-adique

Dans tout ce paragraphe, on désigne par K un corps p-adique et on pose $\Gamma = \mathrm{Gal}\,(\overline{K}/K)$. On a défini au paragraphe 6.6. des applications α^r, pour lesquelles on dispose du théorème de dualité 6.29, que nous allons maintenant appliquer.

Proposition 7.13 *Soit M un Γ-module discret de type fini. Alors les applications*

$$\alpha^r(\Gamma, M) : \mathrm{Ext}^r_\Gamma(M, \overline{K}^*) \to H^{2-r}(\Gamma, M)^*$$

sont des isomorphismes pour tout $r \geq 1$. Si de plus M est fini, alors α^0 est également un isomorphisme (de groupes finis).

Démonstration : On applique le théorème de dualité 6.29 à la formation de classes $(\Gamma, \overline{K}^*)$. Soit $U = \mathrm{Gal}\,(\overline{K}/L)$ un sous-groupe ouvert de Γ. Alors $\alpha^1(U, \mathbf{Z}/n)$ est l'application

$$L^*/{L^*}^n \to U^{\mathrm{ab}}/n$$

induite par l'application de réciprocité ω_L. Comme ω_L induit un isomorphisme du complété profini de L^* sur U^{ab}, on en déduit que $\alpha^1(U, \mathbf{Z}/n)$ est un isomorphisme, et le théorème 6.29 dit alors que $\alpha^r(\Gamma, M)$ est bien un isomorphisme pour $r \geq 1$.

Si maintenant M est fini d'ordre s il suffit de vérifier que $\alpha^0(U, \mathbf{Z}/n)$ est bijective pour tout n divisant s et tout U suffisamment petit (voir la remarque après la preuve du théorème 6.29) On peut donc supposer que L contient les racines n-ièmes de l'unité. Alors on a des flèches

$$\mu_n(L) \to H^2(L, \mathbf{Z}/n)^* \to (U^{\mathrm{ab}})[n]$$

et on sait que la flèche composée (induite par l'application de réciprocité) est un isomorphisme, via le corollaire 7.12 et le fait que L^* et son complété profini ont même sous-groupe de n-torsion.

On en déduit que la première flèche (qui est $\alpha^0(U, \mathbf{Z}/n)$) est injective, mais comme $H^2(L, \mathbf{Z}/n) = H^2(L, \mu_n) = (\mathrm{Br}\, L)[n] \simeq \mathbf{Z}/n$ est de cardinal n, on en déduit que $\alpha^0(U, \mathbf{Z}/n)$ est également surjective.

□

Theorème 7.14 (Tate) *Soit K un corps p-adique. Soit M un Γ_K-module fini de dual $M^D = \mathrm{Hom}(M, \overline{K}^*)$. Alors pour tout $r \geq 0$ le cup-produiit*

$$H^r(K, M) \times H^{2-r}(K, M^D) \to \mathrm{Br}\, K = \mathbf{Q}/\mathbf{Z}$$

est un accouplement parfait de groupes finis.

Démonstration : On sait déjà que tous les groupes qui interviennent sont finis (théorème 5.13). Par ailleurs on a la compatibilité des accouplements définis par les Ext et les cup-produits (proposition 6.26). Il suffit alors d'appliquer le résultat précédent en remarquant que

$$\mathrm{Ext}^r_\Gamma(M, \overline{K}^*) = H^r(K, M^D)$$

pour tout $r \geq 0$ via la proposition 6.25, vu que $\mathrm{Ext}^i_{\mathbf{Z}}(M, \overline{K}^*) = 0$ pour $i > 0$ par divisibilité de $\overline{K}^*$ (ce point est essentiel !).

□

Remarque : Supposons seulement que M est de type fini. Alors pour $r = 1$, l'énoncé est valable tel quel (avec la même preuve). Pour $r = 0$ et $r = 2$, il faut remplacer les H^0 par leurs complétés profinis, voir l'exercice 4 de ce chapitre.

Le théorème de dualité permet de préciser la dimension cohomologique stricte de Γ :

Theorème 7.15 *Soit K un corps p-adique. Alors la dimension cohomologique stricte de K est 2.*

Démonstration : On utilise la proposition 3.23. Soit U un sous-groupe ouvert de Γ. On a alors $H^3(U, \mathbf{Z}) = H^2(U, \mathbf{Q}/\mathbf{Z})$ comme on l'a déjà vu. Alors en appliquant le théorème 7.14 à $M = \mathbf{Z}/n$ et en passant à la limite, on obtient que $H^2(U, \mathbf{Q}/\mathbf{Z})$ est dual de $\varprojlim_n \mu_n(L)$, où L est l'extension finie de K correspondant à U (ce dernier groupe est le *module de Tate* du groupe $\mu(L)$ des racines de l'unité dans L^*). Mais L (qui est un corps p-adique) ne contient qu'un nombre fini de racines de l'unité (parce que U_L est isomorphe au produit d'un groupe fini et de $\mathbf{Z}_p^r$, ou encore via la filtration du groupe des unités) donc $H^0(L, \mu) = \mu(L)$ est fini. On en conclut que $\varprojlim_n \mu_n(L) = 0$, ce qui conclut la preuve.

□

7.4. Notion de module dualisant

Soit G un groupe profini de dimension cohomologique $n < +\infty$. On considère le foncteur $A \mapsto H^n(G, A)^*$ de la catégorie C_G^f des G-modules discrets finis vers la catégorie des groupes abéliens (rappelons que $^* := \mathrm{Hom}(., \mathbf{Q}/\mathbf{Z})$). Il se trouve qu'on a un résultat général d'algèbre homologique (cf. [14], paragraphe I.3.5., lemme 6) qui garantit, sous des hypothèses assez faibles, que ce foncteur est représentable par un G-module discret de torsion. Plus précisément :

Theorème 7.16 *Soit G un groupe profini de dimension cohomologique $n < +\infty$. On suppose que pour tout $A \in C_G^f$, le groupe $H^n(G, A)$ est fini. Alors il existe un G-module discret de torsion I tels que les foncteurs $\mathrm{Hom}_G(., I)$ et $H^n(G, .)^*$ (de C_G^f dans $\mathcal{A}b$) soient isomorphes. On dit que I est le module dualisant du groupe profini G.*

On a un théorème et des définitions analogues avec la p-dimension cohomologique (en se limitant aux modules de torsion p-primaire).

Il est en réalité possible de montrer l'existence du module dualisant (et également d'en donner une description explicite) sans l'hypothèse de finitude sur $H^n(G, A)$, mais cela demande pas mal d'efforts (voir [14], partie I, annexe 1, ou encore [12], paragraphe III.4).

Par ailleurs, il est parfois possible de calculer le module dualisant assez facilement si on connaît son existence, et d'en déduire rapidement des théorèmes de dualité. Cette méthode fonctionne bien pour le groupe de Galois d'un corps p-adique (voir exercice 1 de ce chapitre) et permet de se passer de résultats nettement plus compliqués (Tate-Nakayama, théorème d'existence). Son inconvénient principal est que cela ne marche pas bien si le module dualisant n'est pas un groupe divisible (dans le cas du groupe de Galois d'un corps p-adique K, le module dualisant consiste en toutes les racines de l'unité de $\overline{K}$), ce qui fait que dans le cas des corps de nombres on est obligé d'avoir recours aux résultats plus sophistiqués du chapitre 6..

7.5. Caractéristique d'Euler-Poincaré, application à la cohomologie non ramifiée

Soit K un corps p-adique de groupe de Galois absolu $\Gamma = \mathrm{Gal}\,(\overline{K}/K)$. Soit A un Γ-module fini. Notons $h^i(A)$ le cardinal du groupe fini $H^i(K, A) = H^i(\Gamma, A)$.

Définition 7.17 La *caractéristique d'Euler-Poincaré* de A est le nombre rationnel strictement positif

$$\chi(A) := \frac{h^0(A).h^2(A)}{h^1(A)}$$

Si $0 \to A \to B \to C \to 0$ est une suite exacte de Γ-modules, alors on obtient $\chi(B) = \chi(A).\chi(C)$ via la suite exacte longue de cohomologie. Un théorème de Tate ([14], Théorème 5 p. 109) donne l'égalité

$$\chi(A) = 1/[\mathcal{O}_K : a\mathcal{O}_K]$$

où a est le cardinal de A (en particulier $\chi(A)$ ne dépend que de a). La démonstration de ce théorème est longue et fait appel à des résultats fins de la théorie des représentations des groupes finis. Nous allons donc seulement traiter un cas particulier plus simple, qui suffira pour l'application à la cohomologie non ramifiée.

Proposition 7.18 *Supposons que le cardinal a de A soit premier à p. Alors $\chi(A) = 1$.*

Démonstration : Soit U le groupe d'inertie $\mathrm{Gal}\,(\overline{K}/K_{\mathrm{nr}})$. Le quotient Γ/U est isomorphe à $\widehat{\mathbf{Z}}$. D'autre part la théorie des groupes de ramification donne que U possède un unique p-Sylow U_p qui est distingué dans U et le quotient $V := U/U_p$ est isomorphe à $\mathbf{Z}'_p := \prod_{l \neq p} \mathbf{Z}_l$. Plus précisément on a $U_p = \mathrm{Gal}\,(\overline{K}/K_{\mathrm{mr}})$, où K_{mr} est l'extension maximale modérément ramifiée de K.

Lemme 7.19 *Le groupe $H^i(U, A)$ est fini pour tout $i \geq 0$ et nul si $i \geq 2$.*

Démonstration : Le cas $i = 0$ est immédiat. On sait (théorème 5.1) que U est de dimension cohomologique ≤ 1 d'où $H^i(U, A) = 0$ pour $i \geq 2$. D'autre part $H^i(U_p, A) = 0$ pour $i \geq 1$ car U_p est un pro-p-groupe et le cardinal de A est premier à p. Ainsi $H^1(U, A) = H^1(V, A^{U_p})$ via la suite exacte de restriction-inflation et on est ramené à montrer que $H^1(V, A^{U_p})$ est fini. En décomposant le V-module fini A^{U_p} en somme directe finie de ses composantes l-primaires (pour l premier différent de p), on voit qu'il reste à vérifier que $H^1(\mathbf{Z}_l, B)$ est fini [38] pour tout module fini l-primaire B. Soit W un sous-groupe ouvert de $\mathbf{Z}_l$ qui agit trivialement sur B, alors via la suite de restriction inflation il suffit de voir que $H^1(W, B)$ est fini (vu que $\mathbf{Z}_l/W$ est

38. Voir l'exercice 8 du chapitre 3 pour une généralisation.

fini, donc aussi $H^1(\mathbf{Z}_l/W, B))$ et donc que $\mathrm{Hom}_c(W, B)$ est fini. Mais si B est de cardinal l^m, alors $\mathrm{Hom}_c(W, B) = \mathrm{Hom}(W/l^m W, B)$ est fini car $W/l^m W$ est fini (le sous-groupe ouvert W de $\mathbf{Z}_l$ contient $N\mathbf{Z}_l$ pour N assez grand, donc $W/l^m W$ est un sous-quotient de $\mathbf{Z}_l/l^{m+N}\mathbf{Z}_l$ qui est fini).

□

Reprenons la preuve de la proposition 7.18. La suite exacte des premiers termes de la suite spectrale de Hochschild-Serre

$$H^i(\Gamma/U, H^j(U, A)) \Rightarrow H^{i+j}(\Gamma, A)$$

donne, compte tenu des résultats ci-dessus :

$$H^0(K, A) = H^0(\widehat{\mathbf{Z}}, H^0(U, A)); \quad H^2(K, A) = H^1(\widehat{\mathbf{Z}}, H^1(U, A))$$

et une suite exacte

$$0 \to H^1(\widehat{\mathbf{Z}}, H^0(U, A)) \to H^1(K, A) \to H^0(\widehat{\mathbf{Z}}, H^1(U, A)) \to 0$$

Pour conclure, il suffit d'appliquer le lemme suivant aux $\widehat{\mathbf{Z}}$-modules finis $H^0(U, A)$ et $H^1(U, A)$:

Lemme 7.20 *Soit M un $\widehat{\mathbf{Z}}$-module fini. Alors $H^0(\widehat{\mathbf{Z}}, M)$ et $H^1(\widehat{\mathbf{Z}}, M)$ sont finis de même cardinal.*

Preuve du lemme : Soit F le générateur topologique canonique de $\widehat{\mathbf{Z}}$. Soit $s = mn$, où n et m sont des entiers choisis tels que F^m opère trivialement sur M et $M = M[n]$. Alors on peut voir M comme un $\mathbf{Z}/s$-module et la norme $N_{\mathbf{Z}/s} : M \to M$ est l'application nulle vu que pour tout x de M, on a

$$N_{\mathbf{Z}/s}(x) = (1 + F + ... + F^{mn-1})x = n(1 + F + ... + F^{m-1}).x = 0$$

Alors $H^0(\widehat{\mathbf{Z}}, M)$ est le noyau de l'endomorphisme $F - 1$ de M, tandis que $H^1(\widehat{\mathbf{Z}}, M)$ est ici simplement la limite inductive sur i (et on peut se limiter aux i multiples de s) des $H^1(\mathbf{Z}/i, M)$. Mais $H^1(\mathbf{Z}/i, M) = \widehat{H}^{-1}(\mathbf{Z}/i, M)$ (théorème 2.10) est le conoyau de $F-1$ puisque $N_{\mathbf{Z}/i}$ est nulle pour i multiple de s, d'où le résultat.

□

Définition 7.21 Soit A un Γ-module. On dit que A est *non ramifié* si le groupe $U = \mathrm{Gal}\,(\overline{K}/K_{\mathrm{nr}})$ opère trivialement sur A. Dans ce cas on définit les groupes $H^i_{\mathrm{nr}}(K, A) := H^i(\mathrm{Gal}\,(K_{\mathrm{nr}}/K), A)$.

Proposition 7.22 *Soit A un Γ-module fini et non ramifié. Alors on a les égalités $H^0_{\mathrm{nr}}(K, A) = H^0(K, A)$ et $H^i_{\mathrm{nr}}(K, A) = 0$ pour $i \geq 2$. Le groupe $H^1_{\mathrm{nr}}(K, A)$ s'identifie à un sous-groupe de $H^1(K, A)$ et son cardinal est celui de $H^0(K, A)$.*

Démonstration : L'assertion sur H^0 est immédiate, celle sur H^i pour $i \geq 2$ résulte de ce que $\mathrm{cd}(\widehat{\mathbf{Z}}) = 1$. Enfin l'assertion sur H^1 vient du lemme 7.20 appliqué à A.

□

Theorème 7.23 *Soit A un Γ-module fini, non ramifié, d'ordre premier à p. Alors son dual A' possède ces mêmes propriétés. De plus, dans la dualité entre $H^1(K, A)$ et $H^1(K, A')$, chacun des sous-groupes $H^1_{\mathrm{nr}}(K, A)$ et $H^1_{\mathrm{nr}}(K, A')$ est l'orthogonal de l'autre.*

Démonstration : Soit μ le Γ-module des racines de l'unité dans $\overline{K}^*$ (c'est le module dualisant de Γ) et soit $\bar{\mu}$ le sous-module formé des éléments d'ordre premier à p. Comme les racines n-ièmes de l'unité pour n premier à p sont dans K_{nr}, le Γ-module $\bar{\mu}$ est non ramifié, ce qui implique immédiatement que $A' = \mathrm{Hom}(A, \bar{\mu})$ est non ramifié. Le cup-produit

$$H^1_{\mathrm{nr}}(K, A) \times H^1_{\mathrm{nr}}(K, A') \to H^2(k, \mu)$$

se factorise par $H^2_{\mathrm{nr}}(k, \bar{\mu})$ qui est nul, ce qui implique que $H^1_{\mathrm{nr}}(K, A)$ et $H^1_{\mathrm{nr}}(K, A')$ sont orthogonaux. Pour conclure il suffit de montrer que le cardinal $h^1(A')$ de $H^1(K, A')$ est le produit $h^1_{\mathrm{nr}}(A).h^1_{\mathrm{nr}}(A')$ des cardinaux de $H^1_{\mathrm{nr}}(K, A)$ et $H^1_{\mathrm{nr}}(K, A')$. En effet cela donnera que l'homomorphisme

$$H^1_{\mathrm{nr}}(K, A) \to (H^1(K, A')/H^1_{\mathrm{nr}}(K, A'))^*$$

qui est induit par la dualité locale est un isomorphisme (on sait déjà que cet homomorphisme est injectif par le théorème 7.14). Or $h^1_{\mathrm{nr}}(A) = h^0(A)$ et $h^1_{\mathrm{nr}}(A') = h^0(A') = h^2(A)$ par la proposition 7.22 et le théorème 7.14. Ce dernier théorème donne aussi $h^1(A) = h^1(A')$. Le résultat découle alors de la proposition 7.18.

□

Remarque : Milne a généralisé ce théorème sous des hypothèses beaucoup plus faibles, voir [10], chapitre III.7.

7.6. Exercices

1. Soit G un groupe profini de dimension cohomologique $n \in \mathbf{N}^*$. Soit I son module dualisant.

a) Montrer que si H est un sous-groupe ouvert de G, alors I (vu comme H-module) est encore module dualisant pour H.

On suppose dans toute la suite que $G = \mathrm{Gal}\,(\overline{K})/K)$, où K est un corps p-adique.

b) Montrer que le module dualisant de G est le module μ constitué de toutes les racines de l'unité de $\overline{K}$.

c) Retrouver le théorème de dualité locale de Tate pour un G-module fini M (pour le cas $i = 1$, on plongera M dans un G-module induit).

2. Soit G un groupe profini de dimension cohomologique $n \in \mathbf{N}^*$. Soit I son module dualisant. Soit p un nombre premier. Montrer que $\mathrm{scd}_p(G) = n+1$ si et seulement s'il existe un sous-groupe ouvert H de G tel que I^H contienne un sous-groupe isomorphe à $\mathbf{Q}_p/\mathbf{Z}_p$ (critère de Serre). Retrouver alors que si K est un corps p-adique, on a $\mathrm{scd}(K) = 2$.

3. Soit K un corps p-adique. Soit A une *variété abélienne* sur K. Pour $n > 0$, soit A_n le sous-groupe de $A(\overline{K})$ constitué des éléments de n-torsion. On rappelle les faits suivants : la multiplication par n dans $A(\overline{K})$ est surjective, le module galoisien A_n est dual [39] de A'_n, où A' est la *variété abélienne duale* de A, et $A(K) = H^0(K, A(\overline{K}))$ est un groupe de Lie p-adique compact,

a) Montrer que $H^2(K, A) = \varinjlim_n H^2(K, A_n)$.

b) Montrer que le sous-groupe de torsion de $A'(K)$ est fini.

c) En déduire que $H^2(K, A) = 0$.

4. Soit $G = \mathrm{Gal}\,(\overline{K}/K)$ le groupe de Galois d'un corps p-adique K. Soit M un G-module discret de type fini. On garde les notations du paragraphe 7.3. On rappelle que $H^1(K, M)$ est fini (cf. exercice 5 du chapitre 5) et on note $M' = \mathrm{Hom}(M, \overline{K}^*)$ le dual de Cartier de M. On pourra admettre que si

$$0 \to A \to B \to C \to 0$$

est une suite exacte de groupes topologiques abéliens avec B localement compact, totalement discontinu et engendré par une partie compacte, telle que $A \to B$ soit strict d'image fermée et $B \to C$ soit ouverte, alors la suite des complétés profinis

$$0 \to A^\wedge \to B^\wedge \to C^\wedge \to 0$$

reste exacte (cf. [5], appendice).

a) Montrer que $\alpha^0(G, M)$ induit un isomorphisme du complété profini $\mathrm{Hom}_G(M, \overline{K}^*)^\wedge$ sur $H^2(G, M)^*$ (on pourra commencer par le cas où G agit trivialement sur M).

39. Ceci résulte de l'existence de l'accouplement de Weil.

b) Déduire de a) que le cup-produit induit une dualité de Pontryagin entre le groupe profini $H^0(K,M)^\wedge$ et le groupe discret $H^2(K,M')$, ainsi qu'entre le groupe profini $H^0(K,M')^\wedge$ et le groupe discret $H^2(K,M)$.

8. Théorèmes de dualité pour les corps de nombres

Dans tout ce chapitre, on désigne par k un corps de nombres (i.e. une extension finie de $\mathbf{Q}$) et par $G_k = \mathrm{Gal}\,(\bar{k}/k)$ son groupe de Galois absolu. Pour toute place v de k (archimédienne ou non), on note k_v le complété de k en v. On note $\mathcal{O}_v$ l'anneau des entiers de k_v si v est une place finie, et on pose $\mathcal{O}_v = k_v$ si v est archimédienne. On notera Ω_k l'ensemble de toutes les places de k.

8.1. Quelques rappels de théorie du corps de classes global

Dans ce paragraphe, nous allons énoncer (sans donner les démonstrations en détails) les résultats que nous allons ensuite utiliser pour appliquer le théorème de dualité associé à une formation de classes aux modules galoisiens sur un corps de nombres.

Définition 8.1 Le *groupe des idèles* I_k de k est le produit restreint des k_v^* relativement aux $\mathcal{O}_v^*$. Le *groupe des classes d'idèles* C_k de k est le quotient du groupe multiplicatif I_k par k^* (plongé diagonalement dans I_k).

Le groupe I_k est équipé de sa topologie de produit restreint, qui en fait un groupe séparé, localement compact. D'autre part, si K est une extension finie de k, on a une injection naturelle de I_k dans I_K, d'où la définition suivante :

Définition 8.2 On pose $I = \varinjlim_K I_K$, où K décrit les extensions finies de k. De même on pose $C := I/\bar{k}^*$; c'est la limite inductive des C_K.

Pour K/k finie galoisienne, on a une action de $\mathrm{Gal}\,(K/k)$ sur I_K, via son action naturelle pour toute place v de k sur $\bigoplus_{w|v} K_w^*$. En passant à la limite, on obtient une structure de G_k-module discret sur I avec $I_K = I^{G_K}$ pour toute extension finie de K de k, et de même $C_K = C^{G_K}$ via Hilbert 90.

Pour toute place v de k, on fixe un k-plongement de $\bar{k}$ dans $\bar{k}_v$, et en particulier une place $\bar{v}$ de $\bar{k}$ au-dessus de v, ce qui permet, pour toute extension finie galoisienne K de k, d'avoir une place privilégiée de K au-dessus de v ;

pour simplifier on notera encore K_v le complété de K en cette place. Si K/k est une extension finie galoisienne de groupe G, on a alors un sous-groupe de décomposition [40] associé $G_v \subset G$.

Proposition 8.3 *Soit v une place finie de k qui est non ramifiée dans l'extension K/k. Soit $\mathcal{O}_{K_v}$ l'anneau des entiers de K_v. Alors le G_v-module $\mathcal{O}_{K_v}^*$ est cohomologiquement trivial.*

Démonstration : Il suffit de vérifier que si F est un corps p-adique et F' une extension finie galoisienne non ramifiée de F (dont on note $\mathcal{G}$ le groupe de Galois), alors $H^q(\mathcal{G}, U_{F'}) = 0$ pour $q > 0$ (où $U_{F'}$ désigne le groupe des unités de $\mathcal{O}_{F'}$). Soit $\kappa_{F'}$ le corps résiduel de F' et soit $U_{F'}^1$ le sous-groupe de $U_{F'}$ constitué des x tels que la valuation de $(1-x)$ soit > 0. On sait déjà (proposition 5.3) que $H^q(\mathcal{G}, U_{F'}^1) = 0$. On conclut alors en utilisant la suite exacte longue associée à

$$0 \to U_{F'}^1 \to U_{F'} \to \kappa_{F'}^* \to 0$$

et le fait que $H^q(\mathcal{G}, \kappa_{F'}^*) = 0$ pour $q \geq 1$ (ceci vient de Hilbert 90 pour $q = 1$, de la nullité du groupe de Brauer du corps fini $\kappa_{F'}$ pour $q = 2$, et de la 2-périodicité de la cohomologie du groupe cyclique $\mathcal{G}$ pour $q \geq 3$).

□

Une conséquence facile de la proposition précédente est l'égalité

$$\widehat{H}^i(G, I_K) = \bigoplus_{v \in \Omega_k} \widehat{H}^i(G_v, K_v^*) \tag{9}$$

pour tout $i \in \mathbf{Z}$ ([12], Prop. 8.1.2.). Le théorème de Hilbert 90 joint au fait que $H^3(G_v, K_v^*) = 0$ (qui résulte du théorème 2.10 et de Hilbert 90 pour v réelle, et de la proposition 6.20 appliquée à $M = \mathbf{Z}$ pour v finie vu que $H^1(G_v, \mathbf{Z}) = 0$) donne alors

Proposition 8.4 *Soit K/k une extension finie galoisienne de groupe G. Alors $H^1(G, I_K) = H^3(G, I_K) = 0$.*

Un passage à la limite non trivial (la difficulté est de montrer le fait non évident que si on fixe une place $\bar{v}$ de $\bar{k}$ au-dessus de v, alors son sous-groupe de décomposition est bien le groupe de Galois absolu de k_v et pas seulement un

40. Ce sous-groupe de décomposition n'est donc a priori bien défini qu'à conjugaison près, mais ce n'est pas gênant en ce qui concerne la cohomologie, voir le début du paragraphe 4.1.

quotient de ce dernier, cf. [12], Prop. 8.1.5. Attention, *I n'est pas* le produit restreint des $\bar{k}_v^*$) donne aussi

$$H^i(k, I) = \bigoplus_{v \in \Omega_k} H^i(k_v, \bar{k}_v^*)$$

pour tout $i \geq 1$. En particulier $H^1(k, I)$ et $H^3(k, I)$ sont nuls.

Définition 8.5 Soit K/k une extension finie galoisienne de groupe G. Pour toute place v de k, on note $G_v = \mathrm{Gal}\,(K_v/k_v)$ le sous-groupe de décomposition associé à v. On définit alors

$$\mathrm{inv}_{K/k} : H^2(G, I_K) \to \frac{1}{[K:k]}\mathbf{Z}/\mathbf{Z}$$

par la formule :

$$\mathrm{inv}_{K/k}(c) = \sum_{v \in \Omega_k} \mathrm{inv}_{K_v/k_v}(c_v)$$

où c_v est la composante en v de $c \in H^2(G, I_K) = \bigoplus_{v \in \Omega_k} H^2(G_v, K_v^*)$.

Ici inv_{K_v/k_v} est l'invariant local induit par $j_v : \mathrm{Br}\, k_v \to \mathbf{Q}/\mathbf{Z}$ (pour v réelle c'est juste l'isomorphisme de $\mathrm{Br}\,\mathbf{R}$ avec $\mathbf{Z}/2$, et pour v complexe c'est l'application nulle). D'autre part, pour toute place v de k, on dispose de l'application de réciprocité $(., K_v/k_v) : k_v^* \to G_v^{\mathrm{ab}} \subset G^{\mathrm{ab}}$ de la définition 6.14 (si v est archimédienne on prend pour $(., K_v/k_v)$ l'application induite par l'homomorphisme surjectif de k_v^*/k_v^{*2} sur G_v^{ab}). On définit alors

$$(., K/k) : I_k \to G^{\mathrm{ab}}$$

par

$$(\alpha, K/k) = \prod_{v \in \Omega_k} (\alpha_v, K_v/k_v) \tag{10}$$

Le produit est bien défini car si v est non ramifée dans K/k et $\alpha_v \in \mathcal{O}_v^*$, alors $(\alpha_v, K_v/k_v) = 1$ (en effet $\widehat{H}^0(G_v, \mathcal{O}_{K_v}^*) = 0$ pour une telle v via la proposition 8.3, donc tous les éléments de $\mathcal{O}_v^*$ sont des normes de K_v/k_v).

Un résultat important de la théorie du corps de classes global (qu'il faut montrer indépendamment) est la *loi de réciprocité* suivante. Pour une preuve, voir par exemple le paragraphe 10 de l'exposé de Tate dans [3] (chapitre VII).

Theorème 8.6 *Soit K une extension finie cyclique de k. Alors $(a, K/k) = 1$ pour tout $a \in k^*$. Autrement dit $(., K/k)$ se factorise en un homomorphisme $C_k \to G^{\mathrm{ab}}$.*

D'autre part la proposition 6.15 donne facilement :

Proposition 8.7 *Soit K/k une extension finie galoisienne de groupe G. Alors pour tout $\chi \in H^1(G, \mathbf{Q}/\mathbf{Z})$ et tout $\alpha \in I_k$, on a*

$$\chi((\alpha, K/k)) = \mathrm{inv}_{K/k}(\alpha \cup \chi)$$

où, pour le cup-produit, α est vu dans $H^0(G, I_K)$ et χ dans $H^2(G, \mathbf{Z})$.

Une propriété fondamentale de la théorie du corps de classes global est le théorème suivant. Via le passage aux p-Sylow, on se ramène facilement pour la démonstration (cf. [12], Prop. 8.1.12) au cas d'un p-groupe, puis par récurrence sur le cardinal de G au cas d'un groupe cyclique, mais pour ce dernier cas il faut utiliser l'*axiome du corps de classes* (lequel résulte des "deux inégalités fondamentales") qui dit que si K/k est cyclique, alors $\widehat{H}^i(G, C_K) = 0$ si $i = 1$ et $\widehat{H}^i(G, C_K)$ est de cardinal $[K : K]$ si $i = 0$ ([11], chap. 6, 4.4.).

Theorème 8.8 *Soit K/k une extension finie galoisienne de groupe G. Alors $H^1(G, C_K) = 0$. De même $H^1(k, C) = 0$.*

On passe maintenant à l'étude du H^2, qui va se ramener au groupe de Brauer. On déduit [41] des résultats locaux, du théorème 8.6 et de la proposition 8.7 le théorème suivant ([12], proposition 8.1.15) :

Theorème 8.9 *Soit K/k une extension cyclique de groupe G. Alors on a une suite exacte*

$$0 \to H^2(G, K^*) \to H^2(G, I_K) \overset{\mathrm{inv}_{K/k}}{\to} \frac{1}{[K : k]}\mathbf{Z}/\mathbf{Z} \to 0$$

Il se trouve que dans le cas d'un corps de nombres k, le groupe $\mathrm{Br}\, k$ s'obtient comme réunion des $\mathrm{Br}\,(K/k)$ pour K/k finie galoisienne *cyclique* ([12], prop. 8.1.14 ; cela résulte du théorème 8.8 et de la proposition 8.1.9. de [12], qui dit que $H^2(k, I)$ est aussi la réunion des $H^2(\mathrm{Gal}\,(K/k), I_K)$ pour K/k cyclique).). On obtient alors en passant à la limite :

Corollaire 8.10 (Brauer-Hasse-Noether) *On a des suites exacte*

$$0 \to \mathrm{Br}\, k \to H^2(k, I) \overset{\mathrm{inv}_k}{\to} \mathbf{Q}/\mathbf{Z} \to 0$$

et

$$0 \to \mathrm{Br}\, k \to \bigoplus_{v \in \Omega_k} \mathrm{Br}\, k_v \overset{\mathrm{inv}_k}{\to} \mathbf{Q}/\mathbf{Z} \to 0$$

où $\mathrm{inv}_k = \sum_{v \in \Omega_k} \mathrm{inv}_v$.

41. Noter que dans la preuve de la proposition 8.1.15 de [12], le théorème 8.6 est implicitement supposé connu ; il ne résulte pas aisément des résultats précédents du chapitre.

Remarque : Ce corollaire joint à la proposition 8.7 donne en particulier que le théorème 8.6 vaut encore pour une extension galoisienne finie K/k quelconque (pas forcément cyclique). En effet si $a \in k^*$, alors $(a \cup \chi) \in \mathrm{Br}\,(K/k)$ donc $\mathrm{inv}_{K/k}(a \cup \chi) = 0$, ce qui implique que $\chi((a, K/k)) = 0$ pour tout caractère χ de G^{ab}.

Soit K une extension algébrique de k. Pour toute place v de k, on notera encore $K_v = Kk_v$ (attention si K/k n'est pas finie, ce n'est pas en général le complété de K en une place au-dessus de v).

Corollaire 8.11 *Soit p un nombre premier. Soit K une extension algébrique (infinie) de k, supposée totalement imaginaire si $p = 2$. Supposons que p^∞ divise $[K_v : k_v]$ pour toute place finie v de k. Alors* $\mathrm{cd}_p(G_K) \leq 1$.

Démonstration : Il suffit de vérifier que $(\mathrm{Br}\, L)\{p\} = 0$ pour toute extension finie L de K via le théorème 4.11. Comme L vérifie les mêmes hypothèses que K, on est ramené à montrer que $(\mathrm{Br}\, K)\{p\} = 0$. Comme $\mathrm{Br}\, K$ est la limite inductive des $\mathrm{Br}\, F$ pour F extension finie de k, il suffit de voir si F est une telle extension, tout élément α de torsion p-primaire dans $\mathrm{Br}\, F$ a une restriction nulle à $\mathrm{Br}\, K$. Notons que $\mathrm{Br}\, K$ s'injecte dans la somme directe (pour v place de k) des $\mathrm{Br}\, K_v$ (passer à la limite dans le théorème de Brauer-Hasse-Noether). Soit F_v le complété de F en une place au-dessus de v. Alors la restriction α_v de α à $\mathrm{Br}\, F_v$ a une restriction nulle dans $\mathrm{Br}\, K_v$: pour v réelle cela résulte de l'hypothèse $p \neq 2$, et pour v finie cela vient de ce que p^∞ divise $[K_v : k_v]$ (donc aussi $[K_v : F_v]$) et de ce que la restriction multiplie l'invariant local par le degré de l'extension (proposition 5.8). Ceci implique que la restriction de α à $\mathrm{Br}\, K$ est nulle comme on voulait.

□

On aimerait utiliser les applications $\mathrm{inv}_{K/k} : H^2(\mathrm{Gal}\,(K/k), I_K) \to \mathbf{Q}/\mathbf{Z}$ pour définir des applications analogues sur $H^2(\mathrm{Gal}\,(K/k), C_K)$. En général il y a une difficulté pour le faire à un niveau fini, car l'application canonique

$$H^2(\mathrm{Gal}\,(K/k), I_K) \to H^2(\mathrm{Gal}\,(K/k), C_K)$$

n'est pas surjective. Cependant, la proposition suivante ([12], Prop. 8.1.20., qui repose encore sur l'axiome du corps de classes) permet de le faire à la limite :

Proposition 8.12 *La suite*

$$0 \to \mathrm{Br}\, k \to H^2(k, I) \to H^2(k, C) \to 0$$

est exacte.

On déduit alors via le corollaire 8.10 un isomorphisme canonique $\mathrm{inv}_k : H^2(k, C) \simeq \mathbf{Q}/\mathbf{Z}$. Soit alors K/k une extension finie galoisienne de groupe G. On a $\mathrm{inv}_K \circ \mathrm{Res} = [K : k]\mathrm{inv}_k$ via la propriété analogue au niveau local. Comme $H^2(G, C_K)$ s'injecte dans $H^2(k, C)$ via le théorème 8.8 et la suite de restriction-inflation, on obtient un isomorphisme

$$\mathrm{inv}_{K/k} : H^2(G, C_K) \to \frac{1}{[K : k]}\mathbf{Z}/\mathbf{Z}$$

et en passant à la limite un isomorphisme $\mathrm{inv}_k : H^2(G_k, C) \to \mathbf{Q}/\mathbf{Z}$ vérifiant

Theorème 8.13 *Les isomorphismes*

$$\mathrm{inv}_K : H^2(G_K, C) \to \mathbf{Q}/\mathbf{Z}$$

(définis pour toute extension K/k finie) constituent une formation de classes sur le G_k-module C, limite inductive des groupes de classes d'idèles $C_K = I_K/K^*$

En particulier, comme $C^{G_k} = C_k$ via Hilbert 90, on obtient un homomorphisme de réciprocité

$$\omega : C_k \to G_k^{\mathrm{ab}}$$

dont le noyau est le groupe des normes universelles.

Rappelons que via la formule du produit, on a un homomorphisme surjectif

$$|.| : C_k \to \mathbf{R}_+^*, \quad \alpha \mapsto \prod_{v \in \Omega_k} |\alpha_v|_v$$

dont le noyau C_k^0 est compact ([3], exposé II, paragraphe 16). Ici $|.|_v$ désigne la valeur absolue normalisée en v (attention pour v complexe c'est le *carré* du module usuel).

Proposition 8.14 *Pour tout corps de nombres k, l'homomorphisme ω est surjectif.*

Démonstration : On sait déjà que l'image de ω est dense (proposition 6.21), il suffit donc de voir qu'elle est compacte. Or C_k et C_k^0 ont même image par ω vu que $\mathbf{R}_+^*$ n'a pas de quotient fini non trivial. Le résultat en découle.

□

Remarque : Dans le cas d'un corps de fonctions sur un corps fini, l'application ω est injective, mais n'est plus surjective.

Corollaire 8.15 *Soit $D_k = \bigcap_K N_{K/k}C_K$ le groupe des normes universelles dans C_k. On a une suite exacte*

$$0 \to D_k \to C_k \stackrel{\omega}{\to} G_k^{\mathrm{ab}} \to 0$$

On a enfin le théorème d'existence suivant ([11], Th. VI.1.6., ou encore [3], exposé VII, paragraphe 12) :

Theorème 8.16 *Les groupes de norme $N_{K/k}$ pour K/k finie abélienne sont exactement les sous-groupes (ouverts) d'indice fini de C_k.*

On en déduit alors ([12], Th. 8.2.1.) l'importante propriété suivante :

Theorème 8.17 *Le groupe des normes universelles D_k est un groupe divisible. C'est la composante connexe de* 1 *dans C_k.*

Noter que la composante neutre D_k peut être très compliquée (cf. [12], Chapitre VIII, paragraphe 2). Dans le cas où k est une extension finie de $\mathbf{F}_q(t)$, le groupe compact C_k^0 est déjà complètement discontinu (donc profini), ce qui fait que le groupe des normes universelles est trivial et l'application de réciprocité $\omega : C_k \to G_k^{\mathrm{ab}}$ est injective (en d'autres termes la composante connexe du neutre de C_k est triviale dans le cas d'un corps de fonctions). Par contre ω n'est plus surjective, mais a un conoyau isomorphe à $\widehat{\mathbf{Z}}/\mathbf{Z}$ (comme dans le cas local), cf. [12], proposition 8.1.26.

8.2. La P-formation de classes associée à un groupe de Galois de ramification restreinte

Il est souvent utile pour les applications de travailler non plus avec le groupe de Galois absolu G_k d'un corps de nombres k, mais avec certains quotients $G_{k,S}$ de G_k associés à un sous-ensemble non vide S de Ω_k. Le lecteur désirant se familiariser avec la dualité de Poitou-Tate est invité à sauter cette section en première lecture et à supposer $S = \Omega_k$ dans le reste de ce chapitre.

Dans toute la suite, on désigne par S un sous-ensemble de Ω_k contenant toutes les places archimédiennes (en particulier S est non vide[42]). On fixe

42. Cette hypothèse est importante quand on travaille avec un corps de fonctions au lieu d'un corps de nombres.

une clôture algébrique $\bar{k}$ de k et on note k_S l'extension maximale de k incluse dans $\bar{k}$ qui est non ramifiée en dehors de S, puis on pose $G_S = \mathrm{Gal}\,(k_S/k)$. On désigne par $\mathcal{O}_{k,S}$ l'anneau des S-entiers de k (par exemple si $S = \Omega_k$ on a simplement $\mathcal{O}_{k,S} = k$ et si $S = \Omega_\infty$ est l'ensemble des places archimédiennes on a $\mathcal{O}_{k,S} = \mathcal{O}_k$). Ainsi si S est fini, le schéma $\mathrm{Spec}\,(\mathcal{O}_{k,S})$ est un ouvert de Zariski de $\mathrm{Spec}\,(\mathcal{O}_k)$ et l'extension k_S est "peu ramifiée" (par exemple si $S = \Omega_\infty$ c'est l'extension maximale de k non ramifiée en tout idéal premier de $\mathcal{O}_k$). Si au contraire S contient presque toutes les places de k, l'extension k_S est "proche" de $\bar{k}$, le cas $S = \Omega_k$ correspondant à $k_S = \bar{k}$.

On notera P l'ensemble des nombres premiers ℓ tels que ℓ^∞ divise l'ordre de G_S ; en particulier P contient tous les ℓ inversibles[43] dans $\mathcal{O}_{k,S}$ (i.e. tels que S contienne toutes les places divisant ℓ) car pour un tel ℓ, le corps k_S contient toutes les racines de l'unité d'ordre une puissance de ℓ et on sait que si ζ_{ℓ^m} est une racine primitive ℓ^m-ième de l'unité, alors $\mathbf{Q}(\zeta_{\ell^m})$ est de degré $\ell^{m-1}(\ell-1)$ sur $\mathbf{Q}$.

Soit F une extension finie (galoisienne) de k. On note I_F son groupe des idèles et C_F son groupe des classes d'idèles. Pour simplifier les notations, on appellera souvent encore S l'ensemble des places de F divisant une place de k appartenant à S. On note $U_{F,S} \simeq \prod_{w \notin S} \mathcal{O}_w^*$ le sous-groupe de I_F constitué des familles $(a_w)_{w \in \Omega_F}$ dont la composante en w est triviale (resp. inversible) si la place $w \in \Omega_F$ est dans S (resp. n'est pas dans S). Enfin, on pose $C_S(F) = C_F/U_{F,S}$ et on appelle C_S la limite inductive des $C_S(F)$ quand F décrit les extensions finies galoisiennes de k incluses dans k_S. Le but de ce paragraphe est de montrer qu'on peut définir une P-formation de classes (G_S, C_S) à partir de la formation de classes (G_k, C) du théorème 8.13.

Lemme 8.18 *Soit $I_{F,S}$ le sous-groupe de I_F constitué des familles $(a_w)_{w \in \Omega_F}$ dont la composante en w est triviale pour toute place $w \in \Omega_F$ non dans S (ainsi $I_{F,S}$ s'identifie au produit restreint des F_w^* pour w place de F au-dessus d'une place de S). Alors on a une suite exacte*

$$0 \to C_{F,S} \to C_S(F) \to \mathrm{Cl}_{F,S} \to 0$$

où $\mathrm{Cl}_{F,S}$ est le groupe des classes d'idéaux de $\mathcal{O}_{F,S}$ et $C_{F,S}$ est le quotient de $I_{F,S}$ par le groupe des unités $\mathcal{O}_{F,S}^*$ de $\mathcal{O}_{F,S}$. Si S contient presque toutes les places de k, alors $C_{F,S} = C_S(F)$.

Attention, on voit donc que si S n'est pas cofini dans Ω_k, $C_S(F)$ et $C_{F,S}$ sont en général différents. Le premier est plus utile dans la mesure ou comme

43. Si $k = \mathbf{Q}$, Chenevier et Clozel ont démontré récemment dans [4] que si S contient au moins deux places finies, l'ensemble P contient tous les nombres premiers.

on va le voir (lemme 8.19, c)), il vérifie une bonne propriété de descente galoisienne, ce qui n'est pas le cas de $C_{F,S}$. Bien entendu, si $S = \Omega_k$, alors $C_S(F) = C_{F,S} = C_F$.

Démonstration : On a dans I_F les égalités

$$F^* \cap U_{F,S} = \{1\}; \quad I_{F,S} \cap (F^*.U_{F,S}) = \mathcal{O}_{F,S}^*$$

. Ainsi $U_{F,S}$ s'identifie à un sous-groupe de C_F et on a un plongement

$$C_{F,S} \hookrightarrow C_F/U_{F,S} = C_S(F)$$

Le conoyau de cette flèche s'identifie à $I_F/I_{F,S}.U_{F,S}.F^*$, i.e. au quotient de $I_F/I_{F,S}.U_{F,S} \simeq \bigoplus_{v \notin S} \mathbf{Z}$ par l'image de F^* relativement à l'application

$$F^* \to \bigoplus_{v \notin S} \mathbf{Z}, \quad a \mapsto (w(a))_{w \notin S}$$

Ainsi ce conoyau est bien isomorphe au groupe des classes d'idéaux de $\mathcal{O}_{F,S}$ (noter que les idéaux premiers de $\mathcal{O}_{F,S}$ correspondent aux places de F non dans S ; en langage géométrique $\mathrm{Cl}_{F,S}$ est le groupe des classes de diviseurs de Weil de $\mathrm{Spec}\,(\mathcal{O}_{F,S})$).

Enfin si S contient presque toutes les places de k, alors $\mathcal{O}_{F,S}$ est un anneau de Dedekind qui n'a qu'un nombre fini d'idéaux premiers, c'est donc un anneau principal ([2], paragraphe 2, proposition 1), ce qui implique que son groupe des classes est nul.

□

Lemme 8.19 *a) Le groupe $C_S = \varinjlim_{F \subset k_S} C_S(F)$ est aussi la limite inductive des $C_{F,S}$.*

b) Pour toute extension finie galoisienne F de k, le $\mathrm{Gal}\,(F/k)$-module $U_{F,S}$ est cohomologiquement trivial. Le G_S-module $U_S := \varinjlim_{F \subset k_S} U_{F,S}$ est cohomologiquement trivial.

c) On a $C_S^{G_S} = C_S(k)$.

Démonstration : a) Via le lemme précédent, il suffit de vérifier que $\varinjlim_{F \subset k_S} \mathrm{Cl}_{F,S} = 0$. Ceci est une conséquence immédiate du *théorème de l'idéal principal* ([11], chapitre VI, paragraphe 7.5), qui dit que tout idéal de $\mathcal{O}_{F,S}$ devient principal dans l'extension abélienne maximale de F non ramifiée en dehors de S et complètement décomposée aux places de S.

b) Le même argument que pour l'égalité (9) donne

$$\widehat{H}^i(\mathrm{Gal}\,(F/k), U_{F,S}) = \bigoplus_{v \notin S} \widehat{H}^i(\mathrm{Gal}\,(F_v/k_v), \mathcal{O}_v^*)$$

pour tout $i \in \mathbf{Z}$, après quoi le résultat pour $U_{F,S}$ découle de la proposition 8.3 vu que pour $v \notin S$, l'extension F_v/k_v est non ramifiée. On en déduit le résultat pour U_S en passant à la limite.

c) Soit $C(k_S)$ la limite inductive des C_F pour F extension finie galoisienne de k incluse dans k_S. En passant à la limite dans la définition de $C_S(F)$, on obtient une suite exacte

$$0 \to U_S \to C(k_S) \to C_S \to 0 \tag{11}$$

On applique alors la suite exacte de cohomologie pour l'action du groupe G_S (noter que $U_S^{G_S} = U_{k,S}$ est clair et comme on l'a déjà vu $C(k_S)^{G_S} = C_k$). Comme U_S est un G_S-module cohomologiquement trivial, on a $H^1(G_S, U_S) = 0$ d'où $C_S^{G_S} = C_k/U_{k,S} = C_S(k)$.

□

Theorème 8.20 *La formation de classes (G_k, C) du théorème 8.13 induit une P-formation de classes (G_S, C_S).*

Démonstration : Soit $H_S := \mathrm{Gal}\,(\bar{k}/k_S)$. On sait (vu la définition de P) que la formation de classes (G_k, C) induit une P-formation de classes (G_S, C^{H_S}). Ici C^{H_S} est la limite inductive $C(k_S)$ des C_F (pour F extension finie galoisienne de k incluse dans k_S). Comme (d'après le lemme précédent) le G_S-module U_S est cohomologiquement trivial, la suite exacte (11) montre que les groupes de cohomologie $H^i(G_S, C^{H_S})$ s'identifient aux $H^i(G_S, C_S)$ pour $i \geq 1$, d'où le résultat.

□

On aura enfin besoin de l'analogue du théorème 8.17.

Proposition 8.21 *Soit $D_S(k)$ la composante connexe du neutre dans $C_S(k)$. Alors on a $D_S(k) = D_k U_{k,S}/U_{k,S}$. Le groupe $D_S(k)$ est divisible, et on a une suite exacte*

$$0 \to D_S(k) \to C_S(k) \xrightarrow{\omega} G_S^{\mathrm{ab}} \to 0$$

Démonstration : Le groupe $C_S(k)$ est le quotient de C_k par le sous-groupe compact $U_{k,S}$. De ce fait la surjection canonique $p : C_k \to C_S(k)$ est un morphisme propre, et l'image de la composante neutre D_k de C_k par p est donc la composante neutre de $C_S(k)$, ce qui prouve la première assertion. Alors $D_S(k)$ est divisible comme quotient d'un groupe divisible.

Maintenant, l'image de $U_{k,S}$ par $\omega : C_k \to G_k^{\mathrm{ab}}$ est, d'après le lemme 7.11 et la formule (10), le sous-groupe H de G_k^{ab} engendré par les sous-groupes d'inertie I_v pour $v \notin S$, ce qui fait que le corps fixe de H est la sous-extension maximale de k^{ab} non ramifiée en dehors de S, c'est-à-dire k_S^{ab} (en effet un sous-groupe de G_k^{ab} contient I_v si et seulement si l'extension de k qui lui correspond est non ramifiée en v). On a donc un diagramme commutatif dont les lignes sont exactes et les flèches verticales injectives :

$$\begin{array}{ccccccccc} 0 & \longrightarrow & D_k \cap U_{k,S} & \longrightarrow & U_{k,S} & \longrightarrow & \mathrm{Gal}\,(k^{\mathrm{ab}}/k_S^{\mathrm{ab}}) & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & D_k & \longrightarrow & C_k & \xrightarrow{\omega} & \mathrm{Gal}\,(k^{\mathrm{ab}}/k) & \longrightarrow & 0 \end{array}$$

Comme $D_S(k)$, $C_S(k)$, et G_S^{ab} sont les conoyaux respectifs des flèches verticales de gauche, du milieu, et de droite, le résultat découle du lemme du serpent.

□

8.3. Énoncé des théorèmes de Poitou-Tate

On garde les notations de la section précédente. Cette section est consacrée à l'énoncé des théorèmes principaux de ce chapitre, qui sont des théorèmes de dualité pour la cohomologie des corps de nombres. Comme on l'a déjà observé, la méthode passant par le module dualisant (qu'on a utilisée pour les corps locaux) ne marche pas bien même pour un corps de nombres totalement imaginaire. On va donc à la place suivre la méthode de [10], chapitre I.4, qui utilise de façon essentielle le théorème de dualité 6.29 pour une (P)-formation de classes démontré au chapitre précédent. En première lecture, on pourra supposer jusqu'à la fin de ce chapitre que l'ensemble $S \subset \Omega_k$ est l'ensemble de toutes les places de k, ce qui évite quelques complications liées à la ramification restreinte.

Theorème 8.22 *Soit M un G_S-module de type fini. Soit $\ell \in P$. Alors l'homomorphisme*

$$\alpha^r(G_S, M)\{\ell\} : \mathrm{Ext}^r_{G_S}(M, C_S)\{\ell\} \to H^{2-r}(G_S, M)^*\{\ell\}$$

(cf. théorème 6.29) est un isomorphisme[44] *pour tout* $r \geq 1$.

Démonstration : On applique la version "P-formations de classes" du théorème 6.29. Quitte à passer à une extension finie de k incluse dans k_S (correspondant à un sous-groupe ouvert U de G_S), il suffit de vérifier que pour tout $m > 0$, l'application $\alpha^1(G_S, \mathbf{Z}/\ell^m)$ est bijective. Or, d'après le lemme 6.27 b), l'application $\alpha^1(G_S, \mathbf{Z}/\ell^m) : C_S(k)/\ell^m \to G_S^{\mathrm{ab}}/\ell^m$ est induite par l'application de réciprocité ω et la proposition 8.21 montre alors que c'est un isomorphisme (noter l'importance du fait que le noyau $D_S(k)$ de la flèche $C_S(k) \to G_S^{\mathrm{ab}}$ induite par ω soit divisible).

□

Le but est maintenant de passer de ce résultat abstrait à un théorème de dualité plus explicite, en particulier quand M est fini. On commence par fixer quelques notations supplémentaires, qui seront en vigueur jusqu'à la fin de ce chapitre.

Si v est une place de k, on note $G_v \subset G_k$ le sous-groupe de décomposition en v, qui s'identifie au groupe de Galois absolu du complété k_v ; si v est finie, on note $k(v)$ le corps résiduel en v, et $G(v)$ le groupe de Galois absolu de $k(v)$. Pour tout G_S-module M, on a donc des applications de restriction $H^i(G_S, M) \to H^i(G_v, M)$ (définies pour toute place v de k ; on s'en servira surtout pour $v \in S$).

Avertissement : Dans cette section, $H^i(k_v, M)$ désignera toujours $H^i(G_v, M)$ *sauf pour* $i = 0$ *et* v *archimédienne*, auquel cas ce sera par convention le groupe modifié de Tate $\widehat{H}^0(G_v, M)$, c'est-à-dire $\{0\}$ si v est complexe et le quotient de $M^{G_{\mathbf{R}}}$ par le groupe des normes $N_{G_{\mathbf{R}}} M$ si v est réelle, où $G_{\mathbf{R}} := \mathrm{Gal}\,(\mathbf{C}/\mathbf{R})$.

Soient maintenant v une place finie du corps de nombres k et M un G_S-module non ramifié en v (i.e. non ramifié pour l'action induite de G_v). Pour $i \geq 0$, on dispose donc des groupes de cohomologie non ramifiée $H^i_{\mathrm{nr}}(k_v, M)$. On posera pour simplifier $H^i_{\mathrm{nr}}(k_v, M) = H^i(k_v, M)$ si v est une place archimédienne. Si M est un G_S-module de type fini, alors M est non ramifié en dehors d'un nombre fini de places (parce que tout élément de M est stabilisé par un sous-groupe ouvert d'indice fini de G_S, et une extension finie de k n'est ramifiée qu'en un nombre fini de places). Cela justifie la définition suivante :

44. Attention, l'assertion (qu'on peut trouver dans [10]) que $\alpha^0(G_S, \mathbf{Z}/\ell^m)$ est surjective semble (disons pour $\ell \neq 2$ pour éviter les complications liées aux places réelles) conditionnelle à l'hypothèse que $H^2(G_S, \mathbf{Q}_\ell/\mathbf{Z}_\ell) = 0$, résultat qui est connu ([12], Th. 10.2.3.) si S contient presque toutes les places de k, mais est en général relié à la *conjecture de Leopoldt*. Voir [12], paragraphe X.3., pour une discussion de cette conjecture.

Définition 8.23 Soit M un G_S-module de type fini. On définit $\mathbf{P}^i_S(k, M)$ (ou $\mathbf{P}^i_S(M)$ si k est sous-entendu) comme le *produit restreint* pour v dans S des $H^i(k_v, M)$ par rapport aux $H^i_{\mathrm{nr}}(k_v, M)$.

Ainsi $\mathbf{P}^i_S(k, M)$ est consitué des familles $(x_v)_{v\in S}$ avec $x_v \in H^i(k_v, M)$ pour toute $v \in S$, et $x_v \in H^i_{\mathrm{nr}}(k_v, M)$ pour presque toute v. Quand $S = \Omega_k$, on abrègera $\mathbf{P}^i_{\Omega_k}(k, M)$ en $\mathbf{P}^i(k, M)$.

Noter que $\mathbf{P}^0_S(k, M) = \prod_{v\in S} H^0(k_v, M)$ (c'est un groupe compact si M est fini). Le groupe $\mathbf{P}^1_S(k, M)$, muni de sa topologie de produit restreint (chaque $H^1(k_v, M)$ étant considéré comme discret) est localement compact. Enfin $\mathbf{P}^2_S(k, M) = \bigoplus_{v\in S} H^2(k_v, M)$ si M est fini, et c'est alors un groupe discret. Noter aussi que pour $i \geq 3$, on a $\mathbf{P}^i_S(k, M) = \bigoplus_{v\in\Omega_{\mathbf{R}}} H^i(k_v, M)$ puisque pour v finie, le corps k_v est de dimension cohomologique stricte 2 (théorème 7.15).

Remarques : a) Si on ne suppose pas M de type fini, la définition des $\mathbf{P}^i$ est plus compliquée, et s'interprète mieux dans le langage de la cohomologie étale. On n'utilisera donc pas cette notion dans ce cours.

b) Si M est un G_S-module de type fini et $v \notin S$, alors M est non ramifié en v puisque k_S est non ramifiée en dehors de S.

Lemme 8.24 *Soit M un G_S-module de type fini. Soit $i \geq 0$. L'image de l'application diagonale (induite par les restrictions)*

$$\beta^i : H^i(G_S, M) \to \prod_{v\in S} H^i(k_v, M)$$

est incluse dans $\mathbf{P}^i_S(k, M)$.

Démonstration : Soit $x \in H^i(G_S, M)$. Il existe une extension finie galoisienne $F \subset k_S$ de k telle que l'action de $\mathrm{Gal}\,(k_S/F)$ sur M soit triviale et x soit dans l'image de $H^i(\mathrm{Gal}\,(F/k), M)$. La restriction de x à $H^i(k_v, M)$ est alors dans $H^i_{\mathrm{nr}}(k_v, M)$ dès que v est non ramifiée dans l'extension F/k, donc pour presque toute place v de k.

□

Le lemme suivant est l'analogue du théorème de dualité locale 7.14 pour le corps des réels (pour le corps des complexes l'assertion est triviale via nos conventions sur $H^0(k_v, M)$) :

Lemme 8.25 *Soit M un $G_{\mathbf{R}}$-module fini. Alors le cup-produit*

$$\widehat{H}^i(G_{\mathbf{R}}, M) \times \widehat{H}^{2-i}(G_{\mathbf{R}}, M') \to \mathrm{Br}\,\mathbf{R} = \mathbf{Z}/2\mathbf{Z}$$

est une dualité parfaite de groupes finis de 2-torsion pour $i = 0, 1, 2$.

Démonstration : Comme le groupe de Galois $G_{\mathbf{R}}$ de $\mathbf{R}$ est d'ordre 2, on peut supposer que M est de torsion 2-primaire. On peut également supposer M simple en procédant par récurrence sur l'ordre de M et en utilisant le lemme des cinq pour montrer l'isomorphisme de $\widehat{H}^i(G_{\mathbf{R}}, M)$ avec $\widehat{H}^{2-i}(G_{\mathbf{R}}, M')^*$. Maintenant, le seul $G_{\mathbf{R}}$-module simple est $\mathbf{Z}/2\mathbf{Z}$ avec action triviale (utiliser le lemme 3.15 pour voir d'abord que l'action est triviale) puisque $G_{\mathbf{R}}$ est un 2-groupe. Finalement pour $M = \mathbf{Z}/2\mathbf{Z}$ avec action triviale, tous les groupes considérés valent $\mathbf{Z}/2\mathbf{Z}$ et le résultat est immédiat vu que l'accouplement n'est pas nul (pour $i = 1$ on le voit en identifiant le premier groupe avec $\widehat{H}^{-1}(G_{\mathbf{R}}, \mathbf{Z}/2)$ et $\operatorname{Br}\mathbf{R}$ avec $\widehat{H}^0(G_{\mathbf{R}}, \mathbf{Z}/2)$).

□

Proposition 8.26 *Soit M un G_S-module fini. Alors l'application*

$$\beta^1 : H^1(G_S, M) \to \mathbf{P}^1_S(k, M)$$

est propre (i.e. l'image réciproque d'une partie compacte de $\mathbf{P}^1_S(k, M)$ est finie).

Démonstration : Soit T une partie de S avec $S - T$ fini. On pose $P_T = \prod_{v\in S-T} H^1(k_v, M) \times \prod_{v\in T} H^1_{\mathrm{nr}}(k_v, M)$. Rappelons que tous les $H^1(k_v, M)$ (et donc aussi les $H^1_{\mathrm{nr}}(k_v, M)$) sont finis via le corollaire 5.13. Ainsi P_T est compact (produit de compacts), et tout sous-ensemble compact P de $\mathbf{P}^1_S(k, M)$ est contenu dans un P_T (recouvrir P par les ouverts $P \cap P_T$, et en extraire un recouvrement fini). Il suffit donc de montrer que l'image réciproque X_T de P_T par β^1 est finie. Il existe une extension finie galoisienne $F \subset k_S$ de k telle que $\operatorname{Gal}(F/k)$ opère trivialement sur M. Pour $v \in T$, l'image de X_T dans $H^1(F, M)$ est non ramifiée en dehors de toute place de F au-dessus de v. Comme le noyau de $H^1(k, M) \to H^1(F, M)$ est fini, il suffit de montrer que cette image est finie, c'est-à-dire qu'on se ramène au cas où l'action de G_S sur M est triviale. Alors $H^1(G_S, M)$ consiste en les homomorphismes continus de G_S dans M. Un tel homomorphisme f a un noyau de la forme $\operatorname{Gal}(G_S/F)$, avec $F \subset k_S$ extension finie galoisienne de degré au plus $d := \#M$. Mais l'hypothèse que la restriction $f_v \in H^1(k_v, M)$ est non ramifiée pour $v \in T$ signifie que F doit être non ramifiée aux places de T. D'après le théorème d'Hermite, il n'existe qu'un nombre fini de telles extensions. Comme pour chaque telle F, le groupe $\operatorname{Hom}(\operatorname{Gal}(F/k), M)$ est lui-même fini, le résultat en découle.

□

À partir de maintenant on désigne par M un G_S-module fini *dont l'ordre est inversible sur $\mathcal{O}_{k,S}$*. En particulier tous les nombres premiers ℓ divi-

sant l'ordre de M sont dans l'ensemble P associé à S comme dans le paragraphe 8.2. On note $M' = \mathrm{Hom}(M, \bar{k}^*) = \mathrm{Hom}(M, k_S^*)$ le G_S-module dual de Cartier de M. Enfin, pour tout groupe topologique abélien A, on note $A^* = \mathrm{Hom}_c(A, \mathbf{Q}/\mathbf{Z})$ le groupe des homomorphismes continus de A dans $\mathbf{Q}/\mathbf{Z}$ (qu'on appellera dual de A) et on équipe A^* de la topologie de la convergence simple.

Remarque : Attention, le groupe A^* est bien le dual de Pontryagin de A si A est profini ou encore discret de torsion, mais pour des groupes abéliens localement compacts [45] et complètement discontinus quelconques, la situation est plus compliquée puisque par exemple avec notre définition, le dual de $\mathbf{Z}$ est $\mathbf{Q}/\mathbf{Z}$ mais celui de $\mathbf{Q}/\mathbf{Z}$ est $\widehat{\mathbf{Z}}$ (ce qui montre que l'appellation traditionnelle de dual de A pour A^* est dangereuse !). Par ailleurs, si

$$0 \to A \to B \to C \to 0$$

est une suite exacte courte (les morphismes étant supposés continus) de groupes abéliens localement compacts et complètement discontinus, la suite duale

$$0 \to C^* \to B^* \to A^* \to 0$$

est bien exacte. On prendra garde que ceci n'implique pas que le dual d'un morphisme continu injectif entre de tels groupes est surjectif, par exemple $\mathbf{Z} \to \mathbf{Z}_p$ est injectif, mais le morphisme dual $\mathbf{Q}_p/\mathbf{Z}_p \to \mathbf{Q}/\mathbf{Z}$ n'est pas surjectif (le problème est que le quotient $\mathbf{Z}_p/\mathbf{Z}$ n'est pas séparé, ou encore que le morphisme considéré n'est pas *strict*. Du coup on n'a pas une suite exacte courte dont les trois termes non nuls restent dans la catégorie considérée).

Proposition 8.27 *a) Le dual $\mathbf{P}^0_S(k, M)^*$ du groupe compact $\mathbf{P}^0_S(k, M)$ est le groupe discret $\mathbf{P}^2_S(k, M')$.*

b) Le dual $\mathbf{P}^1_S(k, M)^*$ du groupe localement compact $\mathbf{P}^1_S(k, M)$ est le groupe localement compact $\mathbf{P}^1_S(k, M')$

Démonstration : Cela résulte immédiatement de la définition de la topologie de produit restreint et des théorèmes 7.14 et 7.23, combinés au lemme 8.25.

□

En utilisant la proposition 8.27, on a pour $i = 0, 1, 2$ des applications continues

$$\gamma^i : \mathbf{P}^i_S(k, M') \to H^{2-i}(G_S, M)^*$$

45. Par convention, "localement compact" signifiera toujours pour nous séparé, localement compact, et dénombrable à l'infini.

obtenues en dualisant β^{2-i}. Pour $i = 1, 2$, on définit

$$Ш^i_S(k, M) = \mathrm{Ker}\,[\beta^i : H^i(G_S, M) \to \mathbf{P}^i_S(k, M)]$$

(on notera parfois $Ш^i_S(M)$ pour $Ш^i_S(k, M)$ si k est sous-entendu.

Nous pouvons maintenant énoncer le résultat principal de ce chapitre (et peut-être de tout ce cours !).

Theorème 8.28 (Poitou-Tate) *Soit M un G_S-module fini dont le cardinal est inversible dans $\mathcal{O}_{k,S}$. Alors :*

a) Pour $r \geq 3$, on a $H^r(G_S, M) \simeq \bigoplus_{v\in\Omega_\mathbf{R}} H^r(k_v, M)$.

b) On a une suite exacte à 9 termes

$$\begin{array}{ccccccc}
0 & \longrightarrow & H^0(G_S, M) & \xrightarrow{\beta_0} & \prod_{v\in S} H^0(k_v, M) & \xrightarrow{\gamma^0} & H^2(G_S, M')^* \\
 & & & & & & \downarrow \\
 & & H^1(G_S, M')^* & \xleftarrow{\gamma_1} & \mathbf{P}^1_S(k, M) & \xleftarrow{\beta_1} & H^1(G_S, M) \\
 & & \downarrow & & & & \\
 & & H^2(G_S, M) & \xrightarrow{\beta_2} & \bigoplus_{v\in S} H^2(k_v, M) & \xrightarrow{\gamma_2} & H^0(G_S, M')^* \longrightarrow 0
\end{array}$$

c) Les groupes $Ш^1_S(k, M')$ et $Ш^2_S(k, M)$ sont finis et duaux.

Noter que le premier terme est fini et les trois termes suivants sont compacts. De façon duale, le dernier terme est fini et les trois termes précédents sont discrets. Le "terme du milieu" $\mathbf{P}^1_S(k, M)$ est seulement localement compact. Si on dualise la suite, on obtient la même suite avec M et M' échangés (via la proposition 8.27).

Corollaire 8.29 *Soit p un nombre premier inversible dans $\mathcal{O}_{k,S}$, et qu'on suppose différent de 2 si k a des places réelles. Alors G_S est de p-dimension cohomologique ≤ 2.*

Démonstration : Cela résulte de l'assertion a) du théorème précédent. □

Remarque : Pour $S = \Omega_k$, on a (sous les mêmes hypothèses) $\mathrm{cd}_p(G_k) = 2$ vu que $H^2(G_k, \mu_p) = (\mathrm{Br}\, k)[p]$ est non nul via le corollaire 8.10 (Brauer-Hasse-Noether). Par ailleurs, la détermination de $\mathrm{scd}_p(G_S)$ est un problème très difficile, qui est encore ouvert en général. On verra dans le prochain chapitre (théorème 9.9) que si S contient presque toutes les places de k, alors $\mathrm{scd}_p(G_S) = 2$ (toujours sous les hypothèses du corollaire précédent). Noter aussi que si p n'est pas inversible dans $\mathcal{O}_{k,S}$, on ne peut a priori pas dire grand chose sur $\mathrm{cd}_p(G_S)$, par exemple si S est l'ensemble de toutes les places archimédiennes G_S pourrait être fini non nul, auquel cas il y a des p tels que $\mathrm{cd}_p(G_S) = +\infty$ (via l'exercice 1 du chapitre 3).

Corollaire 8.30 *Supposons S fini. Soit M un G_S-module fini d'ordre inversible dans $\mathcal{O}_{k,S}$. Alors les groupes $H^r(G_S, M)$ sont finis pour tout $r \geq 0$.*

Démonstration : Ici les groupes $\mathbf{P}^r_S(k, M)$ sont finis via le corollaire 5.13 ; le résultat découle alors de la finitude de $Ш^r_S(k, M)$ pour $r = 1, 2$, et de l'assertion a) du théorème de Poitou-Tate pour $r \geq 3$.

□

8.4. Preuve du théorème de Poitou-Tate

On garde les notations des deux paragraphes précédents. En particulier S est un sous-ensemble de Ω_k contenant toutes les places archimédiennes ; on note I_S la limite inductive des groupes d'idèles ("restreints à S") $I_{F,S}$ (pour F extension finie galoisienne de k incluse dans k_S) et C_S la limite inductive des $C_S(F)$. D'après le lemme 8.19 a), le groupe C_S est aussi la limite inductive des $C_{F,S} = I_{F,S}/\mathcal{O}^*_{F,S}$; posons alors

$$E_{F,S} = \mathcal{O}^*_{F,S}; \quad E_S = \varinjlim_{F \subset k_S} E_{F,S}$$

La suite exacte

$$0 \to E_{F,S} \to I_{F,S} \to C_{F,S} \to 0$$

qui définit $C_{F,S}$ donne alors en passant à la limite une suite exacte

$$0 \to E_S \to I_S \to C_S \to 0 \tag{12}$$

Le théorème va être obtenu en écrivant la suite exacte longue obtenue en appliquant le foncteur $\mathrm{Hom}_{G_S}(M', .)$ à cette suite exacte, et en calculant les Ext qui apparaissent. Pour C_S, les Ext correspondant ont déjà été calculés dans le théorème 8.22 en utilisant le théorème de dualité générale pour une P-formation de classes.

Lemme 8.31 *Soit M un G_S-module fini, dont le cardinal est inversible dans $\mathcal{O}_{k,S}$. Alors :*

a) Pour tout $r \geq 0$, on a $\mathrm{Ext}^r_{G_S}(M, E_S) = H^r(G_S, M')$.

b) Pour toute place v non dans S et tout $r \geq 0$, on a $H^r(k(v), M') = \mathrm{Ext}^r_{G(v)}(M, \mathcal{O}_v^{\mathrm{nr}^*})$, et les deux groupes sont nuls pour $r \geq 2$.

Notons que pour la première assertion M' désigne le G_S-module $\mathrm{Hom}(M, k_S^*)$ qui est aussi $\mathrm{Hom}(M, E_S)$ parce que $\#M$ est inversible dans $\mathcal{O}_{k,S}$. Pour la deuxième assertion, on regarde M comme un $G(v)$-module (comme $v \notin S$, M est non ramifié en v) et M' désigne son dual $\mathrm{Hom}(M, \overline{k(v)}^*)$. La notation $\mathcal{O}_v^{\mathrm{nr}}$ signifie qu'on considère l'extension maximale non ramifiée de $\mathcal{O}_v$, i.e. l'anneau des entiers de k_v^{nr}.

Démonstration : a) Par définition E_S est ℓ-divisible pour tout nombre premier ℓ inversible dans $\mathcal{O}_{k,S}$. Alors la multiplication par un tel ℓ est surjective dans $\mathrm{Ext}^1_{\mathbf{Z}}(M, E_S)$ via la suite exacte

$$0 \to E_S[\ell] \to E_S \xrightarrow{\cdot \ell} E_S \to 0$$

et le fait que les $\mathrm{Ext}^2_{\mathbf{Z}}$ sont toujours nuls. On en déduit que la multiplication par $\#M$ est surjective et nulle dans $\mathrm{Ext}^1_{\mathbf{Z}}(M, E_S)$, donc finalement $\mathrm{Ext}^1_{\mathbf{Z}}(M, E_S) = 0$. La suite exacte (6) (qui provenait de la suite spectrale des Ext, i.e. du théorème 6.24) donne alors le résultat.

b) C'est similaire, $\mathcal{O}_v^{\mathrm{nr}^*}$ étant ℓ-divisible pour tout ℓ divisant $\#M$ vu que $v \notin S$ (donc v ne divise pas ℓ). D'autre part $H^r(k(v), M') = 0$ si $r \geq 2$ parce que la dimension cohomologique du corps fini $k(v)$ est 1.

□

Le calcul pour I_S est nettement plus compliqué et fait l'objet de la proposition suivante, qui est le coeur de la démonstration du théorème de Poitou-Tate.

Proposition 8.32 *Soit M un G_S-module fini dont le cardinal est inversible dans $\mathcal{O}_{k,S}$. Alors pour tout $r \geq 1$, on a :*

$$\mathrm{Ext}^r_{G_S}(M, I_S) = \mathbf{P}^r_S(k, M')$$

On va travailler avec des sous-ensembles $T \subset S$ finis, vérifiant en outre : T contient toutes les places archimédiennes, les places où M est ramifié, et les places au-dessus des nombres premiers divisant $\#M$. On considère alors les extension finies galoisiennes $F \subset k_S$ telles que l'action de $\mathrm{Gal}\,(k_S/F)$ sur M soit triviale ; comme d'habitude on note (pour $v \in S$) F_v le complété de F en une place au-dessus de v.

Lemme 8.33 *Avec les notations ci-dessus, on a*

$$\mathrm{Ext}^r_{G_S}(M, I_S) = \varinjlim_{F,T} [\prod_{v\in T} \mathrm{Ext}^r_{\mathrm{Gal}\,(F_v/k_v)}(M, F_v^*) \times \prod_{v\in S-T} \mathrm{Ext}^r_{\mathrm{Gal}\,(F_v/k_v)}(M, \mathcal{O}^*_{F_v})]$$

la limite étant prise sur les paires $F \subset k_T$, vérifiant les conditions ci-dessus.

Démonstration : Soit $F \subset k_S$ comme ci-dessus. Soit T_F (resp. S_F) l'ensemble des places de F au-dessus de T (resp. de S). On pose alors

$$I_{F,S\supset T} := \prod_{w\in T_F} F_w^* \times \prod_{w\in S_F - T_F} \mathcal{O}_w^*$$

où F_w est le complété de F en w et $\mathcal{O}_w$ son anneau des entiers. On obtient en particulier

$$I_S = \varinjlim_{F,T} I_{F,S\supset T}$$

vu que pour F fixé, on a

$$\varinjlim_{T\subset S} I_{F,S\supset T} = I_{F,S}$$

(rappelons que $I_{F,S}$ est le produit restreint des F_w^* pour w place de S_F). Il résulte alors de la suite exacte (6) qu'on a :

$$\mathrm{Ext}^r_{G_S}(M, I_S) = \varinjlim_{F,T} \mathrm{Ext}^r_{\mathrm{Gal}\,(F/k)}(M, I_{F,S\supset T})$$

car pour la cohomologie, la propriété analogue est connue (proposition 3.8). Maintenant, on utilise le fait que les $\mathrm{Ext}^r_{\mathrm{Gal}\,(F/k)}(M, .)$ commutent aux produits (pour le voir il suffit de les calculer via une résolution projective de M). D'autre part, si w_1 est une place de F au-dessus de $v \in S$, le groupe $\mathrm{Gal}\,(F_{w_1}/k_v)$ s'identifie à un sous-groupe de décomposition de $\mathrm{Gal}\,(F/k)$, et le $\mathrm{Gal}\,(F/k)$-module $\prod_{w|v} F_w^*$ (resp. $\prod_{w|v} \mathcal{O}_w^*$) au module induit de $F_{w_1}^*$ (resp. $\mathcal{O}_{w_1}^*$) relativement à ce sous-groupe. Le résultat en découle via le "lemme de Shapiro pour les Ext" (qu'on a déjà utilisé dans la preuve du théorème 6.29).

□

L'un des termes qui apparaissent est plus facile à calculer :

Lemme 8.34 *Soit $v \in S - T$. Alors*

$$\mathrm{Ext}^r_{\mathrm{Gal}\,(F_v/k_v)}(M, \mathcal{O}^*_{F_v}) = H^r(G(v), M')$$

et ce groupe est nul si $r \geq 2$.

Démonstration : Comme le G_v-module $\mathcal{O}_v^{\mathrm{nr}^*}$ est cohomologiquement trivial, la suite spectrale des Ext (théorème 6.24, qu'on applique ici avec $N = \mathbf{Z}$) donne alors, pour $v \in S - T$:

$$\mathrm{Ext}^r_{\mathrm{Gal}\,(F_v/k_v)}(M, \mathcal{O}^*_{F_v}) = \mathrm{Ext}^r_{G(v)}(M, \mathcal{O}_v^{\mathrm{nr}^*})$$

qui vaut $H^r(G(v), M')$ d'après le lemme 8.31. Si $r \geq 2$ ce groupe est nul car $G(v)$ est de dimension cohomologique 1.

□

Pour conclure, il faut distinguer les cas $r \geq 2$ et $r = 1$:

Lemme 8.35 *a) Soit $r \geq 2$. Alors*

$$\varinjlim_{F,T} \prod_{v\in T} \mathrm{Ext}^r_{\mathrm{Gal}\,(F_v/k_v)}(M, F_v^*) = \bigoplus_{v\in S} H^r(k_v, M')$$

b) Pour $r = 1$, on a

$$\varinjlim_{F,T} [\prod_{v\in T} \mathrm{Ext}^1_{\mathrm{Gal}\,(F_v/k_v)}(M, F_v^*) \times \prod_{v\in S-T} \mathrm{Ext}^1_{\mathrm{Gal}\,(F_v/k_v)}(M, \mathcal{O}^*_{F_v})] = P^1_S(k, M)$$

.

Démonstration : Si $r \geq 2$, on observe que

$$\varinjlim_{F,T} \prod_{v\in T} \mathrm{Ext}^r_{\mathrm{Gal}\,(F_v/k_v)}(M, F_v^*) = \varinjlim \bigoplus_{v\in S} \mathrm{Ext}^r_{\mathrm{Gal}\,(F_v/k_v)}(M, F_v^*)$$

la limite étant prise sur les extensions finies $F \subset k_S$ de k. Soit alors ℓ un diviseur premier du cardinal de M. Comme par hypothèse $\ell \in \mathcal{O}^*_{k,S}$, on sait que ℓ^∞ divise alors l'ordre de G_S et on en déduit, pour toute place v de S :

$$\varinjlim_{F\subset k_S} (\mathrm{Br}\, F_v)\{\ell\} = 0$$

(via la proposition 5.8) ou encore

$$\varinjlim_{F\subset k_S} H^2(\mathrm{Gal}\,(\bar{k}_v/F_v), \bar{k}_v^*)\{\ell\} = 0$$

On a d'autre part également

$$\varinjlim_{F\subset k_S} H^r(\mathrm{Gal}\,(\bar{k}_v/F_v), \bar{k}_v^*)\{\ell\} = 0$$

pour $r = 1$ (Hilbert 90) et pour $r \geq 3$ (si v est finie cela résulte de $\mathrm{scd}(F_v) = 2$ et si v est réelle du théorème 2.10 joint au cas $r = 2$). La suite spectrale des Ext (théorème 6.24 appliqué encore avec $N = \mathbf{Z}$) donne alors

$$\varinjlim_{F\subset k_S} \mathrm{Ext}^r_{\mathrm{Gal}\,(F_v/k_v)}(M, F_v^*) = \mathrm{Ext}^r_{G_v}(M, \bar{k}_v^*)$$

et ce dernier terme vaut bien $H^r(G_v, M') = H^r(k_v, M')$, par le même argument que dans le lemme 8.31 a) (qui utilise la suite exacte (6)).
Reste à traiter le cas $r = 1$. La suite spectrale des Ext et le théorème de Hilbert 90 donnent pour $v \in T$:

$$\mathrm{Ext}^1_{\mathrm{Gal}\,(F_v/k_v)}(M, F_v^*) = \mathrm{Ext}^1_{G_v}(M, \bar{k}_v^*)$$

qui vaut encore $H^1(G_v, M')$ comme on l'a déjà vu ; ce terme est indépendant de F. D'autre part, pour $v \in S - T$, le lemme 8.31 donne que

$$\mathrm{Ext}^1_{\mathrm{Gal}\,(F_v/k_v)}(M, \mathcal{O}_{F_v}^*) = H^1(G(v), M') \simeq H^1_{\mathrm{nr}}(k_v, M')$$

est encore indépendant de F. Ceci donne finalement que le terme à calculer est

$$\varinjlim_T [\prod_{v\in T} H^1(k_v, M') \times \prod_{v\in S-T} H^1_{\mathrm{nr}}(k_v, M')]$$

la limite étant prise sur les $T \subset S$ finis. Par définition du produit restreint, cette limite vaut précisément $\mathbf{P}^1_S(k, M')$.

□

La proposition 8.32 résulte alors des lemmes 8.33, 8.34, et 8.35 a) si $r \geq 2$ et des lemmes 8.33 et 8.35 b) si $r = 1$.

□

Preuve du théorème de Poitou-Tate : On utilise la suite exacte

$$0 \to E_S \to I_S \to C_S \to 0$$

et les résultats précédents pour identifier les termes de la longue suite exacte $\mathrm{Ext}^r_{G_S}(M', -)$.

a) Supposons d'abord $r \geq 4$. Alors la proposition 8.32, le théorème 8.22 et le lemme 8.31 donnent alors tout de suite le résultat car dans ce cas $\mathrm{Ext}^{r-1}(G_S, C_S)$ et $\mathrm{Ext}^r(G_S, C_S)$ sont nuls. En appliquant la proposition 8.32 pour $r = 2, 3$, le lemme 8.31 pour $r = 3$, et le théorème 8.22 pour $r = 2, 3$, on obtient une suite exacte

$$\mathbf{P}^2_S(k, M) \to H^0(G_S, M')^* \to H^3(G_S, M) \to \mathbf{P}^3_S(k, M) \to 0$$

La flèche $H^0(G_S, M') \to \prod_{v\in S} H^0(k_v, M')$ est injective puisque pour M non nul, S contient au moins une place finie (rappelons que le cardinal de M est inversible dans $\mathcal{O}_{k,S}$ par hypothèse). Comme c'est une flèche entre groupes compacts (le premier est même fini), sa flèche duale est surjective. Or d'après la proposition 8.27, cette flèche duale est précisément $\mathbf{P}^2_S(k, M) \to H^0(G_S, M')^*$, qui est donc surjective.

b) Les six derniers termes s'obtiennent en appliquant le lemme 8.31, le théorème 8.32 et le théorème 8.22 pour $r = 1, 2$. On obtient alors les trois premiers termes en échangeant M et M', puis en dualisant via la proposition 8.27 (ce qui ne pose pas ici de problèmes puisqu'on dualise une suite de groupes discrets).

c) Toujours avec la proposition 8.27, on peut récrire les trois termes du milieu de la suite :

$$\mathbf{P}^1_S(k, M')^* \to H^1(G_S, M')^* \to Ш^2_S(k, M) \to 0$$

ce qui prouve que $Ш^2_S(k, M)$ est dual de $Ш^1_S(k, M')$, qui est fini via la proposition 8.26.

□

Remarques : a) Le fait que ce soient bien les flèches γ_i qui apparaissent dans la suite de Poitou-Tate résulte de leurs définitions et de la compatibilité entre les accouplements donnés par les cup-produits et ceux donnés par les Ext (proposition 6.26). L'identification des flèches β_i est immédiate (elles sont induites par les inclusions $F^* \to F_v^*$, tout comme la flèche $E_S \to I_S$). Les flèches "sans nom" sont plus compliquées ; on peut les préciser via une description explicite de l'accouplement entre $Ш^1_S(M)$ et $Ш^2_S(M')$, cf. [10], p. 65.

b) La finitude de $Ш^2_S(M)$ permet de déduire immédiatement l'analogue de la proposition 8.26 en degré 2 puisque dans ce cas $\mathbf{P}^2_S(M)$ est discret. Il semble difficile (impossible ?) de démontrer cet analogue directement !

8.5. Exercices

1. Soit k un corps de nombres. Soit S un sous-ensemble de Ω_k contenant les places archimédiennes. Soit ℓ un nombre premier inversible dans $\mathcal{O}_{k,S}$. On suppose que $H^2(G_S, \mathbf{Q}_\ell/\mathbf{Z}_\ell) = 0$ (avec les notations du texte). Montrer que l'homomorphisme α^0 du théorème 8.22 est surjectif (la question de savoir si $H^2(G_S, \mathbf{Q}_\ell/\mathbf{Z}_\ell) = 0$ pour S quelconque, sous l'hypothèse habituelle que $\ell \neq 2$ si k a des places réelles, est ouverte).

2. Avec les notations du texte, soit M un G_S-module fini dont l'ordre est inversible dans $\mathcal{O}_{k,S}$. Soit T un sous-ensemble fini de S tel qu'il existe au moins une place finie de S qui n'est pas dans T. On fixe une telle place w.

a) Soit $\chi : H^0(k, M') \to \mathbf{Q}/\mathbf{Z}$ un caractère de $H^0(k, M')$. Montrer qu'il existe $a_w \in H^2(k_w, M)$ tel que pour tout b de $H^0(k, M')$, on ait $-(a_w \cup b_w) = \chi(b)$, où b_w est l'image de b dans $H^0(k_w, M')$.

b) En déduire que l'application diagonale

$$H^2(G_S, M) \to \bigoplus_{v \in T} H^2(k_v, M)$$

est surjective.

9. Quelques applications

On garde les notations du chapitre précédent. En particulier k désigne un corps de nombres, S un ensemble de places de k (contenant toutes les places archimédiennes) et $G_S = \mathrm{Gal}\,(k_S/k)$ est le groupe de Galois de l'extension maximale de k non ramifiée en dehors de S. On note également $\mathcal{O}_S = \mathcal{O}_{k,S}$ l'anneau des S-entiers.

9.1. Nullité de certains $Ш^i$

Le but de ce paragraphe est de présenter quelques résultats d'annulation des groupes $Ш^i(G_S, M)$ quand M est un G_S-module fini et l'ensemble S est "gros". On va voir en particulier que si S contient presque toutes les places de k, alors $Ш^1_S(M) = 0$ si l'action de G_S sur M est triviale, et le même résultat vaut si l'action de G_S sur le dual de Cartier M' est triviale pourvu qu'on évite un cas particulier. On commence par rappeler l'important théorème de théorie des nombres suivant :

Theorème 9.1 (Čebotarev) *Soit L une extension finie galoisienne k dont on note G le groupe de Galois. Soit C une classe de conjugaison de G. Pour toute place finie v de k qui est non ramifiée dans l'extension L/k, on note* Frob_v *le Frobenius en v (c'est un élément de G bien défini à conjugaison près). Alors la densité de Dirichlet $\delta_{L/k}(C)$ des places v telles que* $\mathrm{Frob}_v \in C$ *est*

$$\delta_{L/k}(C) = \#C/\#G$$

Pour une preuve, voir [11], chapitre VII, (13.6.). Rappelons que la densité de Dirichlet d'un ensemble d'idéaux premiers S de $\mathcal{O}_k$ (correspondant à un sous-ensemble S de l'ensemble Ω_f des places finies de k) est la limite (si elle existe)

$$\delta(S) := \lim_{s \to 1} \frac{\sum_{\wp \in S} N\wp^{-s}}{\sum_{\wp \in \Omega_f} N\wp^{-s}}$$

Le théorème de Čebotarev implique en particulier que la "proportion" de places v totalement décomposées dans l'extension L/k est $1/[L : k]$.

Proposition 9.2 *Soit S un ensemble de places de k contenant toutes les places archimédiennes. Soit A un groupe abélien fini muni de l'action triviale de G_S. Soit $T \subset S$ un ensemble de places tel que $\delta(T) > 1/p$, où p est le plus petit diviseur premier de $\#A$. Alors l' application*

$$H^1(G_S, A) \to \prod_{v \in T} H^1(k_v, A)$$

est injective. En particulier si $\delta(S) > 1/p$ on a $Ш^1_S(A) = 0$.

Démonstration : On se ramène immédiatement au cas $A = \mathbf{Z}/l^r\mathbf{Z}$ avec $r \in \mathbf{N}^*$ et l premier. Le noyau de l'application considérée correspond alors aux homomorphismes continus

$$\varphi : G_S \to \mathbf{Z}/l^r\mathbf{Z}$$

dont la restriction au sous-groupe de décomposition en v est triviale pour toute place v de T. Le noyau de φ est donc de la forme $\mathrm{Gal}\,(k_S/L)$, où L est une extension finie de k qui est de degré l^s (avec $s \leq r$ et $l \geq p$) et totalement décomposée aux places de T. Comme $\delta(T) > 1/p \geq 1/l$, le théorème de Čebotarev implique $s = 0$, c'est à dire que φ est l'homomorphisme trivial.

□

Corollaire 9.3 *Soit S un ensemble de places de k contenant toutes les places archimédiennes. Soit A un G_S-module fini, d'ordre inversible dans $\mathcal{O}_S$, et tel que l'action de G_S sur le dual de Cartier A' soit triviale. On suppose de plus que $\delta(S) > 1/p$, où p est le plus petit diviseur premier de $\#A$. Alors $Ш^2_S(A) = 0$.*

Démonstration : Cela résulte de la proposition précédente et de la dualité de Poitou-Tate entre $Ш^2_S(A)$ et $Ш^1_S(A')$.

□

L'étude de $Ш^1_S(A)$ quand l'action de G_S sur A' est triviale (ex. $A = \mu_n$) est plus compliquée. On aura besoin du lemme suivant :

Lemme 9.4 *Soit p un nombre premier. Soit $m > 0$ et soit G un sous-groupe de $(\mathbf{Z}/p^m\mathbf{Z})^*$ qu'on peut voir aussi comme un sous-groupe de $\mathtt{Aut}\,(\mathbf{Z}/p^m\mathbf{Z})$. Soit A le G-module isomorphe à $\mathbf{Z}/p^m\mathbf{Z}$ comme groupe abélien, avec l'action naturelle de G. Alors*

$$\widehat{H}^i(G, A) = 0 \quad \forall i \in \mathbf{Z}$$

sauf dans le cas $p = 2$, $m \geq 2$, et $-1 \in G$, auquel cas $\widehat{H}^i(G, A) = \mathbf{Z}/2$ pour tout $i \in \mathbf{Z}$.

Démonstration : Supposons d'abord $p \neq 2$. Alors le groupe $(\mathbf{Z}/p^m\mathbf{Z})^*$ est cyclique d'ordre $p^{m-1}(p-1)$, et le p-Sylow de G est le groupe $G_1 = \ker[G \to (\mathbf{Z}/p\mathbf{Z})^*]$. On est donc ramené au cas où tous les éléments de G sont dans ce noyau. Fixons alors un générateur α de G et notons p^{m-s} son ordre (avec $s \geq 1$). On peut écrire $\alpha = 1+p^s u$ avec $v_p(u) = 0$. Alors A^G est le noyau de $\alpha - 1 : A \to A$, ce qui donne $A^G = p^{m-s}A$. D'autre part on a

$$\sum_{i=0}^{p^{m-s}-1} \alpha^i = \frac{\alpha^{p^{m-s}} - 1}{\alpha - 1} = p^{m-s}v$$

avec $v_p(v) = 0$, d'où $N_G(A) = p^{m-s}A = A^G$. Finalement $\widehat{H}^0(G, A) = 0$ et on conclut avec l'exercice 3 b) du chapitre 2 et le théorème 2.10.

Supposons maintenant $p = 2$ (et $m \geq 2$). Le cas où G est cyclique et engendré par un α avec $v_2(\alpha - 1) \geq 2$ se traite exactement comme le cas $p \neq 2$. Supposons G cyclique, engendré par α tel que $v_2(\alpha - 1) = 1$; alors $v_2(-\alpha - 1) = s$ avec $2 \leq s \leq m - 1$. Comme $v_2(\alpha - 1) = 1$, on a $A^G = 2^{m-1}A$ et l'ordre de G est $2^{m-s} \geq 2$. On en déduit comme dans le cas p impair que $N_G(A) = 2^{m-1}A$ et on conclut de la même façon.

Reste le cas où G est de la forme $G = \{\pm 1\} \times < \alpha >$ avec $v_2(\alpha - 1) \geq 2$, qui est le seul cas où $p = 2$ et $-1 \in G$. Soit alors 2^{m-s} l'ordre du sous-groupe H engendré par α. Dans ce cas on a

$$\sum_{i=0}^{2^{m-s}-1} \alpha^i + \sum_{i=0}^{2^{m-s}-1} -\alpha^i = 0$$

ce qui donne $N_G A = 0$. De plus $A^G = 2^{m-1}A$ et $I_G A = 2A$, d'où $\widehat{H}^i(G, A) = \mathbf{Z}/2$ pour $i = -1, 0$. Comme d'après ce qui précède on a $\widehat{H}^i(H, A) = 0$ pour tout i, le corollaire 1.24 donne pour tout $i \geq 1$, que

$$H^i(G, A) = H^i(\{\pm 1\}, A^H) = H^i(\{\pm 1\}, 2^{m-s}A)$$

dont le cardinal est celui de $\widehat{H}^0(\{\pm 1\}, 2^{m-s}A)$ (puisque $\{\pm 1\}$ est cyclique), c'est-à-dire 2. Le même argument avec l'homologie donne que le cardinal de $\widehat{H}^i(G, A)$ est 2 pour $i < -1$.

□

Corollaire 9.5 *Soit p un nombre premier et $r \in \mathbf{N}$. On note $k(\mu_{p^r})$ le corps obtenu en adjoignant les racines p^r-ièmes de l'unité à k et on pose $G_{p^r} := \mathrm{Gal}\,(k(\mu_{p^r})/k)$. Dans le cas $p = 2$, on suppose de plus que $\sqrt{-1} \in k$. Alors on a*

$$\widehat{H}^i(G_{p^r}, \mu_{p^r}) = 0$$

pour tout $i \in \mathbf{Z}$.

Démonstration : On peut voir G_{p^r} comme un sous-groupe du groupe $\mathtt{Aut}\,(\mathbf{Z}/p^r\mathbf{Z})$ car le groupe μ_{p^r} est cyclique d'ordre p^r. Il suffit alors d'appliquer le lemme 9.4, l'hypothèse faite dans le cas $p = 2$ assurant que l'on n'est pas dans le cas exceptionnel vu que pour $p = 2$ la conjugaison complexe n'opère pas trivialement sur $\sqrt{-1} \in k$, donc n'est pas dans G_{p^r}.

□

Remarque : On peut déterminer exactement quand $\widehat{H}^i(G_{p^r}, \mu_{p^r}) \neq 0$, cf. [12], pp. 526–527.

Theorème 9.6 *Soit S un ensemble de places de k contenant toutes les places archimédiennes. Soient $p_1, ..., p_n$ des nombres premiers deux à deux distincts dans $\mathcal{O}_S^*$ et m un entier de la forme $m = p_1^{r_1}...p_n^{r_n}$. Soit T un sous-ensemble de S, on suppose que T contient presque toutes les places de k. On suppose enfin que $\sqrt{-1} \in k$ si l'un des p_i est 2. Alors l'homomorphisme*

$$\varphi_{S,T,m} : H^1(G_S, \mu_m) \to \prod_{v \in T} H^1(k_v, \mu_m)$$

est injectif. En particulier $Ш^1_S(k, \mu_m) = 0$.

Remarque : On peut affaiblir l'hypothèse sur T (en la formulant en terme de densité de Dirichlet ; en particulier la preuve fonctionne si on suppose T de densité de Dirichlet 1), et aussi décrire plus précisément le cas exceptionnel quand l'un des p_i est 2.

Démonstration : On se ramène immédiatement au cas où $m = p^r$. Soit alors $K = k(\mu_m)$. Alors K est bien une sous-extension de k_S car m est inversible dans $\mathcal{O}_S^*$. On pose $G = \mathrm{Gal}\,(K/k)$ et on note G_v le sous-groupe de décomposition de K/k en v. Notons $Ш^1_S(T, m)$ le noyau de $\varphi_{S,T,m}$ et $Ш^1(K, T, m)$ celui de l'homomorphisme $H^1(G, \mu_m) \to \prod_{v \in T} H^1(G_v, \mu_m)$. Soit T_K l'ensemble des places de K au-dessus d'une place de T. On a (via la suite exacte de restriction-inflation) un diagramme commutatif exact

$$\begin{array}{ccccccc}
0 & \longrightarrow & Ш^1(K, T, m) & \longrightarrow & H^1(G, \mu_m) & \longrightarrow & \prod_{v \in T} H^1(G_v, \mu_m) \\
 & & \downarrow & & \downarrow & & \downarrow \\
0 & \longrightarrow & Ш^1_S(T, m) & \longrightarrow & H^1(G_S, \mu_m) & \longrightarrow & \prod_{v \in T} H^1(k_v, \mu_m) \\
 & & & & \downarrow & & \downarrow \\
 & & & & H^1(G_{K,S}, \mu_m) & \longrightarrow & \prod_{w \in T_K} H^1(K_w, \mu_m)
\end{array}$$

où $G_{K,S} := \mathrm{Gal}\,(k_S/K)$ et la flèche verticale en bas à droite est induite par les flèches $H^1(k_v, \mu_m) \to \prod_{w|v} H^1(K_w, \mu_m)$ pour $v \in T$. Comme l'action de $G_{K,S}$ sur μ_m est triviale, la proposition 9.2 dit que la flèche horizontale du bas est injective. D'autre part $H^1(G, \mu_m) = 0$ via le corollaire 9.5 et on obtient bien que $Ш^1_S(T, m) = 0$ comme on voulait.

□

Corollaire 9.7 *Soit S un ensemble de places de k contenant toutes les places archimdiennes et tel que $\Omega_k - S$ soit fini. Soient $p_1, ..., p_n$ des nombres premiers deux à deux distincts dans $\mathcal{O}_S^*$ et m un entier de la forme $m = p_1^{r_1}...p_n^{r_n}$. On suppose de plus que $\sqrt{-1} \in k$ si l'un des p_i est 2. Alors $Ш^2_S(k, \mathbf{Z}/m) = 0$.*

Démonstration : Cela résulte de la dualité de Poitou-Tate entre les groupes $Ш^2_S(k, \mathbf{Z}/m)$ et $Ш^1_S(k, \mu_m)$, et du théorème 9.6.

□

Corollaire 9.8 *Soit $m \geq 1$ un entier. Soit T un sous-ensemble de places de k avec $\Omega_k - T$ fini. On suppose de plus que $\sqrt{-1} \in k$ si m est pair. Alors l'application*

$$k^*/k^{*^m} \to \prod_{v \in T} k_v^*/k_v^{*^m}$$

est injective.

Démonstration : On a $H^1(k, \mu_m) = k^*/k^{*^m}$ et $H^1(k_v, \mu_m) = k_v^*/k_v^{*^m}$. On applique alors le théorème 9.6 avec $S = \Omega_k$.

□

Remarque : Le même résultat vaut (avec la même preuve) si T est seulement supposé de densité de Dirichlet 1. De même dans le corollaire 9.7 il est suffisant de supposer S de densité de Dirichlet 1.

9.2. Dimension cohomologique stricte d'un corps de nombres

Soit S un ensemble de places de k tel que S contienne toutes les places archimédiennes. Comme on l'a déjà dit, déterminer $\mathrm{scd}_p(G_S)$ pour p premier inversible dans $\mathcal{O}_S$ est un problème ouvert en général. On a cependant une réponse quand S contient presque toutes les places de k.

Theorème 9.9 *Soit k un corps de nombres. Soit S un ensemble de places de k contenant toutes les places archimédiennes et tel que $\Omega_k - S$ soit fini. Soit p un nombre premier inversible dans $\mathcal{O}_S$. On suppose de plus que k est totalement imaginaire si $p = 2$. Alors* $\mathrm{scd}_p(G_S) = 2$.

En particulier on a $\mathrm{scd}(k) = 2$ pour tout corps de nombres totalement imaginaire.

Démonstration : D'après le corollaire 8.29, on a $\mathrm{cd}_p(G_S) \leq 2$. D'autre part p (et même p^∞) divise l'ordre de G_S, ce qui implique qu'il existe des extensions cycliques de degré p de k incluses dans k_S, et donc en particulier que $H^2(G_S, \mathbf{Z})[p] = H^1(G_S, \mathbf{Q}/\mathbf{Z})[p]$ est non nul. On en déduit que $\mathrm{scd}_p(G_S) \geq 2$. Il suffit donc, d'après la proposition 3.23, de vérifier que $H^2(U, \mathbf{Q}_p/\mathbf{Z}_p) = 0$ pour tout sous-groupe ouvert U de G_S. Comme toute extension finie de k incluse dans k_S vérifie les mêmes hypothèses, on est ramené à montrer que $H^2(G_S, \mathbf{Q}_p/\mathbf{Z}_p) = 0$. Si p est impair ou $\sqrt{-1} \in k$, le corollaire 9.7 donne, en passant à la limite, que l'application

$$H^2(G_S, \mathbf{Q}_p/\mathbf{Z}_p) \to \prod_{v \in S} H^2(k_v, \mathbf{Q}_p/\mathbf{Z}_p)$$

est injective. On conclut avec le fait que $\mathrm{scd}_p(k_v) = 2$ pour v finie (et pour v archimédienne, les hypothèses impliquent $\mathrm{scd}_p(k_v) = 0$).

Si maintenant $p = 2$ et $\sqrt{-1} \notin k$, alors d'après ce qu'on vient de voir si on pose $K = k(\sqrt{-1})$, on a $H^2(G_{K,S}, \mathbf{Q}_2/\mathbf{Z}_2) = 0$, où $G_{K,S} = \mathrm{Gal}\,(k_S/K)$. Mais on sait que la corestriction

$$H^2(G_{K,S}, \mathbf{Q}_2/\mathbf{Z}_2) \to H^2(G_S, \mathbf{Q}_2/\mathbf{Z}_2)$$

est surjective (lemme 3.20) puisque $cd_2(G_S) = 2$, d'où le résultat.

□

Remarque : Là encore, supposer S de densité de Dirichlet 1 est suffisant.

Corollaire 9.10 *On a $H^3(k, \mathbf{Z}) = 0$ et pour $r \geq 4$, l'application naturelle*

$$H^r(k, \mathbf{Z}) \to \bigoplus_{v \in \Omega_{\mathbf{R}}} H^r(k_v, \mathbf{Z})$$

est un isomorphisme. En particulier pour $r \geq 3$, le groupe $H^r(k, \mathbf{Z})$ est nul si r est impair, et isomorphe à $(\mathbf{Z}/2)^t$ si r est pair, où t est le nombre de places réelles de k.

Démonstration : Supposons d'abord $r \geq 4$. Alors

$$H^r(k, \mathbf{Z}) = H^{r-1}(k, \mathbf{Q}/\mathbf{Z}) = \varinjlim_n H^{r-1}(k, \mathbf{Z}/n)$$

est aussi isomorphe à $\varinjlim_n \bigoplus_{v \in \Omega_{\mathbf{R}}} H^{r-1}(k_v, \mathbf{Z}/n)$ via le théorème de Poitou-Tate appliqué aux $\mathbf{Z}/n$ (puisque $(r-1) \geq 3$), et ce dernier groupe est aussi $\bigoplus_{v \in \Omega_{\mathbf{R}}} H^{r-1}(k_v, \mathbf{Q}/\mathbf{Z})$. Le résultat en découle (pour la dernière assertion, on observe que pour v réelle, le groupe $H^r(k_v, \mathbf{Z})$ est isomorphe à $H^1(\mathbf{R}, \mathbf{Z})$ si r est impair et à $\widehat{H}^0(\mathbf{R}, \mathbf{Z})$ si r est pair via le théorème 2.10).

Il reste à montrer que $H^3(k, \mathbf{Z}) = 0$. Si $\sqrt{-1} \in k$, alors k est totalement imaginaire et le résultat découle du théorème 9.9. Sinon posons $L = k(\sqrt{-1})$ et notons $U = \mathrm{Gal}\,(\bar{k}/L)$, le corps L (et donc le groupe profini U) est de dimension cohomologique stricte 2, ce qui implique, pour tout $r \geq 3$, $H^r(G, \mathbf{Z}[G/U]) = H^r(U, \mathbf{Z}) = 0$. Soit $G = \mathrm{Gal}\,(\bar{k}/k)$ et soit σ le générateur du groupe G/U (qui est d'ordre 2), on a une suite exacte de G-modules

$$0 \to \mathbf{Z} \overset{1+\sigma}{\to} \mathbf{Z}[G/U] \overset{1-\sigma}{\to} \mathbf{Z}[G/U] \overset{\sigma \to 1}{\to} \mathbf{Z} \to 0$$

qui fournit (en coupant cette suite exacte en deux suites exactes courtes) des isomorphismes $H^r(G, \mathbf{Z}) \to H^{r+2}(G, \mathbf{Z})$ pour tout entier $r \geq 3$. En particulier on a $H^3(G, \mathbf{Z}) = H^5(G, \mathbf{Z}) = 0$.

□

9.3. Exercices

1. Soit k un corps de nombres. Soient S un ensemble de places de k contenant toutes les places archimédiennes et T un sous-ensemble fini de S. Soit A un G_S-module fini dont l'ordre est inversible dans $\mathcal{O}_{k,S}$, on note A' le dual de Cartier de A.

a) On note N le noyau de l'application naturelle

$$H^1(G_S, A') \to \prod_{v \in S-T} H^1(k_v, A')$$

et C le conoyau de la flèche $\beta^1_{S,T} : H^1(G_S, A) \to \bigoplus_{v \in T} H^1(k_v, A)$. Montrer qu'on a une suite exacte

$$0 \to Ш^1_S(k, A') \to N \to C^* \to 0$$

b) On suppose que l'action de G_S sur A' est triviale et que la densité $\delta(S)$ est au moins $1/p$, où p est le plus petit diviseur premier de $\#A$. Montrer que $\beta^1_{S,T}$ est surjective.

c) On suppose que $A = \mathbf{Z}/m\mathbf{Z}$ (avec action triviale de G_S) avec m inversible dans $\mathcal{O}_{k,S}$. On fait l'hypothèse supplémentaire que S contient presque toutes les places de k. Montrer que si m est impair ou si $\sqrt{-1} \in k$, alors $\beta^1_{S,T}$ est surjective.

2. Soit $k = \mathbf{Q}(\sqrt{7})$. Montrer que l'homomorphisme naturel

$$k^*/k^{*8} \to \prod_{v \in \Omega_k} k_v^*/k_v^{*8}$$

n'est pas injectif (on observera que $16 = 2^4 = (-2)^4 = (1+\sqrt{-1})^8$).

Références

[1] N. Bourbaki : *Algèbre*, chapitre V, Hermann, Paris, 1959.

[2] N. Bourbaki : *Algèbre commutative*, chapitre VII, Hermann, Paris, 1972.

[3] J.W.S. Cassels, A. Fröhlich : *Algebraic number theory*, Academic press, London and New-York, 1967.

[4] G. Chenevier, L. Clozel : *Corps de nombres peu ramifiés et formes automorphes autoduales*, Journal of the A.M.S. **22**, Vol 2, 467–519 (2009).

[5] D. Harari, T. Szamuely : *Arithmetic duality theorems for 1-motives*, J. Reine Angew. Math. **578**, 93-128 (2005).

[6] P. Gille, T. Szamuely : *Central Simple Algebras and Galois Cohomology*, Cambridge Studies in Advanced Mathematics **101**, Cambridge University Press, 2006.

[7] S. Lang : *On quasi-algebraic closure*, Ann. Math. **55**, 373-390 (1952).

[8] S. Mac Lane : *Categories for the working mathematician* (Second edition), Graduate Texts in Mathematics **5**, Springer-Verlag, New York, 1998.

[9] J. S. Milne : *Étale Cohomology*, Princeton University Press, Princeton 1980.

[10] J. S. Milne : *Arithmetic duality theorems* (Second edition), BookSurge, LLC, Charleston, SC, 2006.

[11] J. Neukirch : *Algebraic Number Theory*, Springer-Verlag, 1999.

[12] J. Neukirch, A. Schmidt, K. Wingberg : *Cohomology of number fields* (Second edition), Grundlehren der Mathematischen Wissenschaften **323**, Springer-Verlag 2008.

[13] J-P. Serre : *Corps locaux* (seconde édition), Hermann, Paris, 1968.

[14] J-P. Serre : *Cohomologie galoisienne* (cinquième édition, révisée et complétée), Lecture Notes in Mathematics **5**, Springer-Verlag, Berlin, 1994.

[15] S. Shatz : *Profinite groups, arithmetic, and geometry*, Annals of Mathematics Studies **67**, Princeton University Press, 1972.

[16] C. Weibel : *An introduction to homological algebra*, Cambridge University Press, 1994.