Théorie du corps de classes, M2, Orsay

David Harari

2012/2013 (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. L'auteur remercie A. Jaspers et S. Liu pour leurs commentaires qui ont permis d'améliorer la rédaction de ce texte.

1. Cohomologie des groupes finis

Dans toute cette section, G désigne un groupe **fini** [1] (dont la loi est notée multiplicativement et l'élément neutre 1). Notre but est ici de donner les propriétés essentielles de la cohomologie d'un tel groupe ; pour les détails des démonstrations, on pourra par exemple se reporter aux deux premiers chapitres de [4].

Rappelons que *l'algèbre du groupe* G est l'ensemble $\mathbf{Z}[G]$ des sommes formelles

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

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.

De façon équivalente, un G-module est la donnée d'un module (à gauche) sur l'anneau $R := \mathbf{Z}[G]$.

1. Beaucoup de résultats de cette section sont valables pour un groupe quelconque, mais dans ce cours nous n'utiliserons que la cohomologie des groupes finis et profinis, celle de ces derniers se ramenant au cas fini.

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) Si A et B sont des G-modules, alors $\mathrm{Hom}_{\mathbf{Z}}(A, B)$ est un G-module pour l'action de G définie par $(g.f)(x) = g.f(g^{-1}.x)$, $g \in G$, $f \in \mathrm{Hom}_{\mathbf{Z}}(A, B)$, $x \in A$.

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 est particulièrement important :

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.

Remarque : Comme G est fini, on vérifie que $I_G(A)$ est aussi isomorphe au G-module $\mathbf{Z}[G] \otimes A$, l'action de G étant sur le premier facteur.

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

De façon équivalente, M est induit si et seulement s'il contient un sous-groupe X tel que M soit la somme directe des $g.X$ pour $g \in G$.

1.2. Cohomologie d'un G-module

Fixons un groupe fini G. Les G-module forment une *catégorie abélienne*, que l'on 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.

Rappelons qu'un G-module est projectif si et seulement s'il est facteur direct d'un $\mathbf{Z}[G]$-module libre. Si A est un G-module et 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 $A = I \oplus B$).

□

Proposition 1.6 *Pour tout G-module A, il existe un G-module induit I muni d'un G-morphisme injectif $A \to I$.*

En effet si $I = I_G(A) = \mathrm{Hom}_{\mathbf{Z}}(\mathbf{Z}[G], A)$ est l'induit de A, on plonge A dans $I_G(A)$ en associant à tout $a \in A$ l'application $g \mapsto g.a$ de G dans A.

□

Définition 1.7 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).

D'après ce qui précède, tout G-module injectif est relativement injectif. D'autre part, comme nous avons supposé G fini, cette notion coïncide avec celle de G-module *relativement projectif*, i.e. facteur direct d'un G-module de la forme $\mathbf{Z}[G] \otimes A$.

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, conséquence du fait que $\mathbf{Q}/\mathbf{Z}$ est injectif dans la catégorie des groupes abéliens (car il est divisible) et de ce que si I est injectif dans la catégorie des groupes abéliens, alors le R-module $\mathrm{Hom}_{\mathbf{Z}}(R, I)$ est injectif dans $\mathcal{M}od_R$, cf. [14], paragraphe 2.3.

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 [14] 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. [14], 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*.

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

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

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 les formules $(\varphi+\psi)_* = \varphi_*+\psi_*$ et $(\varphi\circ\psi)_* = \varphi_*\circ\psi_*$; en

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

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 1.8 *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.*

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 ([14], 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 1.8, b) en utilisant cette nouvelle méthode de calcul de la cohomologie. On commence pour cela par une proposition générale (dont la preuve consiste en un calcul un peu long, mais sans difficultés).

Proposition 1.9 *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* $\mathrm{Hom}_G(B, I_G^H(A))$.

Le cas $H = \{1\}$ donne $\mathrm{Hom}_{\mathbf{Z}}(B, A) = \mathrm{Hom}_G(B, I_G(A))$. On peut alors obtenir assez facilement, en utilisant le calcul des groupes de cohomologie via la résolution projective de $\mathbf{Z}$:

Proposition 1.10 *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.

Corollaire 1.11 *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 1.12 *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*

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

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.

En particulier on voit que "la cohomologie de G commute avec les sommes directes" (pour cette propriété, il est vraiment important que G soit fini). On démontre ce résultat via le fait que $\varinjlim$ est un foncteur exact dans la catégorie des groupes abéliens et qu'une limite inductive de G-modules relativement injectifs est un G-module relativement injectif, vu que $\varinjlim$ commute avec $\otimes$ (ce dernier point implique que pour G fini, une limite inductive de G-modules induits reste un G-module induit).

Remarque : L'analogue de la proposition 1.12 avec "limite projective" au lieu de "limite inductive" est en général faux, mais reste vrai si tous les G-modules A_j sont finis.

1.3. 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, il est possible de construire une résolution explicite du G-module $\mathbf{Z}$ (équipé de l'action triviale de G) par des $\mathbf{Z}[G]$-modules libres. Le résultat est alors le suivant :

Theorème 1.13 *Soit A un G-module. 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 $f : G^i \to A$ ("cochaînes non homogènes"), 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-cocycles $Z^1(G, A) \subset K^1$ est le sous-groupe des fonctions f vérifiant de plus $f(g_1 g_2) = f(g_1) + g_1 f(g_2)$ 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 $H^1(G, A) = Z^1(G, A)/B^1(G, A)$.

Remarque : Il est parfois plus commode de voir les éléments de K^i comme des *cochaînes homogènes*, i.e. des fonctions $f : G^{i+1} \to A$ vérifiant

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

pour tout $s \in G$ et tout $g_0, ..., g_i$ de G^{i+1}.

Corollaire 1.14 *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 1.11, 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 **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]

1.4. 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 autre groupe (fini) 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 ([14], Th. 2.4.7) montre alors que pour tout entier $i \geq 0$, on a une unique famille de morphismes de foncteurs

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

4. On peut montrer ([14], 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.

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*.

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 1.15 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 $\mathrm{Res} : H^i(G, A) \to H^i(H, A)$ 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 $\mathrm{Inf} : H^i(G/H, A^H) \to H^i(G, A)$ 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

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

On a alors le très important résultat suivant, dont la preuve est essentiellement formelle à partir de la formule

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

(proposition 1.9) et du fait que $A \mapsto I_G^H(A)$ est un foncteur exact de $\mathcal{M}od_H$ dans $\mathcal{M}od_G$, ce qui résulte de $I_G^H(A) = \mathrm{Hom}_H(\mathbf{Z}[G], A)$ et de ce que $\mathbf{Z}[G]$ est un $\mathbf{Z}[H]$-module libre (prendre comme base un système de représentants des classes à droite de G selon H).

Theorème 1.16 (Lemme de Shapiro) *Les homomorphismes*

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

définis ci-dessus sont des isomorphismes.

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 $\sigma_t : H^i(G, A) \mapsto H^i(G, A)$. On obtient alors par décalage, en plongeant A dans un module induit I (le cas $i = 0$ est immédiat) :

Proposition 1.17 *L'application σ_t est l'identité.*

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 1.17 dit alors que H opère trivialement sur $H^i(H, A)$, autrement dit G/H opère sur $H^i(H, A)$. On a alors le théorème suivant, cas particulier de la suite spectrale des foncteurs composés de Grothendieck ([14], Th. 5.8.3.) :

Theorème 1.18 (Hochschild-Serre) *Soit G un groupe (fini). Soient H un sous-groupe distingué de G et A un G-module. Alors on a une suite spectrale*

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

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*), dont les trois premiers termes non nuls constituent la *suite exacte de restriction-inflation* (qui peut être établie directement avec des calculs de cocycles). On obtient aussi le résultat suivant, qui généralise la dite suite exacte :

Corollaire 1.19 *Soit G un groupe (fini). 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*

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

est exacte.

1.5. Corestriction ; applications

Soit H un sous-groupe d'un groupe fini G. Soit A un G-module. On va voir que l'on peut définir [5] 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. [14], pp. 48–49) car le premier de ces foncteurs est *effaçable* [6] en degré ≥ 1, donc universel. On obtient ainsi des homomorphismes de *corestriction*

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

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

Theorème 1.20 *Soit $m = [G : H]$ l'indice de H dans G. Alors la composée* $\text{Cor} \circ \text{Res}$ *est la multiplication par m dans $H^i(G, A)$.*

5. Dans le cas général où G n'est pas supposé fini, cela marche encore si H est **d'indice fini** dans G, condition que nous retrouverons dans le cadre de la cohomologie d'un groupe profini.

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 : 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 1.11.

□

Corollaire 1.21 *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 1.20 dans le cas $H = \{1\}$.

□

Corollaire 1.22 *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 $i > 0$.*

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 1.21, ils sont finis.

□

Corollaire 1.23 *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 1.21 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.

1.6. Les groupes de cohomologie modifiés de Tate

Il se trouve (notamment pour les questions arithmétiques) 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 les cas $i = 0, -1, -2$ qui seront utiles, le dernier en particulier quand on appliquera le théorème de Tate-Nakayama pour des groupes de Galois de corps locaux ou globaux.

Définition 1.24 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 $\sum_{g\in G} a_g g \mapsto \sum_{g\in G} a_g$.

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 1.25 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 1.26 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 injectif[7] ; les démonstrations sont exactement du même type que pour la cohomologie.

7. Si G n'était pas supposé fini, il faudrait ici considérer à la place les modules *relativement projectifs*.

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

Proposition 1.27 *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.*

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 1.28 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 1.29 *Soit $0 \to A \to B \to C \to 0$ une suite exacte de G-modules. Alors on a une suite exacte longue "fonctorielle" :*

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

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

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

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

Corollaire 1.30 *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.

On va maintenant expliquer comment les morphismes de restriction et de corestriction s'étendent à la cohomologie modifiée. 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 : $\widehat{H}^0(G,A) \to \widehat{H}^0(H,A)$. On a également un homomorphisme de corestriction Cores : $\widehat{H}^0(H,A) \to \widehat{H}^0(G,A)$ induit par $x \mapsto \sum_{g \in G/H} g.x$ de A^H dans A^G. Restriction et corestriction s'étendent en des morphismes de foncteurs cohomologiques, respectivement de $\widehat{H}^n(G,.)$ dans $\widehat{H}^n(H,.)$ et de $\widehat{H}^n(H,.)$ dans $\widehat{H}^n(G,.)$ (pour le voir on utilise les propriétés analogues en homologie, plus quelques calculs directs pour faire les "raccordements"). Par exemple pour $n=-1$, la corestriction 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 $\widehat{H}_0(G,A)$, et la restriction $\widehat{H}_0(G,A) \to \widehat{H}_0(H,A)$ vient de l'homomorphisme $N'_{G/H} : A/I_G A \to A/I_H A$ défini par

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

Le lemme de Shapiro s'étend sans problème à la cohomologie modifiée. On a aussi une généralisation des résultats du chapitre 1 :

Theorème 1.31 *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 $n=0$.

1.7. 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 1.32 *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 $I_G A = \operatorname{Im} D$. 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 1.30, après avoir écrit A comme sous-module (resp. comme quotient) d'un G-module induit I (resp I').

□

1.8. Quotient d'Herbrand

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 groupe finis, on note $h^0(A)$ et $h^1(A)$ leurs cardinaux respectifs.

Définition 1.33 Supposons que $\widehat{H}^0(G,A)$ et $\widehat{H}^1(G,A)$ sont finis. On appelle *quotient d'Herbrand* $h(A)$ du G-module A le nombre rationnel

$$h(A) := \frac{h^0(A)}{h^1(A)}.$$

Les propriétés du quotient d'Herbrand sont résumées dans le théorème suivant :

Theorème 1.34 *Soit G un groupe cyclique.*

a) Soit

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

une suite exacte de G-modules. Si deux des quotients d'Herbrand $h(A)$, $h(B)$, $h(C)$ sont définis, il en va de même du troisième et on a $h(B) = h(A)h(C)$.

b) Si A est un G-module fini, alors $h(A) = 1$.

c) Soit $f : A \to B$ un homomorphisme de G-modules dont le noyau et le conoyau sont finis. Si l'un des quotients d'Herbrand $h(A)$, $h(B)$ est défini, alors il en va de même de l'autre et $h(A) = h(B)$.

Démonstration : a) La suite exacte longue de cohomologie modifiée s'écrit, en tenant compte du théorème de périodicité 1.32 :

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

Cette longue suite exacte est donc 6-périodique ("hexagone exact"). On en déduit une suite exacte :

$$0 \to I_1 \to \widehat{H}^0(G,A) \to \widehat{H}^0(G,B) \to \widehat{H}^0(G,C) \to \widehat{H}^1(G,A) \to \widehat{H}^1(G,B) \to \widehat{H}^1(G,C) \to I_1 \to 0$$

où $I_1 = \mathrm{Im}\,[\widehat{H}^1(G,C) \to \widehat{H}^0(G,A)] = \ker[\widehat{H}^0(G,A) \to \widehat{H}^0(G,B)]$. Il est alors immédiat que si deux des quotients $h(A)$, $h(B)$, $h(C)$ sont définis, le troisième l'est aussi. Si c'est le cas, le produit alterné des cardinaux dans la suite exacte à huit termes ci-dessus est 1, ce qui donne, en appelant s le cardinal de I_1 :

$$h^0(A)h^0(C)h^1(B)s = h^0(B)h^1(A)h^1(C)s$$

soit

$$h(B) = h(A)h(C).$$

b) Soit s un générateur du groupe cyclique G. Soit D la multiplication par $s - 1$ dans A, on a donc une suite exacte

$$0 \to H^0(G,A) \to A \xrightarrow{D} A \to H_0(G,A) \to 0$$

vu qu'un élément x de A est dans $H^0(G,A)$ si et seulement si $s.x - x = 0$, et l'image de D est précisément $I_G(A)$. On a de même une suite exacte

$$0 \to \widehat{H}^{-1}(G,A) \to H_0(G,A) \xrightarrow{N} H^0(G,A) \to \widehat{H}^0(G,A) \to 0$$

Si le cardinal m de A est fini, on obtient donc que $H^0(G,A)$ et $H_0(G,A)$ ont même cardinal via la première suite, puis que $\widehat{H}^{-1}(G,A) \simeq H^1(G,A)$ et $\widehat{H}^0(G,A)$ ont même cardinal via la deuxième suite, d'où $h(A) = 1$.

c) Soit I l'image de f. On a des suites exactes

$$0 \to \ker f \to A \to I \to 0$$

$$0 \to I \to B \to \operatorname{coker} f \to 0$$

D'après b), on a $h(\ker f) = h(\operatorname{coker} f) = 1$. On obtient alors d'après a) que si $h(A)$ (resp. $h(B)$) est défini, alors $h(I)$ l'est également et on a alors $h(B)$ (resp. $h(A)$) défini avec $h(A) = h(I) = h(B)$.

□

1.9. Cup-produits

Soit G un groupe fini. 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 1.3.) :

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

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, en vérifiant de façon calculatoire la formule $d(a \cup b) = (da) \cup b + (-1)^p (a \cup db)$:

Theorème 1.35 *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.

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 G-bilinéaire [8] $\varphi : A \times B \to C$ entre G-modules en utilisant le fait qu'une telle application se factorise à travers $A \otimes B$. On notera $\cup_\varphi$ (ou encore $\cup$ si φ est sous-entendue) le cup-produit ainsi obtenu. On a en outre les deux propriétés de compatibilité suivantes du cup-produit :

8. Cela signifie que φ est bilinéaire, et vérifie de plus $\varphi(g.a, g.b) = g.\varphi(a, b)$ pour tous $a \in A$, $b \in B$, $g \in G$.

Proposition 1.36 *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).

On obtient également par décalage :

Proposition 1.37 *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 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 le théorème de dualité local :

Proposition 1.38 *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 $\beta \in H^{q-1}(G, B'')$.

Il est également possible (cf [10], prop. 1.4.7.) de définir pour G fini le cup-produit $\widehat{H}^p(G, A) \times \widehat{H}^q(G, B) \to \widehat{H}^{p+q}(G, A \otimes B)$ 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.

1.10. Exercices

Dans tous ces exercices, G désigne un groupe fini.

1. Soit H un sous-groupe 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. 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) Comparer $I_G^H(\mathbf{Z})$ et le G-module $\mathbf{Z}[G/H]$ constitué des sommes formelles $\sum_{s\in G/H} n_s s$, $s \in G/H$, l'action de G sur $\mathbf{Z}[G/H]$ étant donnée par l'action à gauche de G sur l'ensemble des classes à gauche G/H.

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

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

d) 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. 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. p-groupes, théorème de Tate-Nakayama

Soit p un nombre premier. Rappelons qu'un *p-groupe* fini est un groupe fini dont le cardinal est une puissance de p. Dans ce chapitre, on va voir que les p-groupes ont des propriétés cohomologiques particulières, qui permettent souvent détudier la cohomologie d'un groupe fini en se ramenant à celle de ses p-Sylow.

2.1. Modules cohomologiquement triviaux

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.

Lemme 2.1 *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.

□

Lemme 2.2 *Soient G un groupe fini et A un G-module. Soient p un nombre premier et H un sous-groupe de G. Alors si p ne divise pas $[G : H]$, l'application* $\mathrm{Res} : H^q(G, A)\{p\} \to H^q(H, A)$ *est injective pour tout $q > 0$.*

Démonstration : Cela résulte immédiatement de la formule $\mathrm{Cor} \circ \mathrm{Res} = .[G : H]$.

□

Lemme 2.3 *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 $g \in G$, $f \in \mathrm{Hom}_{\mathbf{Z}}(A, B)$, $x \in A$.

Démonstration : (Voir aussi [11], prop. 1. p. 149 pour un énoncé un peu plus général). Comme B est 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 induit puisqu'il est la somme directe des $g.\mathrm{Hom}(A, X)$, $\mathrm{Hom}(A, X)$ étant un sous-groupe de $\mathrm{Hom}(A, B)$ (cf. remarque après la définition 1.4).

□

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 $f \mapsto \sum_{g\in G} g.f(g^{-1})$; 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 1.30.

Définition 2.4 Soit G un groupe fini. On dit qu'un G-module A est *cohomologiquement trivial* si pour tout $n > 0$ et tout sous-groupe 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 H de G. Noter qu'un G-module induit est cohomologiquement trivial : cela résulte de ce que A est aussi induit en tant que H-module

Lemme 2.5 *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 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 $H^n(H', A)$. Par ailleurs, on peut bien sûr se limiter aux nombres premiers qui divise le cardinal de G, vu que pour les autres le groupe G_p est trivial.

Démonstration : Soit H un sous-groupe 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 2.2) vu que l'indice $[H : H_p]$ est premier à p.

□

Theorème 2.6 *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 induit (somme directe d'induits). 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 2.3 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 2.1. 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 2.1). 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 2.7 *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

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

ce qui, via la suite exacte,

$$0 \to R \xrightarrow{\cdot p} R \to R/pR \to 0 \tag{2}$$

(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 2.6 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 2.8 *On a $H^1(G, M) = 0$.*

Démonstration : La suite exacte (2) 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 2.3 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 2.2). 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 (1) 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).

□

2.2. Théorème de Tate-Nakayama

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 2.9 *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 2.7, 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 induit, 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 2.10 *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[9] *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 $i \in \mathbf{Z}$.

9. 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 2.7, le G-module A'' est cohomologiquement trivial. D'après le lemme 2.9, 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 2.11 *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 2.10 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 2.9), 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 1.36). Si le résultat voulu vaut pour a_1, il vaut donc également pour a d'où le résultat par récurrence sur q.

□

Theorème 2.12 (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.

□

Nous serons amenés plus tard à appliquer l'énoncé précédent avec $n = -2$, $G = \mathrm{Gal}\,(L/K)$ et $A = L^*$ pour une extension finie galoisienne L d'un corps p-adique K. On en déduira un isomorphisme de $H^{-2}(G, \mathbf{Z}) = G^{\mathrm{ab}}$ sur $\widehat{H}^0(G, L^*) = K^*/NL^*$, une fois vérifiées les hypothèses du théorème dans ce cadre. On verra aussi qu'un énoncé analogue vaut dans le cas global, en remplaçant L^* par *le groupe des classes d'idèles* de L.

2.3. Exercices

1. Soit G un p-groupe fini. Soit A un G-module de p-torsion. Montrer que si $H_0(G, A) = 0$, alors $A = 0$ (considérer le G-module $A' := \mathrm{Hom}_{\mathbf{Z}}(A, \mathbf{Z}/p)$). Ce résultat est-il encore vrai si on suppose seulement que A est p-primaire ?

2. 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.

3. 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. Cohomologie des groupes profinis

En théorie des nombres, on est souvent amené à travailler avec le *groupe de Galois absolu* $\mathrm{Gal}\,(\bar{k}/k)$ d'un corps k (dont on fixe une clôture séparable $\bar{k}$), qui est un exemple de groupe profini. On est donc amené à étendre certaines définitions et propriétés de la cohomologie des groupes finis aux groupes profinis. Par ailleurs, la notion de *dimension cohomologique* joue un rôle important pour les groupes profinis, alors que cette notion n'a en général pas d'intérêt pour les groupes finis (cf. exercice 2. de ce chapitre). On pourra se reporter aux chapitre 3 et 4 de [4] pour plus de détails sur la cohomologie des groupes profinis et le cas particulier de la cohomologie galoisienne.

3.1. Généralités 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[10] 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[11] et totalement discontinu ([10], proposition 1.1.3)[12]. Dans un groupe profini, les sous-groupes ouverts sont d'indice fini (mais attention, il peut arriver que des sous-groupes d'indice fini ne soient pas fermés). 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 $\bar{k}$. 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.

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

d) L'anneau des entiers p-adique $\mathbf{Z}_p$ est un groupe profini pour l'addition.

Définition 3.2 *Soit G un groupe profini. Soient H un sous-groupe fermé de G et p un nombre premier. On dit que H est d'indice*[13] *premier à p s'il n'existe pas de sous-groupe ouvert U de G contenant H tel que p divise le cardinal de l'ensemble*[14] *fini G/U.*

10. 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.

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

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

13. Il est possible plus généralement de définir l'indice d'un sous-groupe fermé, qui est un *nombre surnaturel*.

14. Noter qu'on ne peut pas ici se restreindre aux sous-groupes U distingués : par exemple le sous-groupe ouvert $H = \mathrm{Gal}\,(\overline{\mathbf{Q}}/\mathbf{Q}(\sqrt{3}))$ de $G = \mathrm{Gal}\,(\overline{\mathbf{Q}}/\mathbf{Q})$ est d'indice 3, mais le seul sous-groupe ouvert distingué de G qui contient H est G tout entier.

En particulier on dira que l'ordre de G est premier à p si le sous-groupe trivial est d'indice premier à p. Au contraire, la notion suivante généralise celle de p-groupe fini :

Définition 3.3 On dit que G est un *pro-p-groupe* s'il est limite projective de p-groupes finis (de façon équivalente, cela signifie que pour tout sous-groupe ouvert U de G, le groupe fini G/U est un p-groupe). Un *p-sous-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 H soit d'indice premier à p.

La proposition ci-dessous (dont la preuve se déduit des résultats analogues pour les groupes finis) résume les propriétés des indices et des sous-groupes de Sylow.

Proposition 3.4 *a) Soient $K \subset H \subset G$ des groupes profinis. Si H est d'indice premier à p dans G et K d'indice premier dans H, alors K est d'indice premier dans G.*

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.

3.2. Cohomologie d'un G-module discret

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) si le fixateur de tout élément de A est un sous-groupe ouvert de A.

Définition 3.5 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.

Bien entendu pour G fini ceci coïncide avec la notion habituelle de G-module. 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. Soit k un corps de groupe de Galois absolu $\Gamma_k = \mathrm{Gal}\,(\bar{k}/k)$.

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).

La catégorie C_G des G-modules discrets possède assez d'injectifs [15] et on peut donc utiliser les foncteurs dérivés du foncteur $A \mapsto A^G$ de C_G dans Ab pour définir les groupes de cohomologie $H^i(G, A)$. Une autre définition (équivalente, voir le paragraphe 3.3. de [4]) est d'utiliser les cochaînes :

Proposition 3.6 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 1.13). Les groupes de cohomologie $H^q(G, A)$ sont alors les groupes de cohomologie du complexe $(K^q(G, A))$.

La cohomologie d'un groupe profini se ramène alors à celle de ses quotients finis via la proposition suivante et son corollaire.

Proposition 3.7 *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 $q \in \mathbf{N}$:*

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

Corollaire 3.8 *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 $A = \varinjlim_U A^U$.

15. mais pas assez de projectifs ; noter par exemple que pour G infini, $\mathbf{Z}[G]$ n'est pas un G-module discret. On peut par contre travailler avec le G-module discret $\mathbf{Z}[G/U]$ pour U sous-groupe ouvert de G.

Corollaire 3.9 *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 3.10 *Pour $q \geq 1$, les groupes $H^q(G, A)$ sont de torsion.*

Cela résulte du corollaire 3.8 et du corollaire 1.21.

Les propriétés de la cohomologie d'un groupe profini G se déduisent immédiatement de celle d'un groupe fini via le corollaire 3.8. 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. En particulier :

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).
2. Pour tout sous-groupe fermé H de G, les homomorphismes de restriction et d'inflation sont définis comme dans le paragraphe 1.4., et le lemme de Shapiro reste vrai. Il en va de même de la proposition 1.17 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 1.20 et le corollaire 1.23 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 1.9. (si ce n'est que dans la définition il faut prendre des cochaînes continues), et jouit des mêmes propriétés.

Par contre, bien qu'il soit possible de les définir, nous n'utiliserons pas de groupes modifiés de Tate $\widehat{H}^i(G, A)$ pour G infini et $i \leq 0$.

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 $\mathbf{Z}$.

3.3. Dimension cohomologique

La notion de p-dimension cohomologique d'un groupe profini est très importante. 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), voir l'exercice 2. de ce chapitre.

Définition 3.11 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, ou encore via la proposition 3.7 que $H^q(G, A)$ soit nul si on suppose de plus A de torsion p-primaire).

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

Le cas des pro-p-groupes est particulièrement agréable :

Theorème 3.12 *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 (esquisse): 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 $H^{n+1}(G, \mathbf{Z}/p) = 0$. On note d'abord qu'un G-module discret A qui est simple [17] et p-primaire est isomorphe à $\mathbf{Z}/p$: en effet on voit tout de suite que A est engendré par tout élément non nul, donc est fini. On se ramène alors au cas où G est un p-groupe fini (vu que G contient un sous-groupe ouvert qui agit trivialement sur A), auquel cas le lemme 2.1 donne aisément que l'action de G est triviale, puis que $A = \mathbf{Z}/p$ par simplicité.

Ceci étant établi, on montre alors que $H^{n+1}(G, A) = 0$ pour tout A fini et p-primaire, par récurrence sur le cardinal de A (puisque le cas A simple résulte de ce qui précéde, vu qu'alors $A = \mathbf{Z}/p$). Ceci vaut encore pour tout A qui est p-primaire (pas forcément fini) via le corollaire 3.9. Enfin, la propriété $H^q(G, A) = 0$ pour tout $q > n$ et tout module p-primaire A se montre par récurrence sur $q > n$ en plongeant A dans $I_G(A)$ (qui est encore p-primaire car ses éléments sont des fonctions **localement constantes** du groupe compact G dans A, qui ne prennent donc qu'un nombre fini de valeurs), puis en appliquant l'hypothèse de récurrence à $I_G(A)/A$.

□

17. Rappelons qu'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.

Exemple. Prenons $G = \mathbf{Z}_p = \varprojlim_n (\mathbf{Z}/p^n)$. On a $H^2(G, \mathbf{Z}/p) = 0$ via la proposition 3.7 : en effet d'après le théorème 1.32, 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 3.12 dit alors que $\mathrm{cd}_p(\mathbf{Z}_p) \leq 1$, et l'égalité vient de ce que

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

Définition 3.13 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 $\mathrm{scd}(G) = \sup_p \mathrm{scd}_p(G)$.

Proposition 3.14 *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 3.14 : 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 3.15 *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.

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.

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 (en effet $H^1(\mathbf{Z}/2, \mathbf{Z}/2) = \mathbf{Z}/2$ et on applique ensuite le théorème 1.32).

Démonstration : 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 2.2.

□

Remarque : On a encore l'égalité $\mathrm{cd}_p(H) = \mathrm{cd}_p(G)$ pour tout sous-groupe ouvert H de G **si on suppose** $\mathrm{cd}_p(G)$ **finie** (voir l'exercice 1 de ce chapitre). De même pour scd_p. Par contre, on verra que le groupe de Galois de $\mathbf{Q}(i)$ est de dimension cohomologique 2, alors que c'est un sous-groupe ouvert du groupe de Galois de $\mathbf{Q}$, qui est de 2-dimension cohomologique infinie puisqu'il contient un sous-groupe isomorphe à $\mathbf{Z}/2$ (engendré par la conjugaison complexe).

Corollaire 3.16 *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 $\mathrm{scd}_p(\widehat{\mathbf{Z}}) = \mathrm{scd}_p(\mathbf{Z}_p) = 2$.

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 3.17 *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 : Cela résulte de la suite spectrale de Hochschild-Serre, qui donne que si A est un G-module discret, alors chaque $H^n(G, A)$ admet une filtration dont les quotients successifs sont des sous-quotients des $H^i(G/H, H^j(H, A))$ pour $i + j = n$.

□

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

Proposition 3.18 *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 par la proposition 3.15. 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 3.14. 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 3.14).

□

3.4. Premières notions de cohomologie galoisienne

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

Soit M un Γ_k-module discret. Les groupes de cohomologie $H^q(\Gamma_k, M)$ pour $q \geq 0$ ont été définis au chapitre précédent. Si maintenant k_1 est une extension de corps de k de clôture séparable $\bar{k}_1$ 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 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 1.17. En particulier deux clôtures séparables de k définissent des $H^q(\Gamma_k, M)$ canoniquement isomorphes, ce qui permet de noter $H^q(k, M)$

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.

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 3.19 *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 3.20 *On a $H^q(k, \bar{k}) = 0$ pour tout $q > 0$.*

Démonstration : Le corollaire se déduit de la proposition via le corollaire 3.8. La proposition résulte de ce que d'après le théorème de la base normale (cf. [2], paragraphe 10), le $\mathrm{Gal}\,(L/k)$-module L est induit (isomorphe à $\mathbf{Z}[\mathrm{Gal}\,(L/k)] \otimes_{\mathbf{Z}} k$).

□

Le résultat suivant est peut-être l'énoncé le plus célèbre en cohomologie galoisienne :

Theorème 3.21 (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 3.8. Soit $s \mapsto a_s$ un cocycle dans $Z^1(G, L^*)$. D'après le théorème d'indépendance linéaire des morphismes de Dedekind ([2], 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 :

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

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

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

□

Corollaire 3.22 *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.

□

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

Contrairement au groupe additif $\bar{k}$, le groupe multiplicatif $\bar{k}^*$ peut avoir une cohomologie non triviale. En particulier, son deuxième groupe de cohomologie va jouer un rôle important quand k est un corps local ou global.

Définition 3.23 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 3.24 *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 3.21 (Hilbert 90) et du corollaire 1.19, 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 $A = \bar{k}^*$.

□

21. Ce morphisme n'est bien défini qu'à conjugaison près, mais le même raisonnement qu'au paragraphe 3.4. montre que l'homomorphisme $\mathrm{Br}\,k \to \mathrm{Br}\,K$ est bien défini.

Remarque : Il existe une autre définition du groupe de Brauer, basée sur les algèbres centrales simples, voir par exemple [11], chapitre X, paragraphe 5. En particulier, on a $\mathrm{Br}\, k = 0$ si et seulement si la seule algèbre à division de dimension finie sur k et de centre k est k. Cela permet par exemple de montrer que toute algèbre à division [22] finie est un corps via le corollaire 3.31.

Proposition 3.25 *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).

□

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 1.32 vu que $\Gamma_{\mathbf{R}}$ est cyclique.

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

Définition 3.26 Soient k un corps et p un nombre premier. La p-dimension cohomologique [23] (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. Si k est de caractéristique p, sa p-dimension cohomologique est toujours ≤ 1 (voir exercice 9 de ce chapitre).

Le cas où k est de dimension cohomologique ≤ 1 est particulièrement important. Il est remarquable que cette propriété puisse être caractérisée en n'utilisant que le groupe de Brauer des extensions finies de k.

22. Ce qu'on appelle parfois en français un *corps gauche*, terminologie qui présente l'inconvénient qu'un corps gauche n'est alors pas un corps...

23. La définition que nous adoptons ici est la plus simple, mais ce n'est pas "la bonne" si k est imparfait de caractéristique p, voir par exemple [12], chapitre II.3 pour le cas de la dimension cohomologique 1.

Theorème 3.27 *Soit k un corps. Soit p un nombre premier différent de la caractéristique de k. Alors les assertions suivantes sont équivalentes :*

i) On a $\mathrm{cd}_p(k) \leq 1$.

ii) Pour toute extension algébrique séparable K du corps k, la p-torsion $(\mathrm{Br}\, K)[p]$ *de* $\mathrm{Br}\, K$ *est nulle.*

iii) Pour toute extension finie séparable K de k, la p-torsion $(\mathrm{Br}\, K)[p]$ *de* $\mathrm{Br}\, K$ *est nulle.*

Bien entendu, si k est de caractéristique zéro, on peut remplacer partout cd_p par cd et $(\mathrm{Br}\, K)[p]$ par $\mathrm{Br}\, K$.

Démonstration : Supposons i) vérifiée. Soit K une extension algébrique séparable de k. Alors son groupe de Galois absolu Γ_K est isomorphe à un sous-groupe fermé de Γ_k, d'où $\mathrm{cd}_p(K) \leq 1$ via la proposition 3.15, ce qui implique $(\mathrm{Br}\, K)[p] = H^2(K, \mu_p) = 0$. L'implication ii) $\Rightarrow$ iii) est triviale.

Supposons donc iii). Soit G_p un p-Sylow de Γ_k et $K \subset \bar{k}$ son corps fixe. Alors K contient le groupe μ_p des racines p-ièmes de l'unité de $\bar{k}$, car le degré $[K(\mu_p) : K]$ divise p et $p-1$. Comme K est alors réunion d'extensions finies séparables de k contenant μ_p, la propriété iii) donne

$$H^2(K, \mu_p) = H^2(K, \mathbf{Z}/p) = 0$$

donc $\mathrm{cd}_p(k) = \mathrm{cd}_p(K) \leq 1$ par le corollaire 3.16 et le théorème 3.12.

□

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 3.28 *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, [5], 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, [5], Th. 6.2.8.). Il en va de même de $k((t))$ (résultat dû à Lang, [5], Th. 6.2.1.)

3. Lang ([6]) a également démontré que l'extension maximale non ramifiée d'un corps p-adique [24] est C_1.

Lemme 3.29 *Soit k un corps C_1 et soit k_1 une extension algébrique de k. Alors k_1 est C_1.*

24. 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 : 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 3.30 *Soit k un corps C_1. Alors* $\mathrm{cd}(k) \leq 1$ *et* $\mathrm{Br}\, k = 0$.

La réciproque est fausse : Ax a construit un corps de dimension cohomologique 1 qui n'est pas C_1, cf. [12], exercice p.90. Noter que $\mathrm{Br}\, k = 0$ est vrai pour tout corps k de dimension cohomologique 1 si k est de caractéristique zéro (via le théorème 3.27). En caractéristique $p > 0$, il peut y avoir (avec notre définition de $\mathrm{cd}_p(k)$) un problème pour la p-partie si k n'est pas parfait, par exemple la p-torsion du groupe de Brauer d'un corps local de caractéristique p est isomorphe à $\mathbf{Z}/p$ (voir théorème 4.8) ; pour k parfait de caractéristique p, l'application $x \mapsto x^p$ dans $\bar{k}^*$ est un isomorphisme, ce qui donne immédiatement $(\mathrm{Br}\, k)[p] = 0$.

Démonstration : Soit K une extension algébrique séparable de k. Soit L une extension finie galoisienne 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. En combinant cela avec le théorème de Hilbert 90, on obtient $\widehat{H}^n(G, L^*) = 0$ pour $n = 0, 1$, où $G := \mathrm{Gal}\,(L/K)$. Ceci vaut aussi pour toute extension intermédiaire L/K' de l'extension L/K grâce au lemme 3.29. Le théorème 2.7 permet alors de conclure que le G-module L^* est cohomologiquement trivial. En particulier $\mathrm{Br}\,(L/K) = H^2(G, L^*)$ est nul, et en passant la limite on obtient $\mathrm{Br}\, K = 0$. Le résultat découle alors du théorème 3.27 (combiné, en caractéristique p, au fait que $\mathrm{cd}_p(k) \leq 1$ est automatique).

□

Corollaire 3.31 *Un corps fini est de dimension cohomologique* ≤ 1 *et son groupe de Brauer est nul.*

Noter que ce corollaire peut aussi s'obtenir en notant que le groupe de Galois d'un corps fini est isomorphe à $\widehat{\mathbf{Z}}$, combiné pour la deuxième partie au fait qu'un corps fini est parfait.

3.6. Exercices

1. Soit G un groupe profini. Soit H un sous-groupe ouvert de G. On définit un homomorphisme $\pi : I := I_G^H(A) \to A$ par la formule

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

a) Montrer que π est surjectif et que l'homomorphisme induit $H^n(G, I) = H^n(H, A) \to H^n(G, A)$ est la corestriction.

b) En déduire que si $n = \mathrm{cd}_p(G)$ est finie, alors la corestriction

$$H^n(H, A)\{p\} \to H^n(G, A)\{p\}$$

est surjective pour tout G-module discret de torsion A. Énoncer un résultat analogue en supposant que $n = \mathrm{scd}_p(G)$ est finie.

c) On suppose que $n = \mathrm{cd}_p(G)$ est finie. Montrer que $n = \mathrm{cd}_p(H)$. A-t-on l'analogue avec scd_p ?

d) Donner un exemple de groupe profini G possédant un sous-groupe ouvert H avec $\mathrm{cd}_p(G)$ infinie et $\mathrm{cd}_p(H)$ finie.

2. 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 est premier à p.

b) Montrer que si $\mathrm{cd}_p(G)$ n'est ni nul ni infini, alors pour tout $m > 0$, le groupe G possède un sous-groupe ouvert d'indice p^m.

c) En déduire que si G est fini, alors $\mathrm{cd}_p(G) = 0$ si p ne divise pas l'ordre de G, et $\mathrm{cd}_p(G) = +\infty$ si p divise l'ordre de G.

3. 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 $q > n$.

4. 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).

5. 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.

6. 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 $H^n(H, \mathbf{Q}_p/\mathbf{Z}_p) \neq 0$.

7. 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 $H^n(H, A) = 0$.

a) Montrer qu'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.

b) Montrer qu'un G-module induit est cohomologiquement trivial.

8. 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.

9. Soit k un corps de caractéristique $p > 0$, de clôture séparable $\bar{k}$. Soit Φ l'application de $\bar{k}$ dans $\bar{k}$ définie par $\Phi(x) = x^p - x$.

a) Montrer que $H^1(k, \mathbf{Z}/p) = k/\Phi(k)$ et $H^q(k, \mathbf{Z}/p) = 0$ pour $q \geq 2$ ("théorie d'Artin-Schreier").

b) En déduire que $\mathrm{cd}_p(k) \leq 1$.

10. 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) Soit k' une extension algébrique de k. Comparer $\mathrm{cd}_p(k)$ et $\mathrm{cd}_p(k')$.

c) En déduire que si K est une extension de k de degré de transcendance N, alors

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

11. 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).

12. On considère le groupe profini $\widehat{\mathbf{Z}}$. Soit M un G-module fini. Soit F le générateur topologique canonique de $\widehat{\mathbf{Z}}$.

a) Montrer qu'il existe des entiers positifs m et n tels que : F^m opère trivialement sur M et M est de n-torsion.

b) On pose $s = mn$ et on considère M comme un $\mathbf{Z}/s$-module. Montrer que la norme $N_{\mathbf{Z}/s} : M \to M$ est l'application nulle.

c) Montrer que pour i entier multiple de s, le groupe $H^1(\mathbf{Z}/i, M)$ est isomorphe au conoyau de l'endomorphisme $F - 1 : M \to M$.

d) En déduire que les groupes $H^0(\widehat{\mathbf{Z}}, M)$ et $H^1(\widehat{\mathbf{Z}}, M)$ sont finis de même cardinal.

4. Le groupe de Brauer d'un corps local

Dans toute cette section, on désigne par K un *corps local*, c'est-à dire un corps complet pour une valuation discrète v à corps résiduel fini κ de caractéristique p. Rappelons que quand K est de caractéristique zéro, c'est un *corps p-adique*, c'est-à dire une extension finie du corps des nombres p-adiques $\mathbf{Q}_p$; sinon K est de caractéristique p et il est alors isomorphe au corps des séries de Laurent $\kappa((t))$.

L'étape la plus importante dans le calcul du groupe de Brauer d'un corps local consiste à montrer que le groupe de Brauer de l'extension maximale non ramifiée K_{nr} est trivial (et en fait même que K_{nr} est de dimension cohomologique 1). On peut obtenir ceci directement si on connaît le théorème de Lang ([6]), ou encore le montrer avec la même technique que dans le théorème 3.30 via des calculs de normes dans les corps locaux ([11], section XII.1). Une autre option est d'utiliser la caractérisation du groupe de Brauer en termes d'algèbres simples centrales ([11], section XII.2). Nous allons suivre ici la méthode de [10] (voir aussi l'exposé de Serre dans [3]), qui est un peu moins générale au sens où elle utilise l'hypothèse κ fini, mais qui a l'avantage de ne s'appuyer que sur ce qui a été vu précedemment dans ce cours.

4.1. Cohomologie du groupe des unités

On note U_K le groupe multiplicatif des unités de l'anneau des entiers $\mathcal{O}_K$ de K (autrement dit U_K est l'ensemble des éléments de valuation nulle) et U_K^1 le sous-groupe des *unités principales*, i.e. des éléments x de K vérifiant $v(1-x) \geq 1$. Plus généralement on note U_K^i le sous-groupe des x vérifiant $v(1-x) \geq i$.

Proposition 4.1 *Soit L une extension finie galoisienne de K de groupe de Galois $G = \mathrm{Gal}\,(L/K)$. On suppose que l'extension L/K est non ramifiée. Alors U_L et U_L^1 sont des G-modules cohomologiquement triviaux.*

Démonstration : Soit λ le corps résiduel de L. Comme l'extension L/K est non ramifiée, on a aussi $G = \mathrm{Gal}\,(\lambda/\kappa)$. On a par ailleurs une filtration du groupe des unités de L :

$$U_L \supset U_L^1 \supset ... \supset U_L^i \supset ...$$

avec $U_L^i/U_L^{i+1} \simeq \lambda$ pour tout $i > 0$. Il en résulte que chaque U_L^i/U_L^{i+1} est un G-module cohomologiquement trivial via la proposition 3.19, et par récurrence sur i on en déduit immédiatement qu'il en va de même pour U_L^1/U_L^i pour

tout $i > 0$. Comme la cohomologie d'un groupe fini commute avec les limites projectives de modules finis, on en déduit que $U_L^1 = \varprojlim_{i>0}(U_L^1/U_L^i)$ est un G-module cohomologiquement trivial.

D'autre part, pour tout sous-groupe H de G (correspondant à une extension finie κ' de κ), on a $H^1(H, \lambda^*) = 0$ par Hilbert 90, et $H^2(H, \lambda^*) = 0$ par la nullité du groupe de Brauer du corps fini κ'. Le théorème 2.7 dit alors que λ^* est un G-module cohomologiquement trivial. C'est donc aussi le cas de U_L via la suite exacte

$$0 \to U_L^1 \to U_L \to \lambda^* \to 0.$$

□

Lemme 4.2 *Soit L une extension finie galoisienne de K de groupe G. Alors il existe un sous G-module V_1 de U_L^1 qui est d'indice fini et cohomologiquement trivial.*

Démonstration : D'après le théorème de la base normale, il existe $\alpha \in L$ tel que la famille $(g.\alpha)_{g\in G}$ soit une base du K-ev L. Pour $a \in K^*$ de valuation suffisamment grande, on a alors $M \subset \mathcal{O}_L$, où M est l'$\mathcal{O}_K$-module engendré par $(ag.\alpha)_{g\in G}$. On note que le G-module M est isomorphe à $\mathcal{O}_K[G]$, et par ailleurs c'est un sous-groupe ouvert du groupe profini $\mathcal{O}_L$ (en effet il est défini par une condition du type : $x \in M$ ssi chacune de ses coordonnées x_i sur la base $(g.\alpha)$ est de valuation $\geq m_i$, où $m_1, ..., m_n$ sont des entiers fixés). En particulier M est d'indice fini dans $\mathcal{O}_L$, d'où un entier $m \geq 1$ tel que $M \supset \pi^m\mathcal{O}_L$, où π est une uniformisante de K. On définit alors un sous-G-module (le fait que ce soit un sous-groupe pour la multiplication résultant de la propriété $M \supset \pi^m\mathcal{O}_L$) V_i de U_L^1 par $V_i = 1 + \pi^{m+i}M$. Chaque V_i/V_{i+1} est isomorphe à $M/\pi M$ via

$$v_i \mapsto \pi^{-m-i}(v_i - 1) \quad (\pi M)$$

ce qui implique que ce sont des G-modules finis et cohomologiquement triviaux (isomorphes à l'induit $(\mathcal{O}_K/\pi)[G]$). Par récurrence, il en va de même des V_1/V_i pour $i \geq 1$. Ainsi leur limite projective V_1 est également un G-module cohomologiquement trivial, et V_1 est clairement d'indice fini dans U_L^1.

□

Proposition 4.3 ("Axiome du corps de classes") *Soit L une extension finie et galoisienne de K, de groupe G cyclique. Alors $H^1(G, L^*) = 0$ et $\widehat{H}^0(G, L^*)$ est de cardinal $[L : K]$.*

Démonstration : La première assertion vient de Hilbert 90. Appliquons le lemme précédent. Le quotient d'Herbrand $h(G, V_1)$ est 1 car V_1 est cohomologiquement trivial, et $h(G, U_L/V_1) = 1$ via le théorème 1.34, b). On en déduit $h(G, U_L) = 1$ par le théorème 1.34, a). Comme le G-module trivial $\mathbf{Z}$ est isomorphe au quotient L^*/U_L, on obtient $h(G, L^*) = h(G, \mathbf{Z}) = [L : K]$ vu que $H^1(G, \mathbf{Z}) = 0$ et $\widehat{H}^0(G, \mathbf{Z}) = \mathbf{Z}/[L : K]\mathbf{Z}$. Comme $H^1(G, L^*) = 0$, ceci donne que le cardinal de $\widehat{H}^0(G, L^*)$ est $[L : K]$ comme on voulait.

□

4.2. Calcul du groupe de Brauer

Soit K_{nr} l'extension maximale non ramifiée de K. Le groupe de Galois $\widetilde{\Gamma}_K = \mathrm{Gal}\,(K_{\mathrm{nr}}/K) \simeq \mathrm{Gal}\,(\bar{\kappa}/\kappa)$ (que nous noterons simplement $\widetilde{\Gamma}$ s'il n'y a pas de confusion possible) est isomorphe à $\widehat{\mathbf{Z}}$; il est topologiquement engendré par le Frobenius F. On a des isomorphismes :

$$H^2(\widetilde{\Gamma}, K_{\mathrm{nr}}^*) \xrightarrow{\beta} H^2(\widetilde{\Gamma}, \mathbf{Z}) \xrightarrow{\delta^{-1}} H^1(\widetilde{\Gamma}, \mathbf{Q}/\mathbf{Z}) \xrightarrow{\gamma} \mathbf{Q}/\mathbf{Z}.$$

Ici β est induit par la suite exacte

$$0 \to U_{K_{\mathrm{nr}}} \to K_{\mathrm{nr}}^* \xrightarrow{v} \mathbf{Z} \to 0$$

(où $U_{K_{\mathrm{nr}}} \subset K_{\mathrm{nr}}^*$ est le sous-groupe des unités, i.e. des inversibles de l'anneau des entiers de K_{nr}) vu que $H^i(\widetilde{\Gamma}, U_{K_{\mathrm{nr}}}) = 0$ pour tout $i > 0$ par la proposition 4.1, en passant à la limite. L'isomorphisme δ vient de la trivialité de la cohomologie de $\mathbf{Q}$. Enfin γ est obtenu en envoyant tout caractère $\chi \in H^1(\widetilde{\Gamma}, \mathbf{Q}/\mathbf{Z})$ sur $\chi(F)$.

Proposition 4.4 *Soit* $\mathrm{inv}_K : H^2(\widetilde{\Gamma}_K, K_{\mathrm{nr}}^*) \to \mathbf{Q}/\mathbf{Z}$ *la composée des isomorphismes ci-dessus. Soit* L *une extension finie*[25] *de* K*. Alors on a un diagramme commutatif*

$$\begin{array}{ccc} H^2(\widetilde{\Gamma}_K, K_{\mathrm{nr}}^*) & \xrightarrow{\mathrm{inv}_K} & \mathbf{Q}/\mathbf{Z} \\ {\scriptstyle \mathrm{Res}}\downarrow & & \downarrow{\scriptstyle .[L:K]} \\ H^2(\widetilde{\Gamma}_L, L_{\mathrm{nr}}^*) & \xrightarrow{\mathrm{inv}_L} & \mathbf{Q}/\mathbf{Z} \end{array}$$

25. Noter que l'hypothèse que L soit séparable n'est pas ici nécessaire.

Démonstration : Soit e l'indice de ramification de L/K et f le degré résiduel. On a $[L : K] = ef$. Comme l'isomorphisme $\beta_K : H^2(\widetilde{\Gamma}_K, K^*_{\rm nr}) \to H^2(\widetilde{\Gamma}_K, \mathbf{Z})$ est induit par la valuation (et de même pour $\widetilde{\Gamma}_L$), on a $\beta_L \circ {\rm Res} = e.{\rm Res} \circ \beta_K$. La compatibilité de Res avec les suites exactes longues donne, avec des notations similaires, $\delta_L^{-1} \circ {\rm Res} = {\rm Res} \circ \delta_K^{-1}$. Enfin, on a $\gamma_L \circ {\rm Res} = f.{\rm Res} \circ \gamma_K$ car l'image du Frobenius de $\widetilde{\Gamma}_L$ dans $\widetilde{\Gamma}_K$ est la puissance f-ième du Frobenius de $\widetilde{\Gamma}_K$. Le résultat découle alors de la définition de ${\rm inv}_K$.

□

On sait que $H^2(\widetilde{\Gamma}_K, K^*_{\rm nr}) = {\rm Br}\,(K^{\rm nr}/K)$ est un sous-groupe du groupe de Brauer ${\rm Br}\,K$. Le très important énoncé suivant montre que c'est en fait ${\rm Br}\,K$ tout entier. La méthode que nous avons suivie ne repose finalement que sur des résultats généraux de cohomologie des groupes combinés avec les propriétés de base des corps locaux. Par contre elle passe par le lemme 4.2 et la proposition 4.3, qui utilisent de façon essentielle le fait que le corps résiduel de K est fini, alors que d'autres méthodes fonctionnent pour tout corps K complet pour une valuation discrète à corps résiduel parfait.

Theorème 4.5 *On a* ${\rm Br}\,(K^{\rm nr}/K) = {\rm Br}\,K$.

Démonstration : Soit L une extension finie galoisienne de K de groupe de Galois G. Soit $n = [L : K]$. La preuve repose sur deux lemmes :

Lemme 4.6 *Le groupe $H^2(G, L^*)$ est fini et son cardinal divise n.*

Démonstration : Si G est cyclique, cela résulte immédiatement de la proposition 4.3 et du théorème 1.32. Si maintenant G est un ℓ-groupe avec ℓ premier, son centre est non trivial et il possède donc a fortiori un sous-groupe distingué $H = {\rm Gal}\,(L/K_1)$ de cardinal ℓ. On obtient alors le résultat par récurrence sur le cardinal de G via la suite exacte

$$0 \to H^2({\rm Gal}\,(K_1/K), K_1^*) \to H^2(G, L^*) \to H^2({\rm Gal}\,(L/K_1), L^*).$$

Dans le cas général, soit S l'ensemble des nombres premiers divisant n et considérons, pour $\ell \in S$, un ℓ-Sylow G_ℓ de G. Comme $H^2(G, L^*) = \bigoplus_{\ell \in S} H^2(G, L^*)\{\ell\}$, la proposition 2.2 dit que la restriction

$$H^2(G, L^*) \to \bigoplus_{\ell \in S} H^2(G_\ell, L^*)$$

est injective. Le cas des ℓ-groupes (appliqué à l'extension finie de K associée à chaque G_ℓ par la correspondance de Galois) donne alors que le cardinal de $H^2(G, L^*)$ est fini et divise $\prod_{\ell \in S} \#G_\ell = n$.

□

Lemme 4.7 *Soit K_n l'extension non ramifiée de K de degré n. Alors on a*

$$H^2(G, L^*) = H^2(\mathrm{Gal}\,(K_n/K), K_n^*),$$

où on a identifié les deux groupes avec leur image dans $\mathrm{Br}\,K$.

Démonstration : D'après le lemme 4.6, le cardinal de $H^2(G, L^*)$ divise $n = [L : K] = [K_n : K]$, qui est le cardinal de $H^2(\mathrm{Gal}\,(K_n/K), K_n^*)$ d'après la proposition 4.3 et le théorème 1.32 puisque K_n/K est cyclique (elle est non ramifiée et le corps résiduel de K est fini). Il suffit donc de montrer que $H^2(\mathrm{Gal}\,(K_n/K), K_n^*) \subset H^2(G, L^*)$. D'après la proposition 4.4, on a un diagramme commutatif dont les flèches inv_K et inv_L sont des isomorphismes et la première ligne est exacte :

$$\begin{array}{ccccccc}
0 & \longrightarrow & H^2(G, L^*) & \longrightarrow & \mathrm{Br}\,K & \xrightarrow{\mathrm{Res}} & \mathrm{Br}\,L \\
 & & & & \uparrow & & \uparrow \\
 & & & & H^2(\widetilde{\Gamma}_K, K_{\mathrm{nr}}^*) & \xrightarrow{\mathrm{Res}} & H^2(\widetilde{\Gamma}_L, L_{\mathrm{nr}}^*) \\
 & & & & \downarrow{\scriptstyle \mathrm{inv}_K} & & \downarrow{\scriptstyle \mathrm{inv}_L} \\
 & & & & \mathbf{Q}/\mathbf{Z} & \xrightarrow{.n} & \mathbf{Q}/\mathbf{Z}
\end{array}$$

Soit $a \in H^2(\mathrm{Gal}\,(K_n/K), K_n^*)$. Alors on a $na = 0$ et $a \in H^2(\widetilde{\Gamma}_K, K_{\mathrm{nr}}^*)$ puisque K_n/K est non ramifiée. Le diagramme donne alors que la restriction de a à $\mathrm{Br}\,L$ est nul, i.e. $a \in H^2(G, L^*)$.

□

Fin de la preuve du théorème 4.5 : Comme $\mathrm{Br}\,K$ est la limite inductive (sur les extensions finies galoisiennes L de K) des $H^2(\mathrm{Gal}\,(L/K), L^*)$, le lemme précédent donne que $\mathrm{Br}\,K$ est inclus dans la limite inductive (sur $n > 0$) des $H^2(\mathrm{Gal}\,(K_n/K), K_n^*)$, donc dans $\mathrm{Br}\,(K_{\mathrm{nr}}/K)$.

□

On en déduit :

Theorème 4.8 *Soit K un corps local. Alors on a un isomorphisme*

$$\mathrm{inv}_K : \mathrm{Br}\,K \to \mathbf{Q}/\mathbf{Z}.$$

Si L est une extension finie de K, la restriction $\mathrm{Br}\,K \to \mathrm{Br}\,L$ *correspond à la multiplication par* $[L : K]$ *dans* $\mathbf{Q}/\mathbf{Z}$ *et si de plus L/K est séparable, la corestriction* $\mathrm{Br}\,L \to \mathrm{Br}\,K$ *correspond à l'identité de* $\mathbf{Q}/\mathbf{Z}$.

Démonstration : Cela résulte du théorème 4.5, de la proposition 4.4, et de la formule $\mathrm{Cor} \circ \mathrm{Res} = .[L : K]$.

□

Corollaire 4.9 *Sous les hypothèses du théorème 4.8, un élément a de $\mathrm{Br}\, K$ a une image nulle dans $\mathrm{Br}\, L$ si et seulement si $na = 0$.*

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

4.3. Dimension cohomologique ; théorème de finitude

Soit ℓ un nombre premier. Soit G un groupe profini. On dira que ℓ^∞ divise l'indice d'un sous-groupe fermé H de G si pour tout $m > 0$, il existe un sous-groupe ouvert U de G contenant H tel que G/U soit divisible par ℓ^m. De même on dira que l'ordre de G est divisible par ℓ^∞ si ℓ^∞ divise l'indice de $\{1\}$ dans G.

On déduit du théorème 4.5 la dimension cohomologique d'un corps local :

Theorème 4.10 *Soit K un corps local. Soit ℓ un nombre premier. On note K^{nr} l'extension maximale non ramifiée de K.*

a) Soit L une extension algébrique séparable de K. Si ℓ^∞ divise $[L : K]$, alors $\mathrm{cd}_\ell(L) \leq 1$ (et $(\mathrm{Br}\, L)\{\ell\} = 0$).

b) On a $\mathrm{cd}(K_{\mathrm{nr}}) \leq 1$.

c) Si ℓ est différent de la caractéristique de K, on a et $\mathrm{cd}_\ell(K) = 2$. En particulier $\mathrm{cd}(K) = 2$.

Démonstration : a) Noter déjà que si ℓ est la caractéristique de K, la propriété $\mathrm{cd}_\ell(L) \leq 1$ est automatique. Il suffit de montrer que $(\mathrm{Br}\, L_1)\{\ell\} = 0$ pour toute extension algébrique séparable de L (théorème 3.27), et on est immédiatement ramené au cas $L_1 = L$ vu que ℓ^∞ divise a fortiori $[L_1 : K]$. On observe que $\mathrm{Br}\, L$ est la limite inductive des $\mathrm{Br}\, K'$ pour K' extension finie de K incluse dans L, les flèches de transition étant les restrictions (cela résulte de la proposition 3.7). Soit K' une telle extension et soit $\alpha \in \mathrm{Br}\, K'$ un élément de ℓ^m-torsion avec $m > 0$. Alors il existe une extension intermédiaire K_1 de L/K', finie sur K', et dont le degré sur K' est divisible par ℓ^m vu que ℓ^∞ divise $[L : K']$. Alors la restriction de α dans $\mathrm{Br}\, K_1$ est nulle par le théorème 4.8, donc a fortiori son image dans $\mathrm{Br}\, L$. Finalement on a montré $(\mathrm{Br}\, L)\{\ell\} = 0$ comme on voulait.

b) On applique a) à K^{nr}, ce qui est légitime vu que pour tout ℓ premier, l'ordre de $\mathrm{Gal}\,(K^{\mathrm{nr}}/K) \simeq \widehat{\mathbf{Z}}$ est divisible par ℓ^∞.

c) Soit $\Gamma_K = \mathrm{Gal}\,(\overline{K}/K)$ et prenons pour H le sous-groupe fermé $H := \mathrm{Gal}\,(\overline{K}/K^{\mathrm{nr}})$. On vient de voir que $\mathrm{cd}_\ell(H) \leq 1$ et par ailleurs $\mathrm{cd}_\ell(\Gamma_K/H) \leq 1$ car Γ_K/H est le groupe de Galois absolu du corps résiduel κ, qui est supposé fini. On obtient alord $\mathrm{cd}_\ell(K) \leq 2$ par la proposition 3.17. D'autre part pour ℓ différent de la caractéristique de K, on a $H^2(K, \mu_\ell) = (\mathrm{Br}\,K)[\ell] \neq 0$, donc $\mathrm{cd}_\ell(K) = 2$.

□

Remarque : Si K est de caractéristique $p > 0$, alors $\mathrm{cd}_p(K) = 1$ avec notre définition (bien que $(\mathrm{Br}\,K)[p]$ ne soit pas nul, ce qui montre que cette définition n'est pas bonne pour les corps imparfaits de caractéristique p...). En effet on sait que $\mathrm{cd}_p(K) \leq 1$, et $H^1(K, \mu_p) = K^*/K^{*^p}$ est non nul. Par ailleurs on verra plus tard que pour $\ell \neq \mathrm{Car}\,K$, on a $\mathrm{scd}_\ell(K) = 2$.

Proposition 4.11 *Soit K un corps p-adique. Soit $n > 0$.*

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, $i \geq 1$ ([11], 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. Comme $\mathrm{Br}\,K \simeq \mathbf{Q}/\mathbf{Z}$, on a $H^2(K, \mu_n) = (\mathrm{Br}\,K)[n] \simeq \mathbf{Z}/n\mathbf{Z}$.

□

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 $H^1(K, \mathbf{Z}/p)$ soit fini. Par contre la preuve de la proposition 4.11 fonctionne pour n non divisible par p, et de même le corollaire qui suit est encore valable si l'ordre de M n'est pas divisible par p.

Corollaire 4.12 *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.

□

4.4. Exercices

1. Soit p un nombre premier. Soient $K = \mathbf{F}_p((t))$ et $\overline{K}$ une clôture séparable de K. On note Γ_K le groupe de Galois absolu de K et Γ_p un p-Sylow de Γ_K. Soit $L \subset \overline{K}$ le corps fixe de Γ_p.

a) Montrer que $\mathrm{cd}(L) \leq 1$.

b) A-t-on $\mathrm{Br}\, L = 0$?

2. 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. On suppose que $[L : K]$ est divisible par p^∞. Que vaut $(\mathrm{Br}\, L)\{p\}$?

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.

3. 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.

5. Application de réciprocité d'un corps local ; module dualisant d'un corps p-adique

Dans ce chapitre, on désigne par K un corps local (p-adique, ou extension finie de $\mathbf{F}_p((t))$). Nous commençons l'étude du groupe de Galois abélien

$\mathrm{Gal}\,(K^{\mathrm{ab}}/K)$, qui sera complétée dans la section suivante. Les deux paragraphes qui suivent sont relativement indépendants, mais en rassemblant leurs résultats on peut retrouver le théorème d'existence (exercice 3) qui sera démontré par une autre méthode (théorie de Lubin-Tate) dans le chapitre suivant.

5.1. Application de réciprocité locale

Définition 5.1 Soit L une extension finie galoisienne de groupe G de 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 $\mathrm{inv}_K(u_{L/K}) = 1/n \in \mathbf{Q}/\mathbf{Z}$.

Rappelons qu'on a un isomorphisme $\mathrm{inv}_K : \mathrm{Br}\,K \to \mathbf{Q}/\mathbf{Z}$ (théorème 4.8) et que le groupe $\mathrm{Br}\,(L/K)$ est précisément le sous-groupe de n-torsion de $\mathrm{Br}\,K$ (corollaire 4.9), ce qui justifie la définition ci-dessus. Nous pouvons alors appliquer le théorème 2.12 (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 le théorème 4.8). En prenant $n = -2$ et en appliquant la proposition 1.27, on obtient

Theorème 5.2 *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 5.3 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[26] 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}.

26. Pour effectuer ce passage à la limite, il y a une compatibilité à vérifier entre $\omega_{L/K}$ et $\omega_{F/K}$ si $F \supset L \supset K$; celle-ci résulte de la proposition 5.4 ci-dessous.

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 pour un corps p-adique, le groupe 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 soit le *théorème d'existence* pour les corps locaux, soit le *théorème de dualité locale de Tate* (que nous rencontrerons un peu plus loin dans ce chapitre). 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 5.4 *Soit L une extension finie abélienne d'un corps local 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[27]

$$\chi(\omega_{L/K}(\bar{a})) = \mathrm{inv}_K(\bar{a} \cup d_\chi)$$

où $\mathrm{inv}_K : \mathrm{Br}\,(L/K) \to \mathbf{Q}/\mathbf{Z}$ 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

$$u \cup s = \bar{a} \in \widehat{H}^0(G, L^*)$$

d'où, par associativité du cup-produit (proposition 1.37) et compatibilité avec les cobords (proposition 1.36)

$$\bar{a} \cup d_\chi = u \cup (s \cup d_\chi) = u \cup (d(s \cup \chi))$$

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

$$u \cup (d(s \cup \chi)) = u \cup r = r.u \in \mathbf{Q}/\mathbf{Z}$$

27. 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.

Or on a précisément l'égalité $\mathrm{inv}_K(r.u) = r/n$ par définition de u donc finalement $\mathrm{inv}_K(r.u) = \chi(s)$, ou encore

$$\mathrm{inv}_K(\bar{a} \cup d_\chi) = \chi(s)$$

comme on voulait.

□

Corollaire 5.5 *Soit K un corps local de groupe de Galois $\Gamma = \mathrm{Gal}\,(\overline{K}/K)$. Soit χ un caractère de Γ^{ab} (ou de Γ, cela revient au même). Soit $b \in K^*$. Alors*

$$\mathrm{inv}_K(b \cup \chi) = \chi(\omega(b))$$

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.

□

5.2. Module dualisant ; applications

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. [12], 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 5.6 *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.*

Autrement dit on a $\mathrm{Hom}_G(A, I) \simeq H^n(G, A)^*$ (l'isomorphisme étant fonctoriel) pour tout G-module discret fini A. On a un théorème et des définitions analogues avec la p-dimension cohomologique (en se limitant aux modules de torsion p-primaire). Notons aussi que si A est un G-module discret de torsion (pas forcément fini), on obtient en passant à la limite que le groupe discret $H^n(G, A)$ est dual du groupe profini $\mathrm{Hom}_G(A, I)$ (muni de la topologie de la convergence simple)

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 [12], partie I, annexe 1, ou encore [10], paragraphe III.4). Nous allons ici calculer le module dualisant d'un corps p-adique [28], et en déduire une application à la dimension cohomologique stricte d'un corps p-adique et au théorème de dualité de Tate.

Proposition 5.7 *Soit Γ un groupe profini de dimension cohomologique $n \in \mathbf{N}^*$. Soit U un sous-groupe ouvert de Γ. Soit I le module dualisant de Γ. Alors le module dualisant de U est I vu comme U-module.*

Démonstration : On a $\mathrm{cd}(U) = \mathrm{cd}(\Gamma)$ (cela résulte de l'exercice 1.b) du chapitre 3). Le résultat découle alors du lemme de Shapiro en prenant $M = I_\Gamma^U(A)$ (où A est un U-module fini) dans la propriété qui caractérise le module dualisant.

□

Soit maintenant K un corps p-adique. On a vu (théorème 4.10) que son groupe de Galois $\Gamma := \Gamma_K$ était de dimension cohomologique 2 et que $H^2(\Gamma, A)$ était fini pour tout Γ-module fini A (corollaire 4.12). On peut donc appliquer les résultats précédents avec $n = 2$. La proposition suivante calcule le module dualisant I de Γ.

Proposition 5.8 *Le module dualisant I de Γ est canoniquement isomorphe au Γ-module μ des racines de l'unité de $\overline{K}^*$.*

Démonstration : Soit $n > 0$, notons I_n le noyau de la multiplication par n dans I. Pour tout sous-groupe ouvert U de Γ, I est aussi le module dualisant de U d'où, en appliquant la définition du module dualisant :

$$\mathrm{Hom}_U(\mu_n, I_n) = \mathrm{Hom}_U(\mu_n, I) \simeq H^2(U, \mu_n)^* = \mathbf{Z}/n\mathbf{Z}$$

la dernière égalité venant de la proposition 4.11. Ainsi le groupe $\mathrm{Hom}_U(\mu_n, I_n)$ est indépendant de U et on obtient $\mathrm{Hom}(\mu_n, I_n) \simeq \mathbf{Z}/n\mathbf{Z}$, avec en plus le fait que Γ opère trivialement sur ce groupe (en prenant $U = \Gamma$) et que l'isomorphisme est fonctoriel en n. On choisit le générateur f_n de $\mathrm{Hom}_\Gamma(\mu_n, I_n)$ correspondant à $\bar{1} \in \mathbf{Z}/n\mathbf{Z}$. L'homomorphisme f_n est injectif car d'ordre n. Il est également surjectif sinon on aurait un x de I_n qui n'est pas dans son image, d'où un homomorphisme de μ_n dans I_n qui ne serait pas dans le

28. Comme d'habitude les résultats sont valables pour un corps local de caractéristique p, à condition de se limiter à des modules sans p-torsion.

sous-groupe engendré par f_n. En définissant f par $f_{|\mu_n} = f_n$, on obtient un isomorphisme de Γ-modules de μ dans I.

□

On en déduit :

Theorème 5.9 *Soit K un corps p-adique. Alors la dimension cohomologique stricte de K est 2.*

Démonstration : On utilise la proposition 3.18. 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. D'après la proposition 5.8, ce dernier groupe est dual de $\mathrm{Hom}_U(\mathbf{Q}/\mathbf{Z}, \mu)$. Soit L/K l'extension finie correspondant à U. Alors l'image d'un homomorphisme $f : \mathbf{Q}/\mathbf{Z} \to \mu$ de U-modules doit être divisible et incluse dans $H^0(L, \mu)$. 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 $H^0(L, \mu)$ est fini. On en conclut que $\mathrm{Im}\, f = 0$, soit $\mathrm{Hom}_U(\mathbf{Q}/\mathbf{Z}, \mu) = 0$, ce qui achève la preuve.

□

Soit k un corps de groupe de Galois absolu $\Gamma_k = \mathrm{Gal}\,(\bar{k}/k)$. Pour tout Γ_k-module fini M, on note

$$M' := \mathrm{Hom}_{\mathbf{Z}}(M, \bar{k}^*) = \mathrm{Hom}(M, \mu)$$

son *dual de Cartier*. Si M est d'ordre n, on a aussi $M' = \mathrm{Hom}(M, \mu_n)$.

Theorème 5.10 (Tate) *Soient K un corps p-adique de groupe de Galois Γ, et M un Γ-module fini. Alors pour $i = 0, 1, 2$, le cup-produit*

$$H^i(\Gamma, M) \times H^{2-i}(\Gamma, M') \to H^2(K, \overline{K}^*) = \mathbf{Q}/\mathbf{Z}$$

est une dualité parfaite de groupes finis.

Démonstration : La finitude de tous les groupes a déjà été vue (corollaire 4.12). Pour $i = 2$, le théorème exprime que les groupes $H^2(\Gamma, M)$ et $\mathrm{Hom}_\Gamma(M, \mu)$ sont en dualité via l'application bilinéaire $(x, a) \mapsto a.x$ de $H^2(\Gamma, M) \times \mathrm{Hom}_\Gamma(M, \mu)$ dans $H^2(\Gamma, \mu) = \mathbf{Q}/\mathbf{Z}$; or ceci résulte de la proposition 5.8. Le cas $i = 0$ est symétrique car $(M')' = M$. Pour traiter le cas $i = 1$, il suffit donc de montrer que l'homomorphisme

$$H^1(\Gamma, M) \to H^1(\Gamma, M')^*$$

induit par le cup-produit est injectif (car en appliquant ensuite le même résultat à M', on obtiendra en plus que le cardinal du groupe de gauche est au moins celui du groupe de droite). Pour cela on écrit une suite exacte

$$0 \to M \to B \to C \to 0$$

avec $H^1(\Gamma, B) = 0$ en prenant par exemple pour B l'induit de M. D'après les propriétés de compatibilité du cup-produit vis à vis des suites exactes (proposition 1.38), on a un diagramme commutatif (au signe près) exact

$$\begin{array}{ccccccc} H^0(\Gamma, B) & \longrightarrow & H^0(\Gamma, C) & \longrightarrow & H^1(\Gamma, M) & \longrightarrow & 0 \\ \downarrow & & \downarrow & & \downarrow & & \\ H^2(\Gamma, B')^* & \longrightarrow & H^2(\Gamma, C')^* & \longrightarrow & H^1(\Gamma, M')^* & & \end{array}$$

D'après la proposition 5.8, les deux premières flèches verticales sont des isomorphismes (bien que B et C ne soient pas forcément finis, les Γ-module B' et C' sont de torsion, ce qui suffit). On en déduit l'injectivité de la troisième par chasse au diagramme.

□

Remarque : Pour des corps locaux d'égale caractéristique p, le théorème reste vrai (avec la même preuve) à condition de se limiter à des M dont la torsion est première à p. Sinon le résultat analogue est nettement plus compliqué (voir [13] ou [7], paragraphe III.6.), ne serait-ce que parce que $H^1(\Gamma, M)$ n'est pas fini en général.

Par ailleurs, il existe une généralisation du théorème 5.10 au cas où A est seulement supposé de type fini sur $\mathbf{Z}$ (dans ce cas la situation n'est plus symétrique, le Γ-module A' étant alors le groupe des $\overline{K}$-points d'un *groupe de type multiplicatif* sur K). Voir [12], partie II, paragraphe 5.8.

Theorème 5.11 *Le groupe* Γ^{ab} *est isomorphe à* $(K^*)^\wedge := \varprojlim_{n \in \mathbf{N}^*} (K^*/K^{*n})$.

Noter que $(K^*)^\wedge$ est simplement le complété profini [29] de K^* vu que les K^*/K^{*n} sont finis. En particulier Γ^{ab} est isomorphe (non canoniquement) à $\widehat{\mathbf{Z}} \times U_K$. Ses quotients finis correspondent exactement aux quotients finis de K^* (que l'on précisera plus tard, via le *théorème d'existence*; voir exercice 3 de ce chapitre pour une preuve basée sur les résultats de dualité ci-dessus et le théorème de Tate-Nakayama). Le théorème de dualité 5.10 donne d'ailleurs directement la dualité (classique en théorie du corps de classes local) entre $H^1(\Gamma, \mathbf{Z}/n) = \mathrm{Hom}_c(\Gamma, \mathbf{Z}/n)$ et K^*/K^{*n}.

29. Le théorème vaut pour une extension finie de $\mathbf{F}_p((t))$ à condition de se limiter aux sous-groupes *ouverts* d'indice fini. Cela peut par exemple se déduire de l'analogue du théorème 5.10 dans ce cadre, ou des résultats du prochain chapitre.

Démonstration : Par dualité de Pontryagin, le groupe Γ^{ab} est le dual de son dual $H^1(\Gamma, \mathbf{Q}/\mathbf{Z})$. Comme $H^1(\Gamma, \mathbf{Q}/\mathbf{Z})$ est la limite inductive des $H^1(\Gamma, \mathbf{Z}/n)$, son dual est la limite projective des $H^1(\Gamma, \mathbf{Z}/n)^*$. Or par le théorème de dualité 5.10, le groupe $H^1(\Gamma, \mathbf{Z}/n)^*$ est isomorphe à $H^1(K, \mu_n) = K^*/K^{*n}$.

□

5.3. Exercices

1. 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 $\mathrm{scd}(K) = 2$.

2. 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 [30] 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 $H^2(K, A) = 0$.

3. Soit K un corps p-adique de groupe de Galois absolu $\Gamma = \mathrm{Gal}\,(\overline{K}/K)$. On considère un sous-groupe U d'indice fini de K^*. On se propose de montrer ("théorème d'existence" [31]) qu'il existe une extension abélienne finie L de K (unique à isomorphisme près) telle que $U = NL^*$. La méthode de cet exercice va consister à utiliser l'application de réciprocité (donnée par le théorème de Tate-Nakayama) associée à une extension finie abélienne de K, et le théorème de dualité locale de Tate.

a) Montrer qu'il existe une extension finie abélienne L de K telle que le cup-produit induise une dualité parfaite

$$H^1(\mathrm{Gal}\,(L/K), \mathbf{Q}/\mathbf{Z}) \times K^*/U \to \mathbf{Q}/\mathbf{Z}$$

30. Ceci résulte de l'existence de l'accouplement de Weil.

31. Nous retrouverons ce résultat par une méthode plus explicite dans le prochain chapitre, via la théorie de Lubin-Tate. Notons qu'il vaut encore pour un corps local de caractéristique $p > 0$ à condition de se limiter aux sous-groupes *ouverts* d'indice fini de K^*. On peut aussi l'obtenir en se ramenant aux extensions de Kummer en caractéristique zéro, et d'Artin-Schreier en caractéristique p, voir [11], chapitre XIV.

entre le sous-groupe fini $H^1(\mathrm{Gal}\,(L/K), \mathbf{Q}/\mathbf{Z})$ de $H^1(\Gamma^{\mathrm{ab}}, \mathbf{Q}/\mathbf{Z})$ et le quotient fini K^*/U de $\widehat{K}^*$.

b) Soit $G = \mathrm{Gal}\,(L/K)$ et pour tout a de K^*, notons $\bar{a}$ sa classe dans K^*/NL^*. Montrer que U est le noyau à droite de l'accouplement

$$H^1(G, \mathbf{Q}/\mathbf{Z}) \times K^* \to \mathbf{Q}/\mathbf{Z}$$

donné par $(\chi, a) \mapsto \chi(\omega_{L/K}(\bar{a}))$.

c) En déduire que $U = NL^*$.

d) Montrer que si on fixe la clôture algébrique $\overline{K}$, il existe une unique extension finie abélienne $L \subset \overline{K}$ de K vérifiant c).

e) Montrer que réciproquement pour tout extension finie abélienne L de K, le sous-groupe NL^* de K^* est d'indice fini, et fermé pour la topologie p-adique sur K^* (pour cette dernière propriété, on observera que la norme $N : L^* \to K^*$ est une application *propre*, i.e. l'image réciproque d'un compact est compact). En déduire que tout sous-groupe d'indice fini de K^* est fermé.

4. Soit K un corps p-adique de groupe de Galois absolu $\Gamma = \mathrm{Gal}\,(\overline{K}/K)$. On note $U = \mathrm{Gal}\,(\overline{K}/K_{\mathrm{nr}})$ son groupe d'inertie. On rappelle 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). On considère un Γ-module fini A de cardinal premier à p.

a) Montrer que $H^1(U, A) = H^1(V, A^{U_p})$.

b) Soit ℓ un nombre premier différent de p. Soit B un $\mathbf{Z}_\ell$-module fini et ℓ-primaire. On fixe un sous-groupe ouvert W de $\mathbf{Z}_l$ qui agit trivialement sur B. Montrer que $H^1(W, B)$ est fini, et en déduire que $H^1(\mathbf{Z}_l, B)$ est fini.

c) Montrer que $H^i(U, A)$ est fini pour tout $i \geq 0$ et nul si $i \geq 2$.

5. On garde les hypothèses et notations de l'exercice précédent. On se propose de démontrer que la *caractéristique d'Euler-Poincaré*

$$\chi(A) := \frac{\#H^0(K, A).\#H^2(K, A)}{\#H^1(K, A)}$$

est 1 pour tout Γ-module fini A de torsion première à p (ce résultat admet une généralisation beaucoup plus difficile, due à Tate, cf. [12], paragraphe II.5.7).

a) En utilisant l'exercice précdent, montrer qu'on a

$$H^0(K, A) = H^0(\widehat{\mathbf{Z}}, H^0(U, A)); \quad H^2(K, A) = H^1(\widehat{\mathbf{Z}}, H^1(U, A)),$$

et une suite exacte

$$0 \to H^1(\widehat{\mathbf{Z}}, H^0(U, A)) \to H^1(K, A) \to H^0(\widehat{\mathbf{Z}}, H^1(U, A)) \to 0.$$

b) Conclure en utilisant l'exercice 12 du chapitre 3.

6. Soit K un corps p-adique de groupe de Galois absolu Γ. 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 de cohomologie non ramifiée* $H^i_{\mathrm{nr}}(K, A) := H^i(\mathrm{Gal}\,(K_{\mathrm{nr}}/K), A)$.

a) Soit A un Γ-module fini et non ramifié. Montrer que $H^0_{\mathrm{nr}}(K, A) = H^0(K, A)$, $H^i_{\mathrm{nr}}(K, A) = 0$ pour $i \geq 2$, et que le groupe $H^1_{\mathrm{nr}}(K, A)$ s'identifie à un sous-groupe de $H^1(K, A)$ dont le cardinal est celui de $H^0(K, A)$ (utiliser l'exercice 4).

On suppose dans toute la suite que A est un Γ-module fni, non ramifié, et d'ordre premier à p.

b) Montrer que le dual $A' = \mathrm{Hom}(A, \overline{K}^*)$ possède les mêmes propriétés.

c) Montrer que les groupes $H^1_{\mathrm{nr}}(K, A)$ et $H^1_{\mathrm{nr}}(K, A')$ sont orthogonaux pour l'accouplement local de Tate.

d) En utilisant l'exercice 5, montrer qu'on a

$$\#H^1(K, A') = \#H^1_{\mathrm{nr}}(K, A).\#H^1_{\mathrm{nr}}(K, A').$$

e) En déduire que pour l'accouplement local

$$H^1(K, A) \times H^1(K, A') \to \mathbf{Q}/\mathbf{Z},$$

chacun des sous-groupes $H^1_{\mathrm{nr}}(K, A)$ et $H^1_{\mathrm{nr}}(K, A')$ est l'orthogonal de l'autre.

7. Soit k un corps de groupe de Galois absolu Γ_k. Soit p un nombre premier différent de la caractéristique de k, et tel que k contienne une racine primitive p-ième ζ de 1. Le choix d'une telle ζ permet d'identifier $H^1(k, \mu_p)$ à $H^1(k, \mathbf{Z}/p) \subset H^1(k, \mathbf{Q}/\mathbf{Z})$. Pour tout élément a de k^*, on note $\chi_a \in H^1(k, \mathbf{Z}/p)$ le caractère de Γ_k associé à la classe de a dans $H^1(k, \mu_p) = k^*/k^{*p}$. Pour a, b dans k^*, on définit le *symbole* (a, b) comme le cup-produit de $\chi_a \in H^2(k, \mathbf{Z}) = H^1(k, \mathbf{Q}/\mathbf{Z})$ avec $b \in H^0(k, \bar{k}^*)$.

a) Montrer que 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^* (avec $a \neq 1$ pour la deuxième formule).

c) On suppose que k est un corps local. Montrer que si un élément b de k^* vérifie $(a, b) = 0$ pour tout a de k^*, alors $b \in k^{*p}$.

6. Théorie de Lubin-Tate

Le but de ce chapitre est de donner une description explicite, utilisant les *groupes formels*, de l'extension abélienne maximale d'un corps local. Cela permettra en particulier de donner une preuve facile (et indépendante de la caractéristique) du théorème d'existence (cf. exercice 3 du chapitre précédent), et également d'avoir explicitement des formules pour calculer les symboles locaux $(a, L/K) := \omega_{L/K}(a)$ quand $a \in K^*$ et L est une extension abélienne d'un corps local K. Ces formules seront également utiles pour la théorie du corps de classes global.

Dans toute la suite, on désigne par K un corps local (i.e. complet pour une valuation discrète, à corps résiduel fini) d'anneau des entiers $\mathcal{O}_K$. On pose aussi $U_K = \mathcal{O}_K^*$ et on note $\mathcal{M}_K$ l'idéal maximal de $\mathcal{O}_K$.

6.1. Groupes formels

La loi de groupe multiplicative sur $U_K^1 := 1 + \mathcal{M}_K$ correspond à la loi additive sur $\mathcal{M}_K$ donnée par $(X, Y) \mapsto X + Y + XY$. Cette observation est à l'origine de la définition suivante :

Définition 6.1 Soit A un anneau commutatif. Soit $F \in A[[X, Y]]$ une série formelle en deux variables. On dit que F est une *loi de groupe formel commutatif* si les propriétés suivantes sont satisfaites :

a) (associativité) $F(X, F(Y, Z)) = F(F(X, Y), Z)$.
b) (neutre) $F(0, Y) = Y$ et $F(X, 0) = X$.
c) (symétrique) Il existe un unique $G(X)$ tel que $F(X, G(X)) = 0$.
d) (commutativité) $F(X, Y) = F(Y, X)$.
e) $F(X, Y) \equiv X + Y \pmod{\deg 2}$.

(Deux séries formelles sont congruentes modulo $\deg n$ si elles ont les mêmes termes de degré $< n$; on peut vérifier que c) et e) peuvent se déduire des trois autres propriétés. Rappelons aussi que si n est un entier strictement positif, on peut substituer une famille de n séries formelles sans terme constant dans toute série formelle en n variables).

Si on pose $A = \mathcal{O}_K$, on peut alors définir $x \star y := F(x, y)$ pour x, y dans $\mathcal{M}_K$, ce qui fait de $\mathcal{M}_K$ un groupe commutatif qu'on notera $F(\mathcal{M}_K)$. On peut de même définir $F(\mathcal{M}_L)$ pour toute extension finie L de K, et même pour toute extension algébrique en passant à la limite. Le cas de $1 + \mathcal{M}_K$ correspond à la loi de groupe formel $F(X, Y) = X + Y + XY$.

Soit maintenant K un corps local dont le corps résiduel κ est de cardinal q. On fixe une uniformisante π de K et on pose $A = \mathcal{O}_K$. On note $\mathcal{F}_\pi$

l'ensemble des séries formelles $f \in A[[X]]$ telles que $f(X) \equiv \pi X$ mod. $\deg 2$ et $f(X) \equiv X^q$ mod. π (la deuxième condition signifie que $f(X) - X^q$ est divisible par π dans $A[[X]]$). On peut prendre par exemple $f(X) = \pi X + X^q$, ou encore $f(X) = (1+X)^p - 1$ sur $K = \mathbf{Q}_p$.

Theorème 6.2 *Soit $f \in \mathcal{F}_\pi$. Alors il existe une unique loi de groupe formel $F_f \in A[[X,Y]]$ telle que*

$$f(F_f(X,Y)) = F_f(f(X), f(Y))$$

(autrement dit f est un endomorphisme pour la loi F_f). On dit que F_f est la loi de groupe formel de Lubin-Tate associée à f et π.

La preuve est basée sur la proposition suivante.

Proposition 6.3 *Soient $f, g \in \mathcal{F}_\pi$. Soit $n \in \mathbf{N}^*$ et soit $\phi_1(X_1, ..., X_n)$ une forme linéaire en n variables à coefficients dans A. Alors il existe une unique série formelle $\phi \in A[[X_1, ..., X_n]]$ vérifiant :*

a) $\phi = \phi_1$ mod. $\deg 2$.
b) $f(\phi(X_1, ..., X_n)) = \phi(g(X_1), ..., g(X_n))$.

(On notera parfois $(g, g, ...g)$ la famille $(g(X_1), ..., g(X_n))$, et $\phi \circ g$ la série formelle en n variables $\phi \circ (g, g, ..., g) := \phi(g(X_1), ..., g(X_n)))$.

Démonstration : On construit ϕ par approximation successives : on va montrer par récurrence sur $r \geq 1$ que pour tout $r \geq 1$, il existe une unique (mod. $\deg r + 1$) $\phi^{(r)} \in A[[X_1, ..., X_n]]$ vérifiant a) et b) mod. $\deg r + 1$. Cela donnera bien comme unique solution du problème la série formelle ϕ définie par $\phi = \phi^{(r)}$ mod. $\deg r + 1$ pour tout $r \geq 1$. Noter en particulier qu'on devra avoir $\phi^{(r+1)} - \phi^{(r)}$ congru à 0 mod. $\deg r$.

On commence par prendre $\phi^{(1)} = \phi_1$ (et c'est unique modulo $\deg 2$ d'après a)). Supposons que $\phi^{(i)}$ a été construit pour $i \leq r$, et posons $\phi_i = \phi^{(i+1)} - \phi^{(i)}$, de sorte qu'on a $\phi_1 + ... + \phi_r = \phi^{(r)}$. La condition b) donne $f \circ \phi^{(r)} = \phi^{(r)} \circ g$ mod. $\deg(r+1)$, où on a écrit pour simplifier g au lieu de $(g, g, .., g)$. On cherche alors $\phi^{(r+1)}$ sous la forme $\phi^{(r+1)} = \phi^{(r)} + \phi_{r+1}$, et comme on l'a vu ϕ_{r+1} doit être congru à 0 modulo $\deg r$. On a

$$f \circ \phi^{(r)} \equiv \phi^{(r)} \circ g + E_{r+1}$$

mod. $\deg(r+2)$ avec $E_{r+1} \equiv 0$ mod. $\deg(r+1)$, et il s'agit de corriger l'erreur E_{r+1}. Comme le terme de degré 1 de f (sa dérivée en 0) est π et ϕ_{r+1} est congru à 0 mod. $\deg r$, on obtient

$$f \circ \phi^{(r+1)} \equiv f \circ \phi^{(r)} + \pi\phi_{r+1}$$

mod. $\deg(r+2)$ et de même

$$\phi^{(r)} \circ g + \phi_{r+1} \circ g \equiv \phi^{(r)} \circ g + \pi^{r+1}\phi_{r+1}$$

mod. $\deg(r+2)$ d'où

$$f\circ\phi^{(r+1)} - \phi^{(r+1)}\circ g \equiv f\circ\phi^{(r)} + \pi\phi_{r+1} - (\phi^{(r)}\circ g + \phi_{r+1}\circ g) \equiv E_{r+1} + (\pi - \pi^{r+1})\phi_{r+1}$$

mod. $\deg(r+2)$. On voit alors que l'unique solution est

$$\phi_{r+1} = -E_{r+1}/\pi(1-\pi^r)$$

et il faut juste encore vérifier que ϕ_{r+1} reste à coefficients dans A, ou encore que E_{r+1} est divisible par π. Comme pour $\phi \in \mathbf{F}_q[[X]]$ on a $\phi(X^q) = (\phi(X))^q$ et que $f(X) \equiv g(X) \equiv X^q$ mod. π, on a :

$$f \circ \phi^{(r)} - \varphi^{(r)} \circ g \equiv (\phi^{(r)}(X))^q - \varphi^{(r)}(X^q) \equiv 0$$

mod. π, ce qui conclut la preuve de la proposition.

□

Preuve du théorème 6.2 : On applique la proposition précédente en prenant pour $F_f(X,Y)$ l'unique solution de $F_f(X,Y) \equiv X+Y$ mod. $\deg 2$ et $f\circ F_f = F_f \circ (f,f)$. Pour vérifier les axiomes de groupe formel, on utilise l'unicité dans la proposition : par exemple pour a), on note que $F_f(F_f(X,Y),Z)$ et $F_f(X,F_f(Y,Z))$ sont tous deux solutions de $H(X,Y,Z) = X+Y+Z$ mod. $\deg 2$ et $H(f(X),f(Y),f(Z)) = f(H(X,Y,Z))$.

□

Proposition 6.4 *Soit $f \in \mathcal{F}_\pi$. Soit F_f la loi de groupe formel associée à f comme dans le théorème 6.2. Alors pour tout a de $A = \mathcal{O}_K$, il existe une unique série formelle $[a]_f \in A[[X]]$ vérifiant : $[a]_f \circ f = f \circ [a]_f$ et $[a]_f \equiv aX$ mod.* $\deg 2$. *De plus $[a]_f$ est un endomorphisme pour la loi de groupe formelle F_f.*

Noter que par définition $[1]_f$ est l'identité et $[\pi]_f = f$.

Démonstration : Pour f, g dans $\mathcal{F}_\pi$, définissons $[a]_{f,g}(T) \in A[[T]]$ comme l'unique série formelle (cf. proposition 6.3) vérifiant $[a]_{f,g}(T) \equiv aT$ mod. $\deg 2$ et $f([a]_{f,g}(T)) = [a]_{f,g}(g(T))$. Posons $[a]_f = [a]_{f,f}$. Alors l'unicité dans la proposition 6.3 donne l'égalité

$$F_f([a]_{f,g}(X), [a]_{f,g}(Y)) = [a]_{f,g}(F_g(X,Y)).$$

En effet chaque membre de cette égalité est une série formelle $H(X,Y) \in A[[X,Y]]$, congrue à $aX + aY$ mod. $\deg 2$, et vérifiant $H(g(X), g(Y)) = f(H(X,Y))$. Cela signifie que $[a]_{f,g}$ est un homomorphisme de groupes formels de F_g dans F_f, et en particulier $[a]_f$ est un endomorphisme de F_f. Les deux propriétés voulues résultent de la définition de $[a]_{f,f}$, et l'unicité est claire, toujours via la proposition 6.3.

□

Proposition 6.5 *L'application $a \mapsto [a]_f$ est un homomorphisme injectif d'anneaux de A dans* $\mathrm{End}(F_f)$.

Démonstration : Comme dans la proposition précédente, on montre que

$$[a+b]_{f,g}(T) = F_f([a]_{f,g}(T), [b]_{f,g}(T))$$

et

$$[ab]_{f,h}(T) = ([a]_{f,g} \circ [b]_{g,h})(T). \tag{3}$$

Par exemple les deux membres de la première égalité sont congrus à $aT + bT$ mod. $\deg 2$ et sont solutions de l'équation $f(H(T)) = H(g(T))$. En prenant $f = g = h$ on obtient que $a \mapsto [a]_f$ est un homomorphisme d'anneaux de A dans $\mathrm{End}(F_f)$. Il est injectif car le terme de degré 1 de $[a]_f$ est aX.

□

Noter que la proposition précédente confère à F_f une structure de A-*module formel*. En particulier $F_f(\mathcal{M}_L)$ est muni d'une structure de A-module pour toute extension algébrique L de K.

Proposition 6.6 *Soient $f, g \in \mathcal{F}_\pi$. Alors les lois de groupes F_f et F_g associées respectivement à f et g sont isomorphes.*

Démonstration : Par définition de $[a]_f$, on a $[1]_f(T) = T$. On en déduit via (3) que si a est dans A^*, alors $[a]_{f,g}$ est inversible d'inverse $[a^{-1}]_{g,f}$, et $[a]_{f,g}$ induit donc un isomorphisme de F_g dans F_f.

□

6.2. Changement d'uniformisante

On a vu au paragraphe précédent qu'un changement d'élément f dans $\mathcal{F}_\pi$ donnait des lois de groupes formels isomorphes. Il n'en va plus de même si c'est l'uniformisante π de $A := \mathcal{O}_K$ qu'on change. On va voir cependant qu'on retrouve des lois isomorphes à condition de monter sur l'anneau des entiers

$\widehat{A} := \mathcal{O}_{\widehat{K}}$ de la complétion $\widehat{K}$ de l'extension maximale non ramifiée $K_{\rm nr}$ de K. On note comme d'habitude $U_{\widehat{K}}$ le groupe multiplicatif $\widehat{A}^*$. On note σ le prolongement continu du Frobenius (générateur topologique de $\mathrm{Gal}\,(K_{\rm nr}/K)$) à $\widehat{K}$. Si $x \in \widehat{K}$, on note ${}^{\sigma}x$ le transformé de x par σ, et de même si $\theta \in \widehat{K}[[X]]$ est une série formelle, on note ${}^{\sigma}\theta$ la série formelle obtenue en appliquant σ à tous les coefficients de θ.

Lemme 6.7 *Soit $c \in \widehat{A}$ (resp. $c \in U_{\widehat{K}}$. Alors l'équation ${}^{\sigma}x - x = c$ (resp. ${}^{(\sigma-1)}x = c$) a une solution dans $\widehat{A}$ (resp. dans $U_{\widehat{K}}$).*

De plus, si x est un élément de $\widehat{A}$ vérifiant ${}^{\sigma}x = x$, alors $x \in A$.

Démonstration : Notons que l'uniformisante π reste de valuation 1 dans $\widehat{K}$, d'où des isomorphismes σ-équivariants de $U_{\widehat{K}}/U^1_{\widehat{K}}$ sur $\bar{\kappa}^*$ et de $U^n_{\widehat{K}}/U^{n+1}_{\widehat{K}}$ sur $\bar{\kappa}$ pour $n \geq 1$. Soit $c \in U_{\widehat{K}}$ d'image $\bar{c}$ dans $\bar{\kappa}^*$. L'équation ${}^{\sigma}\bar{x} = \bar{x}.\bar{c}$ a une solution dans $\bar{\kappa}^*$ car elle s'écrit $\bar{x}^q = \bar{x}.\bar{c}$ (où q est le cardinal de κ) et κ est algébriquement clos. Cela permet d'écrire $c =^{(\sigma-1)} x_1.a_1$ avec $x_1 \in U_{\widehat{K}}$ et $a_1 \in U^1_{\widehat{K}}$. Par récurrence on peut écrire $c =^{(\sigma-1)} (x_1 ... x_n).a_n$ avec $x_i \in U^{i-1}_{\widehat{K}}$ et $a_n \in U^n_{\widehat{K}}$; d'où $c =^{(\sigma-1)} x$, où x est le produit infini des x_i (qui converge par complétude de $U_{\widehat{K}}$, vu que son terme général tend vers 1). Le cas de l'équation ${}^{\sigma}x - x = c$ dans $\widehat{A}$ est similaire, via les isomorphismes de $\mathcal{M}^n_{\widehat{K}}/\mathcal{M}^{n+1}_{\widehat{K}}$ avec $\bar{\kappa}$.

Si maintenant $x \in \widehat{A}$ vérifie ${}^{\sigma}x = x$, on montre par récurrence sur $n > 0$ que x s'écrit $x = x_n + \pi^n y_n$ avec $x_n \in A$ et $y_n \in \widehat{A}$: pour $n = 1$, la propriété ${}^{\sigma}x = x$ donne que l'image $\bar{x}$ de x dans $\bar{\kappa}$ est dans κ, donc x s'écrit $x = x_1 + \pi y_1$ avec $x_1 \in A$ et $y_1 \in \widehat{A}$; il suffit ensuite d'appliquer le même raisonnement à y_n au lieu de x. Alors x est la limite des x_n, donc reste dans A puisque A est complet.

□

Lemme 6.8 *Soient π et ω deux uniformisantes de K, on pose $\omega = u.\pi$ avec $u \in U_K$. Soient $f \in \mathcal{F}_\pi$ et $g \in \mathcal{F}_\omega$. Soit $H \in A[[X]]$ une série formelle congrue à uX mod. 2, et vérifiant $f \circ H = H \circ f$. Alors il existe $\varepsilon \in U_{\widehat{K}}$ et une série formelle $\phi(X) \in \widehat{A}[[X]]$, congrue à εX mod. 2, tels que :*

a) ${}^{\sigma}\phi = \phi \circ H$;

b) ${}^{\sigma}\phi \circ f = g \circ \phi$.

Démonstration : La première étape consiste à déterminer une série formelle $\alpha(X)$ vérifiant la condition a). On l'obtient comme la limite d'une suite de polynômes $\alpha_r(x) = \sum_{i=1}^{r} a_i X^i$ dans $\hat{A}[X]$, vérifiant

$$ {}^{\sigma}\alpha_r(X) - \alpha_r(H(X)) \equiv c_{r+1} X^{r+1} $$

mod. $\deg(r+2)$, avec $c_{r+1} \in \widehat{A}$. Pour $r=1$, cela signifie juste que $u =^{(\sigma-1)} a_1$, qui a bien une solution $a_1 = \varepsilon$ dans $U_{\widehat{K}}$ d'après le lemme 6.7. Supposons α_r construit et posons

$$\alpha_{r+1}(X) = \alpha_r(X) + a_{r+1}X^{r+1}$$

avec $a_{r+1} = a.\varepsilon^{r+1}$, où $a \in \widehat{A}$ est solution de ${}^{\sigma}a - a = -c_{r+1}/(\varepsilon u)^{r+1}$ (une telle solution existe par loc. cit.). Comme ${}^{\sigma}\varepsilon = \varepsilon u$, on obtient

$${}^{\sigma}a_{r+1} - a_{r+1}u^{r+1} = ({}^{\sigma}a - a).(\varepsilon u)^{r+1} = -c_{r+1}$$

d'où on déduit

$${}^{\sigma}\alpha_{r+1}(X) - \alpha_{r+1}(H(X)) \equiv (c_{r+1} + ({}^{\sigma}a_{r+1} - a_{r+1}u^{r+1}))X^{r+1} \equiv 0$$

mod. $\deg(r+2)$ comme on voulait.

On observe maintenant que toute serie formelle du type $\phi = \beta \circ \alpha$ avec $\beta(X) \equiv X$ mod. $\deg 2$ vérifie encore la condition a) et il s'agit de choisir β telle que ϕ vérifie aussi b). Pour cela, on pose

$$h =^{\sigma} \alpha \circ f \circ \alpha^{-1} = \alpha \circ H \circ f \circ \alpha^{-1}$$

où α^{-1} est la série formelle sans terme constant réciproque de α (bien définie car $\alpha(X) \equiv \varepsilon X$ mod. $\deg 2$ avec ε inversible). On cherche β telle que $g \circ \beta = \beta \circ h$, ce qui impliquera bien

$$g \circ \phi = g \circ \beta \circ \alpha = \beta \circ h \circ \alpha = \beta \circ^{\sigma} \alpha \circ f =^{\sigma} \phi \circ f$$

comme recherché.

On observe d'abord que

$${}^{\sigma}h =^{\sigma} \alpha \circ H \circ f \circ^{\sigma} \alpha^{-1} =^{\sigma} \alpha \circ f \circ H \circ^{\sigma} \alpha^{-1} = h$$

donc $h \in A[[X]]$ d'après le lemme 6.7. D'autre part $h(X) \equiv^{\sigma} \varepsilon\pi\varepsilon^{-1} \equiv u\pi X \equiv \omega X$ mod. $\deg 2$, et

$$h(X) \equiv^{\sigma} \alpha(f(\alpha^{-1}(X)) \equiv^{\sigma} \alpha(\alpha^{-1}(X)^q) \equiv^{\sigma} \alpha({}^{-\sigma}\alpha(X^q)) \equiv X^q$$

mod. π (observer que modulo π, le Frobenius σ agit comme l'élévation à la puissance q-ième). On détermine alors β comme limite de polynômes β_r de degré $\leq r$, que l'on construit par récurrence pour vérifier

$$g(\beta_r(X)) - \beta_r(h(X)) \equiv c_{r+1}X^{r+1}$$

mod. X^{r+2} avec $c_{r+1} \in A$, ce qui donnera bien $g \circ \beta = \beta \circ h$. On prend $b_1 = 1$. On note que c_{r+1} est nul mod. π car

$$g(\beta_r(X)) \equiv \beta_r(X)^q \equiv \beta_r(X^q) \equiv \beta_r(h(X))$$

mod. π. On pose alors $\beta_{r+1}(X) = \beta_r(X) + b_{r+1}X^{r+1}$ avec

$$b_{r+1} = -c_{r+1}/(\omega - \omega^{r+1}),$$

qui est bien dans A. Alors

$$g(\beta_{r+1}(X)) - \beta_{r+1}(h(X)) \equiv (c_{r+1} + (\omega - \omega^{r+1})b_{r+1})X^{r+1} \equiv 0$$

mod. $\deg(r+2)$ comme recherché, ce qui termine la récurrence.

□

Proposition 6.9 *Soient π et $\omega = u.\pi$ deux uniformisantes de K. Soient $f \in \mathcal{F}_\pi$ et $g \in \mathcal{F}_\omega$. Alors il existe $\varepsilon \in U_{\widehat{K}}$ et $\phi \in \widehat{A}[[X]]$ avec $\phi(X) \equiv \varepsilon X$ mod. 2, tels que :*

a) ${}^\sigma\phi = \phi \circ [u]_f$;
b) $\phi \circ F_f = F_g \circ (\phi, \phi)$;
c) $\phi \circ [a]_f = [a]_g \circ \phi$ *pour tout* $a \in \mathcal{O}_K$.

En particulier ϕ est un isomorphisme de A-modules de F_f sur F_g.

Démonstration : On applique le lemme 6.8 à $H := [u]_f$ (cf. proposition 6.4). On obtient $\phi \in \widehat{A}[[X]]$ avec $\phi(x) \equiv \varepsilon X$ mod. 2 et $\varepsilon \in U_{\widehat{K}}$, vérifiant déjà ${}^\sigma\phi = \phi \circ [u]_f$ et ${}^\sigma\phi \circ f = g \circ \phi$.. Montrons par exemple b) (la preuve de c) est analogue). Soit $\phi^{-1} \in \widehat{A}[[X]]$ la série formelle de valuation nulle réciproque de ϕ (qui existe bien car $\phi(0) = 0$ et $\phi'(0)$ est inversible). Posons $G(X,Y) = \phi(F_f(\phi^{-1}(X), \phi^{-1}(Y))$, il s'agit de montrer que $G = F_g$. Or $G(X,Y) \equiv X + Y$ mod. $\deg 2$, et on a aussi $G \in A[[X,Y]]$ car on a $G = \phi \circ F_f \circ \phi^{-1}$ d'où

$${}^\sigma G =^\sigma \phi \circ F_f \circ^{-\sigma} \phi = \phi \circ [u]_f \circ F_f \circ [u]_f^{-1} \circ \phi^{-1} = G$$

(rappelons que $[u]_f$ commute avec F_f). Il ne reste plus qu'à vérifier (via l'unicité dans la proposition 6.4) que $g \circ G = G \circ g$. Or

$$g \circ G = g \circ \phi \circ F_f \circ \phi^{-1} =^\sigma \phi \circ f \circ F_f \circ \phi^{-1} =$$

$${}^\sigma\phi \circ F_f \circ^{-\sigma} \phi \circ g =^\sigma G \circ g = G \circ g.$$

(en effet f commute avec F_f, et $G \in A[[X,Y]]$ donne ${}^\sigma G = G$).

□

6.3. Corps associés aux points de torsion

Dans toute la suite de ce chapitre, on fixe une clôture séparable $\overline{K}$ de K et on ne considère que des extensions de K incluses dans $\overline{K}$. Soient π une uniformisante de K et $f \in \mathcal{F}_\pi$; on a défini plus haut la loi de groupe (et même

de A-module) formel F_f, et on peut donc considérer le A-module $F_f(\mathcal{M}_{\overline{K}})$ et son sous-groupe de torsion E_f. Plus précisément si E_f^n est le noyau de l'endomorphisme $[\pi^n]_f$, on a $E_f = \bigcup_n E_f^n$. On pose aussi $K_\pi^n = K(E_f^n)$ et $K_\pi = \bigcup_n K(E_f^n)$. Chaque extension $K(E_f^n)$ est galoisienne sur K car les conjugués sur K de tout élément de E_f^n restent dans E_f^n (par définition de E_f^n comme sous-module de π^n-torsion de $F_f(\mathcal{M}_{\overline{K}})$). Le groupe de Galois $G_\pi := \mathrm{Gal}\,(K_\pi/K)$ est la limite projective des $G_{\pi,n} := \mathrm{Gal}\,(K(E_f^n)/K)$. On obtient alors un homomorphisme $G_\pi \to \mathtt{Aut}_A(E_f)$ obtenu en faisant agir G_π sur les points de torsion de $F_f(\mathcal{M}_{\overline{K}})$.

Theorème 6.10 *a) Le A-module E_f est isomorphe à K/A.*

b) L'homomorphisme $\Phi : G_\pi \to \mathtt{Aut}_A(E_f) \simeq A^*$ est un isomorphisme ; plus précisément il induit un isomorphisme Φ_n de $\mathrm{Gal}\,(K_\pi^n/K)$ sur U_K/U_K^n pour tout $n > 0$. En particulier l'extension K_π/K est abélienne.

c) Pour tout $n > 0$, l'uniformisante π est une norme de l'extension K_π^n/K.

d) Soit $L_\pi = K_{\mathrm{nr}}.K_\pi$ l'extension abélienne[32] *de K composée de K_{nr} et K_π. Soit $\theta = \omega_{L_\pi/K} : K^* \to \mathrm{Gal}\,(L_\pi/K)$ l'application de réciprocité. Alors K_π est le sous-corps fixe par $\theta(\pi)$ de L_π ; les corps K_{nr} et K_π sont linéairement disjoints (autrement dit $\mathrm{Gal}\,(L_\pi/K)$ est le produit direct de $\mathrm{Gal}\,(K_{\mathrm{nr}}/K)$ et G_π).*

Noter que la vérification du point d) (très important pour la suite) semble avoir été oubliée dans l'exposé VI de [3] (il n'est pas évident a priori que les définitions de K_π données p. 144 et p. 151 coïncident).

Démonstration : a) D'après la proposition 6.6, on peut prendre f comme on veut dans $\mathcal{F}_\pi$. Soit donc $f = \pi X + X^q$, où q est le cardinal du corps résiduel κ de $A = \mathcal{O}_K$. Comme on l'a vu, on a $[\pi]_f = f$, ce qui fait que E_f^n est l'ensemble des racines de la n-ième itérée f_n de f. On note que pour tout $\alpha \in \mathcal{M}_{\overline{K}}$, l'équation $f(x) = \alpha$ a alors une solution dans $\overline{K}$ (le polynôme f étant séparable), et ses solutions restent de valuation > 0, donc dans $\mathcal{M}_{\overline{K}}$. Ainsi l'$A$-module $F_f(\mathcal{M}_{\overline{K}})$ est divisible (la multiplication par π étant surjective), donc aussi son sous-module de torsion E_f. En particulier E_f est isomorphe à une somme directe de copies de K/A ; mais comme E_f^1 (qui est isomorphe au noyau de la multiplication par π dans K/A) a exactement q éléments (les racines de f), la seule possibilité est que E_f soit isomorphe à K/A.

32. Le composé de deux extensions abéliennes est une extension abélienne, traduction du fait que si H et H' sont deux sous-groupes distingués d'un groupe G avec G/H et G/H' abéliens, alors $G/(H \cap H')$ est abélien.

b) Soit $\tau \in G_\pi$. Il induit un automorphisme du A-module $E_f \simeq K/A$, donc un élément de A^*, d'où un homomorphisme $\Phi : G_\pi \to A^*$, qui est injectif par définition de K_π. Il reste à vérifier que Φ est surjectif. Notons que Φ induit une flèche injective $\Phi_n : \mathrm{Gal}\,(K_\pi^n/K) \to U_K/U_K^n$ (où $U_K^n := 1+\pi^n A$) car E_f^n correspond au sous-groupe de n-torsion $A/\pi^n A$ de K/A, sur lequel U_K^n agit trivialement. Soit $\alpha \in E_f^n \setminus E_f^{n-1}$ et posons $h = f_n/f_{n-1}$. Comme $f/X = X^{q-1} + \pi$, on a

$$h = f(f_{n-1})/f_{n-1} = (f_{n-1}(X))^{q-1} + \pi,$$

ce qui montre que h est de degré $q^n - q^{n-1}$ et est irréductible car c'est un polynôme d'Eisenstein. Comme α est racine de h, le degré $[K(\alpha) : K]$ est celui de h (puisque h est le polynôme minimal de α). On obtient donc que le cardinal de $\mathrm{Gal}\,(K_\pi^n/K)$ est au moins $q^n - q^{n-1}$, qui est le cardinal de U_K/U_K^n (en effet U_K/U_K^1 est isomorphe à κ^*, et les quotients U_K^i/U_K^{i+1} pour $i > 0$ sont isomorphes à κ). Ceci implique que Φ_n est un isomorphisme et $K(\alpha) = K_\pi^n$. En passant à la limite, on obtient que G_π est isomorphe à U_K via Φ.

c) Le polynôme h construit en b) est le polynôme minimal de α, et son terme constant est π. Ainsi π est la norme de $-\alpha$ pour l'extension K_π^n/K.

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

Lemme 6.11 *Soit K un corps local de groupe de Galois $\Gamma_K = \mathrm{Gal}\,(\overline{K}/K)$. Alors si K' est une extension finie non ramifiée (donc cyclique) de K, on a, pour tout x de K^*,*

$$\omega_{K'/K}(x) = F_K^{v(x)} \tag{4}$$

où $\omega_{K'/K}$ est l'application de réciprocité $K^* \to \mathrm{Gal}\,(K'/K)$ et F_K est le Frobenius de $\mathrm{Gal}\,(K'/K)$.

Ce lemme résulte très facilement du fait que pour tout caractère χ de $\mathrm{Gal}\,(K'/K)$, on a

$$\chi(\omega_{K'/K}(x)) = \mathrm{inv}_K(x \cup \chi)$$

(proposition 5.4) et de la définition de inv_K (cf. proposition 4.4).

On peut maintenant démontrer d). Comme $L_\pi \supset K_{\mathrm{nr}}$, on a une suite exacte

$$0 \to H \to \mathrm{Gal}\,(L_\pi/K) \to \mathrm{Gal}\,(K_{\mathrm{nr}}/K) \to 0$$

où $H := \mathrm{Gal}\,(L_\pi/K_{\mathrm{nr}})$ et $\mathrm{Gal}\,(K_{\mathrm{nr}}/K)$ est topologiquement engendré par le Frobenius σ. Comme $\theta(\pi) \in \mathrm{Gal}\,(L_\pi/K)$ est un relèvement de σ d'après le lemme 6.11 (en passant à la limite sur les extensions finies $K' \subset K_{\mathrm{nr}}$ de K), on obtient que $\mathrm{Gal}\,(L_\pi/K)$ est le produit direct de H et du sous-groupe

fermé I_π engendré par $\theta(\pi)$. Autrement dit on a $L_\pi = K_{\rm nr}K'$ avec $K_{\rm nr}$ et K' linéairement disjointes sur K, où K' est le corps fixe de L_π par $\theta(\pi)$.

Or, l'application de réciprocité $K^* \to \mathrm{Gal}\,(K_\pi^n/K)$ est triviale sur l'image de la norme $(K_\pi^n)^* \to K^*$, ce qui implique d'après c) que $\omega_{K_\pi/K}(\pi)$ est trivial. D'après la compatibilité entre $\omega_{L_\pi/K}$ et $\omega_{K_\pi/K}$, on obtient que la restriction de $\theta(\pi)$ à K_π est l'identité, d'où $K_\pi \subset K'$. Comme on a aussi $L_\pi = K_{\rm nr}.K_\pi$, la seule possibilité est $K_\pi = K'$ car le sous-groupe $H' := \mathrm{Gal}\,(L_\pi/K_\pi)$ contient I_π et vérifie $H \cap H' = \{1\}$, il est donc égal à I_π vu que $\mathrm{Gal}\,(L_\pi/K)$ est le produit direct de H et I_π.

□

6.4. Calcul de l'application de réciprocité

On a défini au paragraphe précédent une extension abélienne K_π de K associée à une uniformisante π de $A = \mathcal{O}_K$. Cette extension est linéairement disjointe de $K_{\rm nr}$ (en particulier toutes les extensions finies de K intermédiaires entre K et K_π sont totalement ramifiées). Elle a été construite via le groupe formel de Lubin-Tate associé à π, et admet aussi une caractérisation via l'image de π par l'application de réciprocité (théorème 6.10, d)). L'extension K_π dépend du choix de l'uniformisante π. Néanmoins, on a :

Proposition 6.12 *Soient π et ω deux uniformisantes de K. Soient $L_\pi = K_{\rm nr}.K_\pi$ et $L_\omega = K_{\rm nr}.K_\omega$. Alors $L_\pi = L_\omega$.*

Noter que ce résultat est plus facile si on suppose le théorème d'existence déjà connu (cf. [8], où le théorème d'existence est démontré directement en caractéristique zéro par la méthode classique des extensions de Kummer) ; l'approche que nous suivons ici est celle de l'exposé de Serre dans [3], qui a l'avantage de donner ensuite une preuve rapide du théorème d'existence en toute caractéristique à partir de la théorie de Lubin-Tate.

Démonstration : Soient $f \in \mathcal{F}_\pi$ et $g \in \mathcal{F}_\omega$. La proposition 6.9 dit que les A-modules formels F_f et F_g sont isomorphes sur $\widehat{K}_{\rm nr}$. En particulier les corps engendrés par $\widehat{K}_{\rm nr}$ et les points de torsion respectifs de $F_f(\mathcal{M}_{\overline{K}})$, $F_g(\mathcal{M}_{\overline{K}})$ sont les mêmes, i.e. $\widehat{K}_{\rm nr}.K_\pi = \widehat{K}_{\rm nr}.K_\omega$. A fortiori les complétions respectives de L_π et L_ω sont isomorphes. On conclut avec le lemme suivant (qu'on peut sans doute également démontrer en utilisant le fait que E est le corps des fractions d'un anneau local hensélien qui est réunion d'anneaux de valuations discrètes) :

Lemme 6.13 *Soit E une extension algébrique (finie ou infinie) d'un corps local, de complétion $\widehat{E}$. Soit $\alpha \in \widehat{E}$. Si α est algébrique séparable sur E, alors $\alpha \in E$.*

Démonstration : Soit $\overline{E}$ une clôture séparable de E. Soit E' l'adhérence de E dans $\overline{E}$, on peut alors voir α comme un élément de E' (par définition de la complétion). On observe que tout élément de $\mathrm{Gal}\,(\overline{E}/E)$ est une application continue [33] sur $\overline{E}$: en effet il suffit pour le voir de vérifier que tout automorphisme d'un corps local L est continu ; or la boule unité ouverte $\mathcal{M}_L$ d'un tel corps (i.e. les éléments x de valuation > 0) possède la caractérisation algébrique suivante : un élément x de K est dans $\mathcal{M}_L$ si et seulement si $1+x$ est une puissance n-ième dans L^* pour tout n premier à la caractéristique du corps résiduel de L ("si" est immédiat, et "seulement si" résulte du lemme de Hensel).

On en déduit que tout élément de $\mathrm{Gal}\,(\overline{E}/E)$ induit par continuité l'identité sur E', d'où $E' = E$ par la théorie de Galois, et donc $\alpha \in E$.

□

On peut maintenant démontrer le deuxième théorème principal de cette section, qui relie la construction de Lubin-Tate à l'application de réciprocité.

Theorème 6.14 *Soit K un corps local. Soient π une uniformisante de K et $f \in \mathcal{F}_\pi$. Soit $L = L_\pi = K_{\mathrm{nr}}.K_\pi$. On définit un homomorphisme $r_\pi : K^* \to \mathrm{Gal}\,(L/K)$ par les propriétés :*

a) $r_\pi(\pi)$ est l'identité sur K_π et coïncide avec le Frobenius σ sur K_{nr} ;

b) Pour tout u de U_K, $r_\pi(u)$ est l'identité sur K_{nr} et agit par $[u^{-1}]_f$ sur K_π.

Alors r_π est indépendant du choix de l'uniformisante π, et est égal à l'application de réciprocité $\omega_{L/K} : K^* \to \mathrm{Gal}\,(L/K)$.

Notons que r_π est bien défini car K^* est le produit direct des sous-groupes U_K et $\pi^{\mathbf{Z}}$, et les extensions K_{nr} et K_π sont linéairement disjointes. Rappelons aussi que $[u^{-1}]_f$ peut être vu comme un A-endomorphisme de E_f, donc induit un automorphisme de K_π.

Démonstration : On a déja vu (proposition 6.12) que l'extension $L = L_\pi$ ne dépend pas de π. Soit $\omega = u\pi$ une autre uniformisante. On va montrer que $r_\pi(\omega) = r_\omega(\omega)$, ce qui montrera que pour toute uniformisante ω, $r_\pi(\omega)$ est indépendant de π et donc que r_π est indépendant de π car K^* est engendré

33. Cette vérification semble également avoir été omise dans [3].

par les uniformisantes. On sait déjà que $r_\pi(\omega)$ et $r_\omega(\omega)$ coïncident sur $K_{\rm nr}$ car $r_\pi(\omega) = r_\pi(u).r_\pi(\pi)$; il reste à montrer que $r_\pi(\omega)$ est l'identité sur K_ω.

On a par définition $K_\omega = K(E_g)$ avec $g \in \mathcal{F}_\omega$. Soit $\phi \in \widehat{A}[[X]]$ comme dans la proposition 6.9. Tout élément λ de E_g s'écrit $\lambda = \phi(\mu)$ avec $\mu \in E_f$. Posons $s = r_\pi(\omega)$; il s'agit de vérifier que $s(\lambda) = \lambda$, ou encore ${}^s\phi(\mu) = \phi(\mu)$. On note que $s = r_\pi(\pi).r_\pi(u)$. Comme ϕ est à coefficients dans $\widehat{K}_{\rm nr}$, on a

$$ {}^s\phi =^\sigma \phi = \phi \circ [u]_f.$$

D'autre part

$$ {}^s(\phi(\mu)) =^s \phi({}^s\mu) =^s \phi([u^{-1}]_f(\mu))$$

car $\mu \in K_\pi$ d'où

$$ {}^s(\phi(\mu)) = \phi \circ [u]_f([u^{-1}]_f(\mu)) = \phi(\mu)$$

comme on voulait. Cela prouve que $r_\pi = r_\omega$.

On a vu que l'application de réciprocité $\theta = \omega_{L/K}$ vérifie (théorème 6.10, d)) pour toute uniformisante ω : $\theta(\omega)$ induit le Frobenius σ sur $K^{\rm nr}$ et l'identité sur K_ω. D'après ce qu'on vient de voir, $\theta(\omega) = r_\pi(\omega)$. Ceci étant valable pour toute uniformisante ω, on obtient bien que $r_\pi = r_\omega$ est la même application que θ.

□

Pour achever la description de l'extension abélienne maximale $K^{\rm ab}$ de K, il reste à prouver que $K^{\rm ab} = K_{\rm nr}.K_\pi$, ce qui est l'objet du paragraphe suivant.

6.5. Théorème d'existence

Définition 6.15 On dit qu'un sous-groupe M du groupe multiplicatif K^* est un *groupe de normes* s'il existe une extension abélienne finie E de K telle que $M = N_{E/K}E^*$.

On a en fait que tout sous-groupe de la forme $N_{F/K}F^*$, où F est une extension finie (pas forcément abélienne) de K est un sous-groupe de normes (cf. exercice 1 de ce chapitre).

Lemme 6.16 *Tout sous-groupe M de K^* qui contient un groupe de normes est un groupe de normes.*

Démonstration : Supposons que $M \supset N_{E/K}E^*$, où E est une extension finie abélienne de K. Alors l'image de M par l'application de réciprocité $\omega_{E/K} : K^* \to \mathrm{Gal}\,(E/K)$ est un sous-groupe de la forme $\mathrm{Gal}\,(E/F)$, où F est une extension intermédiaire. Comme $M \supset N_{E/K}E^* = \ker \omega_{E/K}$, M est exactement l'image réciproque de $\mathrm{Gal}\,(E/F)$ par $\omega_{E/K}$. Alors M est le noyau de l'application de réciprocité $\omega_{F/K} : K^* \to \mathrm{Gal}\,(F/K)$ via la compatibilité des applications de réciprocité. Il en résulte que $M = N_{F/K}F^*$ est encore un groupe de normes.

□

Le théorème d'existence donne à la fois une caractérisation des groupes de normes, et l'identification de l'extension abélienne maximale de K avec $K_{\mathrm{nr}}.K_\pi$.

Theorème 6.17 (Théorème d'existence) *Soient K un corps local et π une uniformisante de K. Soit $L = K_{\mathrm{nr}}.K_\pi$, où K_π est l'extension abélienne associée à π comme précédemment.*

a) Soit E une extension finie abélienne de K. Soit N la norme de E à K. Alors le sous-groupe NE^* de K^* est ouvert et d'indice fini.

b) Réciproquement tout sous-groupe ouvert d'indice fini de K^* est de la forme NE^*, où E est une extension finie de K incluse dans L.

c) L'extension L est l'extension abélienne maximale de K et l'extension finie abélienne E de K associée à un sous-groupe ouvert d'indice fini de K^* comme en b) est unique.

Démonstration : a) On sait que l'application de réciprocité induit un isomorphisme de K^*/NE^* sur $\mathrm{Gal}\,(E/K)$, ce qui montre que NE^* est d'indice fini dans K^*. D'autre part la norme $N : E^* \to K^*$ est continue (si on fixe une base du K-espace vectoriel E, c'est un polynôme en les coordonnées) et *propre* (l'image réciproque d'un compact est compact) : en effet la valuation dans K de $N(x)$ est $f.v_L(x)$ (où v_L est la valuation dans L et f le degré résiduel de L/K) via [11], chapitre II, corollaire 4 p. 39), ce qui montre que l'image réciproque de U_K par N est U_L (qui est compact). Or tout compact de K^* est contenu dans une union finie de translatés de U_K vu que U_K est un sous-groupe ouvert de K^*. Ceci implique en particulier que N est fermée, donc NE^* est d'indice fini et fermé dans K^*, i.e. ouvert d'indice fini.

b) Soit M un sous-groupe ouvert d'indice fini de K^*. Le fait que M soit ouvert implique l'existence d'un $n > 0$ tel que $M \supset U_K^n$, et le fait qu'il soit d'indice fini implique l'existence d'un $m > 0$ tel que $\pi^m \in M$. Ainsi M contient le sous-groupe $V_{n,m}$ engendré par U_K^n et π^m. Soit K_m l'extension non

ramifiée de K de degré m, posons $E = K_\pi^n.K_m$, c'est une sous-extension de L. Choisissons $f \in \mathcal{F}_\pi$. Soient $u \in U_K$ et $a \in \mathbf{Z}$. D'après le théorème 6.14, l'image $(u.\pi^a, E/K)$ de $u.\pi^a$ par l'application de réciprocité $\omega_{E/K}$ vaut $[u^{-1}]_f$ sur K_π^n et σ^a (où a est le Frobenius) sur K_m. Il en résulte que le noyau de $\omega_{E/K}$ est exactement $V_{n,m}$ (rappelons que le théorème 6.10 b) donne que $[u]_f$ agit trivialement sur K_π^n si et seulement si $u \in U_K^n$), d'où $V_{n,m} = N_{E/K}E^*$, d'où $V_{n,m} = NE^*$. On conclut avec le lemme 6.16.

c) Soit F une extension finie abélienne de K incluse dans $\overline{K}$. D'après a) et b), on peut écrire $N_{F/K}F^* = N_{E/K}E^*$, où E est une extension finie de K incluse dans L. Comme les adhérences des images respectives de $N_{F/K}F^*$, $N_{E/K}E^*$, par l'application de réciprocité $\omega_K : K^* \to \mathrm{Gal}\,(K^{\mathrm{ab}}/K)$ sont $\mathrm{Gal}\,(K^{\mathrm{ab}}/F)$ et $\mathrm{Gal}\,(K^{\mathrm{ab}}/E)$ (ceci via la compatibilité des applications de réciprocité et le fait que les noyaus respectifs de $\omega_{F/K}$, $\omega_{E/K}$ sont précisément $N_{F/K}F^*$, $N_{E/K}E^*$; cf preuve du lemme 6.16), on obtient $E = F$ par la théorie de Galois. En particulier $F \subset L$, et on a bien montré que L contient toutes les extensions finies abéliennes de K incluses dans $\overline{K}$, ou encore $L = K^{\mathrm{ab}}$ puisque L est une extension abélienne de K.

□

On retrouve au passage un énoncé qu'on avait obtenu dans le cas d'un corps p-adique via le théorème de dualité locale de Tate :

Corollaire 6.18 *L'application de réciprocité* $\omega_K : K^* \to \mathrm{Gal}\,(K^{\mathrm{ab}}/K)$ *induit un isomorphisme du complété de* K^* *(pour la topologie définie par les sous-groupes ouverts d'indice fini) sur* $\mathrm{Gal}\,(K^{\mathrm{ab}}/K)$. *Ce dernier groupe est isomorphe à* $\widehat{\mathbf{Z}} \times U_K$.

En effet le théorème d'existence dit que les sous-groupes ouverts d'indice fini de K^* sont précisément les groupes de normes, et on sait que l'application de réciprocité induit un isomorphisme de $\varprojlim_L K^*/NL^*$ sur $\mathrm{Gal}\,(K^{\mathrm{ab}}/K)$, la limite étant prise sur les extensions finies abéliennes de K.

Remarque : Si K est un corps p-adique, le sous-groupe K^{*^n} de K^* est ouvert pour tout $n > 0$ (ceci résulte du lemme de Hensel pour n premier à p ; on se ramène alors au cas où n est une puissance de p, auquel cas le résultat découle du fait que $U_K^m \subset K^{*^p}$ pour m assez grand via [11], chapitre XIV, prop. 9 p. 219). On en déduit avec le lemme 6.16 que tout sous-groupe d'indice fini de K^* est un groupe de normes (car il contient le groupe de normes K^{*^n} pour un certain $n > 0$), donc est fermé. Par contre, si K est un corps local de caractéristique p, le sous-groupe K^{*^p} n'est plus ouvert [34],

34. Il est encore fermé par compacité de U_K, vu que $K^* \simeq \mathbf{Z} \times U_K$.

sinon il contiendrait U_K^m pour m assez grand, ce qui n'est clairement pas le cas vu que l'équation $1+\pi^m = x^p$ implique $\pi^m = (x-1)^p$, ce qui n'est pas possible si la valuation m du terme de gauche n'est pas divisible par p. De fait, dans ce cas le groupe K^* contient des sous groupes d'indice fini qui ne sont pas fermés (cf. exercice 4 de ce chapitre) et on peut juste dire que tout sous-groupe d'indice fini **premier à** p de K^* est fermé.

Exemple : le cas de $\mathbf{Q}_p$. Pour $K = \mathbf{Q}_p$, on peut prendre $\pi = p$ et $f = (X+1)^p - 1 = pX + C_p^2 X^2 + ... + X^p$. Alors la loi de groupe formelle F_f est simplement $F_f(X,Y) = X + Y + XY$, et $F_f(\mathcal{M}_{\overline{K}})$ est donc isomorphe à $\overline{K}^*$ avec la multiplication usuelle. Ainsi $E_f = U_{p^\infty}$ est constitué des racines de l'unité d'ordre une puissance de p, et l'extension abélienne maximale $\mathbf{Q}_p^{\mathrm{ab}}$ de $\mathbf{Q}_p$ est obtenue comme $\mathbf{Q}_p^{\mathrm{ab}} = \mathbf{Q}_p^{\mathrm{nr}}.\mathbf{Q}_{p^\infty}$, où $\mathbf{Q}_p^\infty$ est le corps obtenu en ajoutant à $\mathbf{Q}_p$ les racines de l'unité d'ordre une puissance de p. Finalement, si $u \in \mathbf{Z}_p^*$, l'élément $[u] = [u]_f$ associé agit sur U_{p^∞} via l'identification de U_{p^∞} avec le groupe additif $\mathbf{Q}_p/\mathbf{Z}_p$; l'image $\theta(\alpha)$ d'un élément $\alpha = p^n u$ de $\mathbf{Q}_p^*$ par l'application de réciprocité $K^* \to \mathrm{Gal}\,(\mathbf{Q}_p^{\mathrm{ab}}/\mathbf{Q}_p)$ est donnée par : $\theta(\alpha)$ induit F^n sur $\mathbf{Q}_p^{\mathrm{nr}}$ (où F est le Frobenius) et $[u^{-1}]$ sur $\mathbf{Q}_p^\infty$. Noter enfin que $\mathbf{Q}_p^{\mathrm{ab}}$ est simplement le corps obtenu à partir de $\mathbf{Q}_p$ en ajoutant toutes les racines de l'unité.

6.6. Exercices

1. Soit K un corps local. Soit E une extension finie séparable de K. On note Γ_K, Γ_E les groupes de Galois absolus respectifs de K et E.

a) Montrer qu'on a un diagramme commutatif

$$\begin{array}{ccc} E^* & \xrightarrow{\omega_E} & \Gamma_E^{\mathrm{ab}} \\ {\scriptstyle N_{E/K}}\downarrow & & \downarrow{\scriptstyle i} \\ K^* & \xrightarrow{\omega_K} & \Gamma_K^{\mathrm{ab}} \end{array}$$

où i est induite par l'inclusion $\Gamma_E \to \Gamma_K$.

b) Soit L l'extension abélienne maximale de K incluse dans E. Montrer que $N_{E/K}E^* = N_{L/K}L^*$.

c) En déduire que l'indice $[K^* : NE^*]$ divise $[E:K]$, et lui est égal si et seulement si E est une extension abélienne de K.

d) Les résultats de b) et c) valent-ils encore si E n'est plus supposée séparable sur K ?

2. Soit K un corps local. Montrer que l'application de réciprocité $K^* \to \mathrm{Gal}\,(K^{\mathrm{ab}}/K)$ induit un isomorphisme de U_K sur le sous-groupe d'inertie $I_K = \mathrm{Gal}\,(K^{\mathrm{ab}}/K^{\mathrm{nr}})$ (utiliser le lemme 6.11 et la compacité de U_K pour la surjectivité, puis le théorème d'existence pour l'injectivité).

3. Soit K un corps local. Montrer que 1 est la seule *norme universelle* de K^*, i.e. le seul élément de K^* qui est dans $N_{L/K}L^*$ pour toute extension finie abélienne L de K.

4. Soit K un corps local de caractéristique $p > 0$. On rappelle que le groupe profini U_K^1 est alors isomorphe à $G = \mathbf{Z}_p^{\mathbf{N}}$.

a) Montrer que le sous-groupe $D = \mathbf{Z}_p^{(\mathbf{N})}$ (constitué des suites presque nulles d'éléments de $\mathbf{Z}_p$) est dense dans G.

b) Montrer qu'il existe un morphisme non nul de groupes abéliens $G \to \mathbf{Z}/p\mathbf{Z}$ qui s'annule sur D.

c) En déduire que K^* possède un sous-groupe d'indice p qui n'est pas fermé.

5. Soit K un corps local. Soient K_1 et K_2 deux extensions finies abéliennes de K. On note E le corps composé $E = K_1K_2$. Montrer que $N_{E/k}E^* = N_{K_1/K}K_1^* \cap N_{K_2/K}K_2^*$.

7. Rappels sur les corps globaux

Dans ce chapitre, nous allons rappeler rapidement les notions de base sur les corps globaux. Pour des démonstrations détaillées, on pourra se reporter par exemple à l'exposé II de [3].

7.1. Définitions, premières propriétés

Définition 7.1 Un *corps global* est soit une extension finie du corps $\mathbf{Q}$ des nombres rationnels (on parle alors de *corps de nombres*), soit une extension finie séparable de $\mathbf{F}_q(t)$ (on parle alors de *corps de fonctions* sur $\mathbf{F}_q$).

Une *place* d'un corps global k est une classe d'équivalence de valeurs absolues non triviales sur k (deux valeurs absolues sont équivalentes si l'une est une puissance de l'autre). Pour tout $\alpha \in k^*$, il n'y a qu'un nombre fini de places v pour lesquelles la valeur absolue correspondante $|\ \alpha\ |_v$ de α est > 1 (cf. [3], lemme p. 60). Plus précisément :

-Dans le cas d'un corps de nombres, il y a un nombre fini non nul de places v *archimédiennes*, qui peuvent être réelles ou complexes (le complété k_v de k pour une telle place est respectivement $\mathbf{R}$ ou $\mathbf{C}$). Les autres places (en nombre infini) sont dites *non archimédiennes* ou *finies* : elles correspondent bijectivement aux idéaux premiers $\wp$ de l'anneau des entiers $\mathcal{O}_k$ de k, fermeture intégrale de $\mathbf{Z}$ dans k (c'est un anneau de Dedekind). Le complété k_v en une place non archimédienne est alors un corps p-adique de corps résiduel $\mathcal{O}_k/\wp$, où p est l'unique nombre premier tel que $\wp$ divise p (i.e. tel que $\wp$ intervienne dans la décomposition en produits d'idéaux premiers de p dans $\mathcal{O}_k$), et les valeurs absolues associées à v sont de la forme $\mid x \mid = a^{-v_\wp(x)}$ avec $a \in \mathbf{R}_+^*$, où $v_\wp$ est la valuation sur k associée à l'idéal premier $\wp$.

-Dans le cas d'un corps de fonctions sur $\mathbf{F}_q$, toutes les places sont non archimédiennes, et les complétés k_v sont isomorphes à un corps local de caractéristique $p = \operatorname{Car} k$. Si X est une courbe projective et lisse sur $\mathbf{F}_q$ de corps de fonctions k, les places de k correspondent bijectivement aux points fermés de la courbe X (il n'y a pas d'analogue canonique de l'anneau des entiers d'un corps de nombres : par exemple pour $k = \mathbf{F}_q(t)$, il y a la place à l'infini en plus des places données par les idéaux premiers de $\mathbf{F}_q[t]$). Les valeurs absolues associées à un point fermé x sont de la forme $\mid f \mid = a^{-v_x(f)}$, où v_x est la valuation de l'anneau de valuation discrète $\mathcal{O}_{X,x}$.

Définition 7.2 La *valeur absolue normalisée* associée à une place v d'un corps global k est : dans le cas où v est réelle, la valeur absolue usuelle de $\mathbf{R}$; dans le cas où v est complexe, le **carré** du module usuel ; dans le cas non archimédien, la valeur absolue donnée par $\mid x \mid_v = q^{-v(x)}$, où q est le cardinal du corps résiduel du corps local k_v.

Une des raisons pour adopter ces conventions est ([3], p. 60) :

Theorème 7.3 (Formule du produit) *Soit k un corps global. Soit $\alpha \in k^*$. Alors on a*

$$\prod_v \mid \alpha \mid_v = 1$$

où v décrit l'ensemble des places de k et $\mid \alpha \mid_v$ est la valuation normalisée associée à v.

Noter que d'après ce qu'on a vu plus haut, on a bien $\mid \alpha \mid_v = 1$ pour presque toute place v de k.

Pour toute place v de k et toute extension finie séparable K de k, on a une décomposition

$$k_v \otimes_k K = K_{w_1} \oplus ... \oplus K_{w_r} \tag{5}$$

où w_1, ..., w_r sont les prolongements de v à K ([3], théorème p. 57). En particulier $r \leq [K : k]$ et pour v non archimédienne, chaque corps local K_{w_i} est une extension finie séparable du corps local k_v. On dira que v est *non ramifiée* dans l'extension K/k si toutes les extensions K_{w_i}/k_v sont non ramifiées ; c'est le cas de presque toutes les places de k ([3], exposé I, corollaire 1 p. 22).

On notera la différence avec la situation où k est un corps local (ou plus généralement un corps complet pour une valuation discrète) : ici le prolongement de v à l'extension K n'est en général pas unique. Par exemple si $k = \mathbf{Q}$, $K = \mathbf{Q}\sqrt{-1}$ et v correspond au nombre premier 5, alors $K \otimes_{\mathbf{Q}} \mathbf{Q}_5 = \mathbf{Q}_5 \oplus \mathbf{Q}_5$ (en effet -1 est un carré dans $\mathbf{Q}_5$ via le lemme de Hensel), donc il y a deux places de K au-dessus de v. Par contre pour $p = 2$ ou $p = 3$, $K \otimes_{\mathbf{Q}} \mathbf{Q}_p$ reste un corps et il n'y a qu'une place de K au-dessus de p (ramifiée pour $p = 2$, non ramifiée pour $p = 3$). On va voir aussi au prochain paragraphe qu'on peut dire nettement plus de choses si l'extension K/k est galoisienne.

7.2. Extensions galoisiennes d'un corps global

Soit k un corps global. Soit L une extension finie galoisienne de k de groupe $G = \mathrm{Gal}\,(L/k)$. Le groupe G opère sur les places de L suivant la formule $\mid a \mid_{\sigma w} := \mid \sigma^{-1} a \mid_w$ pour tout $a \in L$ et tout $\sigma \in G$, ce qui est cohérent avec l'action naturelle de G sur les idéaux premiers de $\mathcal{O}_k$ dans le cas d'un corps de nombres (resp. les points fermés de la courbe projective lisse associée à L dans le cas d'un corps de fonctions). En particulier on a bien $(\sigma\tau)w = \sigma(\tau w)$ pour tous σ, τ dans G. Tout $\sigma \in G$ induit aussi un k_v-isomorphisme entre les complétés L_w et $L_{\sigma w}$.

Définition 7.4 Soit w une place de L au-dessus d'une place v de k (cela signifie que w divise v). Le *groupe de décomposition* G_w de w (relativement à l'extension galoisienne L/k) est le sous-groupe de G constitué des σ tels que $\sigma w = w$.

On observe que $G_{\sigma w} = \sigma G_w \sigma^{-1}$, ce qui fait qu'à conjugaison près, le groupe de décomposition est déterminé par v (ce qui permet par exemple de le noter G_v si G est abélien). Pour une preuve de la proposition suivante, voir par exemple l'exposé VII de [3], prop. 1.2.

Proposition 7.5 *Soit w une place de L au-dessus d'une place v de k. L'extension L_w/k_v est galoisienne et l'injection $G_w \to \mathrm{Gal}\,(L_w/k_v)$ est un isomorphisme. De plus pour chaque place v de k, le groupe G opère transitivement sur les places de L au-dessus de v.*

On en déduit par exemple que la propriété que L_w soit une extension non ramifiée (resp. triviale) de k_v ne dépend pas de la place w de L divisant v (si L_w/k_v est triviale, on dira que v est *totalement décomposée* dans l'extension L/k). Plus généralement, l'indice de ramification e et le degré résiduel f de L_w sur k_v ne dépendent pas de v, ce qui fait qu'on a $[L : k] = n.ef$, où n est le nombre de places de L au-dessus de v. Le cas totalement décomposé correspond à $n = [L : k]$, et $e = f = 1$.

Dans le cas d'une place v finie et non ramifiée pour l'extension L/k, on obtient que pour toute place w de L au-dessus de v, le sous-groupe de décomposition G_w de G est isomorphe au groupe de Galois de l'extension résiduelle $\mathbf{F}_w/\mathbf{F}_v$, où $\mathbf{F}_w$, $\mathbf{F}_v$ désignent respectivement les corps résiduels de k_w, k_v. En particulier le Frobenius $x \mapsto x^{N_v}$ (où N_v est le cardinal du corps fini $\mathbf{F}_v$) admet un unique relèvement F_w à G_w, qu'on appelle *Frobenius* associé à w. A conjugaison près, il ne dépend que de v et on notera $F_{L/k}(v)$ sa classe de conjugaison dans G. Comme tout élément dans cette classe est d'ordre le degré résiduel f, on obtient que v se décompose dans L en $[G :< \sigma >]$ places, où $\sigma \in G$ est un représentant du Frobenius. En particulier elle est totalement décomposée si et seulement si $F_{L/k}(v)$ est trivial. Noter enfin que pour G abélien, le Frobenius en v est un élément bien déterminé de G pour toute place v de k non ramifiée dans L.

7.3. Idèles, théorème d'approximation forte

Définition 7.6 Soit k un corps global. Soit Ω_k l'ensemble de toutes les places de k. Un *idèle* de k est une famille $(x_v)_{v\in\Omega_k}$ dans $\prod_{v\in\Omega_k} k_v^*$, vérifiant $v(x_v) = 0$ (i.e. $\mid x_v \mid_v = 1$) pour presque toute place v de k (autrement dit : $x_v \in \mathcal{O}_v^*$ pour presque toute v, où $\mathcal{O}_v$ est l'anneau des entiers du corps local k_v).

Notons que comme il n'y a qu'un nombre fini de places archimédiennes (dans le cas d'un corps de nombres), on peut remplacer partout "presque toute place" par "presque toute place finie", ce qui justifie de parler de la valuation $v(x_v)$ ou de l'anneau $\mathcal{O}_v$ dans la définition ci-dessus. Les idèles forment un groupe multiplicatif, qu'on notera I_k (ou simplement I s'il n'y a pas d'ambigüité). Ce groupe est donc le produit restreint des k_v^* relativement aux $\mathcal{O}_v^*$. Équipé de sa topologie de produit restreint (pour laquelle une base de voisinages ouverts de 1 est constituée des sous-ensembles du type $\prod_{v\in S} U_v \times \prod_{v\notin S} \mathcal{O}_v^*$, où $S \subset \Omega_k$ est fini et U_v est un ouvert de k_v^* pour $v \in S$), c'est un groupe localement compact [35]. Ce groupe est de plus totalement discontinu dans le cas d'un corps de fonctions (dans le cas d'un corps de nombres, le

35. Par définition on demande qu'un groupe localement compact soit séparé.

groupe des *idèles finis*, constitué des idèles dont la composante aux places archimédiennes est 1, est totalement discontinu). Attention, la topologie sur I_k n'est pas celle induite par la topologie produit de $\prod_{v\in\Omega_k} k_v^*$.

Définition 7.7 Un *idèle principal* est un idèle de la forme $(x, x., ...x, ...)$ avec $x \in k^*$. Le *groupe des classes d'idèles* de k est le quotient $C_k := I_k/k^*$, où on a encore noté k^* le sous-groupe des idèles principaux de k.

C'est ce groupe C_k qui va jouer en théorie du corps de classes global un rôle comparable à celui du groupe multiplicatif en théorie du corps de classes local.

Le théorème suivant nous dit que si S est un ensemble fini de places (qu'on peut supposer contenir les places archimédiennes), on peut approcher une famille d'éléments (α_v) de $\prod_{v\in S} k_v$ par un élément $\beta \in k$ ("approximation faible"), en imposant en plus que β soit entier en dehors de S **et d'une place** v_0 **fixée au départ** (on ne peut pas espérer mieux, à cause de la formule du produit). Plus précisément, on a (pour une preuve, voir [3], exposé II, sections 14 et 15) :

Theorème 7.8 (Approximation forte) *Soit k un corps global et soit v_0 une place de k. On se donne un ensemble fini S de places de k avec $v_0 \notin S$, des éléments $\alpha_v \in k_v$ pour $v \in S$, et $\varepsilon > 0$. Alors il existe $\beta \in k$ avec $\mid \beta - \alpha \mid_v \leq \varepsilon$ pour $v \in S$ et $\mid \beta \mid_v \leq 1$ (i.e. $v(\beta) \geq 0$ si v est non archimédienne) pour toute $v \notin S \cup \{v_0\}$.*

La preuve du théorème d'approximation forte utilise notamment le lemme suivant (proche du théorème de Minkowski en géométrie des nombres), que l'on utilisera un peu plus loin (voir [3], lemme p. 66 pour une preuve) :

Lemme 7.9 *Soit k un corps global. Alors il existe une constante $C > 0$ (ne dépendant que de k) vérifiant : pour tout idèle $(\alpha_v) \in I_k$ vérifiant la condition $\prod_{v\in\Omega_k} \mid \alpha_v \mid_v \geq C$, il existe $\beta \in k^*$ tel que $\mid \beta \mid_v \leq \mid \alpha_v \mid_v$ pour toute place v de k.*

La proposition suivante implique en particulier que le groupe des classes d'idèles C_k est séparé (et donc localement compact comme quotient de I_k).

Proposition 7.10 *Le groupe k^* est discret (et donc fermé) dans I_k.*

Démonstration : Soit S un ensemble fini non vide de places de k, contenant l'ensemble des places archimédiennes si k est un corps de nombres. Soit U le voisinage ouvert de I_k défini par $(\alpha_v) \in U$ si et seulement si $\mid \alpha_v - 1 \mid_v < 1$ pour tout $v \in S$ et $\mid \alpha_v \mid = 1$ pour $v \notin S$. Alors si $x \in k^*$ n'est pas égal à 1, on a $\prod_{v \in \Omega_k} \mid x - 1 \mid_v = 1$ via la formule du produit, ce qui exclut $x \in U$ sinon on aurait $\mid x - 1 \mid_v < 1$ pour $v \in S$ et $\mid x - 1 \mid_v \leq \max(\mid x \mid_v, 1)$ pour $v \notin S$, ce qui impliquerait $\prod_{v \in \Omega_k} \mid x - 1 \mid_v < 1$. Ainsi 1 est un point isolé du sous-groupe image de k^* dans I_k, ce qui montre que ce sous-groupe est discret.

□

Considérons l'homomorphisme continu

$$\mid . \mid : I_k \to \mathbf{R}_+^*, \quad (\alpha_v) \mapsto \prod_{v \in \Omega_k} \mid \alpha_v \mid_v .$$

et notons I_k^0 son noyau. Via la formule du produit, on a $k^* \subset I_k^0$, d'où un homomorphisme induit $\mid . \mid : C_k \to \mathbf{R}_+^*$ de noyau $C_k^0 = I_k^0 / k^*$. Ce groupe va jouer en théorie du corps de classes un rôle analogue à celui de $\mathcal{O}_K^*$ quand K est un corps local (noter par exemple que si k est un corps de nombres, on a $C_k \simeq C_k^0 \times \mathbf{R}_+^*$, tout comme on a $K^* = \mathcal{O}_K^* \times \mathbf{Z}$ pour un corps local K). En particulier on a :

Theorème 7.11 *Le groupe C_k^0 est compact.*

Pour démontrer ce théorème, commençons par rappeler :

Définition 7.12 Une *adèle* de k est une famille $(\alpha_v)_{v \in \Omega_k}$ avec $\alpha_v \in k_v$ pour tout v et $\alpha_v \in \mathcal{O}_v$ pour presque tout v. On note $\mathbf{A}_k$ l'anneau des adèles, équipé de la topologie de produit restreint par rapport aux $\mathcal{O}_v$.

On voit immédiatement que le groupe multiplicatif I_k des idèles est simplement le groupe des inversibles de $\mathbf{A}_k$. Attention par contre à la topologie : la topologie de I_k n'est pas induite par celle de $\mathbf{A}_k$. Le théorème d'approximation forte est un énoncé de densité de k dans l'anneau des "adèles tronqués en v_0" (produit restreint des k_v pour $v \neq v_0$) **pour la $\mathbf{A_Q}$-topologie**.

La preuve du théorème 7.11 repose sur le lemme suivant, qui compare les deux topologies sur I_k^0.

Lemme 7.13 *Le sous-ensemble I_k^0 est un fermé de $\mathbf{A}_k$ pour la $\mathbf{A}_k$-topologie. De plus, les topologies induites par $\mathbf{A}_k$ et I_k sur I_k^0 coïncident.*

Démonstration : Soit $\alpha = (\alpha_v)$ une adèle qui n'est pas dans I_k^0. Il s'agit de trouver un voisinage ouvert W de α dans $\mathbf{A}_k$ qui ne rencontre pas I_k^0. Notons déjà que comme presque tous les $\mid \alpha_v \mid_v$ sont ≤ 1, le produit infini $C = \prod_{v\in\Omega_k} \mid \alpha \mid_v$ a un sens dans $\mathbf{R}_+$. Distinguons deux cas :

a) Supposons $C < 1$. Comme α est une adèle, seul un nombre fini de places v de S vérifient $\mid \alpha_v \mid_v \geq 1$. La propriété $C < 1$ implique alors qu'on peut trouver un ensemble fini S de places de k tel que S contient toutes les places v telles que $\mid \alpha_v \mid_v \geq 1$, et $\prod_{v\in S} \mid \alpha_v \mid_v < 1$. Il suffit alors de prendre W défini par $\mid \xi_v - \alpha_v \mid_v < \varepsilon$ pour $v \in S$ (pour ε assez petit) et $\mid \xi_v \mid_v \leq 1$ pour $v \notin S$.

b) Supposons $C > 1$. On peut encore trouver S fini tel que $\mid \alpha_v \mid_v \geq 1$ pour v non dans S. Quitte à agrandir S, on peut aussi supposer que pour toute v non dans S, la propriété $\mid \xi_v \mid_v < 1$ implique $\mid \xi_v \mid_v < (2C)^{-1}$ (observer que la plus grande valeur absolue < 1 dans k_v est q^{-1}, où q est le cardinal du corps résiduel de $\mathcal{O}_v$; or pour tout entier M il n'y a qu'un nombre fini de places dont le cardinal du corps résiduel est $\leq q$). Pour $\varepsilon > 0$ assez petit, la condition $\mid \xi_v - \alpha_v \mid_v < \varepsilon$ pour $v \in S$ implique alors $1 < \prod_{v\in S} \mid \xi_v \mid_v < 2C$. On peut alors prendre W défini par $\mid \xi_v - \alpha_v \mid_v < \varepsilon$ pour $v \in S$ et $\mid \xi_v \mid_v \leq 1$ pour $v \notin S$.

Finalement I_k^0 est bien fermé dans $\mathbf{A}_k$ et il reste à montrer que les topologies induites sur I_k^0 par $\mathbf{A}_k$ et I_k sont les mêmes. Soit donc $\alpha \in I_k^0$. Il est immédiat qu'un $\mathbf{A}_k$-voisinage de α contient un I_k-voisinage de α par définition des topologies de produit restreint vu que $\mathcal{O}_v^* \subset \mathcal{O}_v$ pour toute place finie v de k. Soit réciproquement H un I_k-voisinage de α, il contient un I_k-voisinage ouvert du type $\mid \xi_v - \alpha_v \mid_v < \varepsilon$ pour $v \in S$ et $\mid \xi_v \mid_v = 1$ pour $v \notin S$, où S contient les places archimédiennes et toutes les places v telles que $\mid \alpha_v \mid_v \neq 1$. On peut aussi supposer comme ci-dessus que pour v non dans S, la condition $\mid \xi_v \mid_v < 1$ implique $\mid \xi_v \mid_v < 1/2$. Maintenant la condition $\alpha \in I_k^0$ permet en plus de choisir ε tel que tout élément (ξ_v) de I_k^0 vérifiant $\mid \xi_v - \alpha_v \mid_v < \varepsilon$ pour $v \in S$ et $\mid \xi_v \mid_v \leq 1$ pour $v \notin S$ vérifie $\prod_{v\in\Omega_k} \mid \xi_v \mid_v < 2$, donc vérifie en fait $\mid \xi_v \mid_v = 1$ pour $v \notin S$. Cela montre que $H \cap I_k^0$ contient un $\mathbf{A}_k$-voisinage de α dans I_k^0 comme on voulait.

□

Preuve du théorème 7.11 : D'après le lemme 7.13, il suffit de trouver un $\mathbf{A}_k$-compact $W \subset \mathbf{A}_k$ tel que le passage au quotient $W \cap I_k^0 \to I_k^0/k^*$ soit surjectif. Choisissons un idèle $\alpha = (\alpha_v)$ tel que $\mid \alpha \mid := \prod_v \alpha_v$ soit $> C$, où C est la constante donnée par le lemme 7.9. On choisit alors pour W le compact (comme produit de compacts) de $\mathbf{A}_k$ défini par $\mid \xi_v \mid_v \leq \mid \alpha_v \mid_v$ pour toute place v. Le lemme 7.9 dit alors que si $\beta = (\beta_v)$ est dans I_k^0, alors on a un $\eta \in k^*$ tel que $\mid \eta \mid_v \leq \mid \beta_v^{-1}\alpha_v \mid_v$ pour toute place v, i.e. $\eta\beta \in W$ comme on voulait.

□

Le théorème 7.11 permet de retrouver deux résultats fondamentaux de la théorie des corps globaux : la finitude du groupe des classes d'idéaux, et le théorème des unités de Dirichlet (on peut aussi aller dans l'autre sens et démontrer le théorème 7.11 en partant de ces propriétés). Disons d'abord quelques mots sur le premier de ces résultats. Supposons d'abord que k est un corps de nombres dont on note Ω_f l'ensemble des places finies. Soit $\mathcal{I}_k$ le *groupe des idéaux* de k, i.e. le groupe abélien constitué des sommes formelles presque nulles $\sum_{v\in\Omega_f} n_v v$ avec $n_v \in \mathbf{Z}$ (c'est le groupe des diviseurs $\mathrm{Div}\,(\mathrm{Spec}\,\mathcal{O}_k)$). Le groupe $\mathcal{I}_k$ est isomorphe (via la décomposition unique d'un idéal en produit d'idéaux premiers dans un anneau de Dedekine) au groupe multiplicatif des idéaux fractionnaires de $\mathcal{O}_k$, les idéaux de $\mathcal{O}_k$ (au sens usuel) correspondant aux sommes formelles presque nulles $\sum_v n_v.v$ avec $n_v \geq 0$. L'application

$$I_k \to \mathcal{I}_k, \quad (\alpha_v) \mapsto \sum_{v\in\Omega_f} v(\alpha_v).v$$

est continue ($\mathcal{I}_k$ étant muni de la topologie discrète) par définition de la topologie de I_k. Par ailleurs l'image de k^* est par définition le groupe des idéaux principaux $\mathcal{P}_k$, et on obtient une surjection (parce qu'il y a au moins une place archimédienne dans k) continue $I_k^0/k^* \to \mathcal{I}_k/\mathcal{P}_k$. Comme un compact discret est fini, le théorème 7.11 donne alors

Theorème 7.14 *Soit k un corps de nombres. Le groupe des classes d'idéaux $\mathrm{Pic}\,(\mathrm{Spec}\,\mathcal{O}_k) = \mathcal{I}_k/\mathcal{P}_k$ est fini.*

La même preuve montre que dans le cas d'un corps de fonctions d'une courbe projective lisse X sur $\mathbf{F}_q$, le groupe $\mathcal{I}_k^0/\mathcal{P}_k = \mathrm{Pic}^{\,0} X$ est fini, où $\mathcal{I}_k^0$ est le groupe des diviseurs de degré zéro sur X. Ici le groupe des diviseurs $\mathcal{I}_k$ est composé des sommes formelles presque nulles $\sum_{v\in\Omega_k} n_v v$ avec $v \in \mathbf{Z}$, et le degré d'un tel diviseur est $\sum_v n_v d_v$, où d_v est le degré sur $\mathbf{F}_q$ du corps résiduel de X en v. En particulier si on enlève un point fermé v_0 de X, l'anneau de Dedekind des fonctions régulières de la courbe affine $Y = X \setminus \{v_0\}$ a un groupe des classes d'idéaux fini (en effet si on note d le degré du point fermé v_0, les diviseurs de Y dont le degré est dans $d\mathbf{Z}$ forment un sous-groupe d'indice fini de $\mathrm{Div}\,Y$, et ce sous-groupe est isomorphe à $\mathrm{Div}^{\,0} X$).

Soit maintenant k un corps global et soit S un ensemble fini de places de k, tel que S contienne l'ensemble Ω_∞ des places archimédiennes. Il est parfois utile de travailler avec le groupe $I_{k,S}$ des *S-idèles* de k, défini comme

$$I_{k,S} = \prod_{v\in S} k_v^* \times \prod_{v\notin S} \mathcal{O}_v^*.$$

Noter en particulier que I_k est la reunion des $I_{k,S}$ pour S fini.

Proposition 7.15 *Pour S fini assez grand, on a $I_k = I_{k,S}.k^*$ (et donc $C_k = I_{k,S}.k^*/k^*$).*

Démonstration : Soit $\mathcal{O}_k$ l'anneau des entiers de k si k est un corps de nombres (resp. l'anneau des fonctions régulières sur la courbe affine $X \setminus \{v_0\}$, où X est une courbe projective lisse sur $\mathbf{F}_q$ de corps des fonctions k, et v_0 est un point fermé de X, dans le cas où k est un corps de fonctions). La finitude du groupe des classes d'idéaux de k permet de choisir des places $v_1, ..., v_r$ de k correspondant à des idéaux premiers $\wp_1, ...\wp_r$ de $\mathcal{O}_k$ tels que les $\wp_i$ engendrent ce groupe des classes d'idéaux. Soit S un ensemble fini de places de k contenant les places archimédiennes dans le cas d'un corps de nombres (resp. v_0 dans le cas d'un corps de fonctions) et les places $v_1, ..., v_r$.

Soit alors $\alpha \in I_k$. Notons $\wp_v$ l'idéal premier associé à une place finie v de k. L'idéal fractionnaire $\prod_{v \notin \Omega_\infty} \wp_v^{v(\alpha_v)}$ (resp. $\prod_{v \neq v_0} \wp_v^{v(\alpha_v)}$ si k est un corps de fonctions) de $\mathcal{O}_k$ s'écrit $(x).I$, où I est un idéal fractionnaire du sous-groupe engendré par les $\wp_i$. Il en résulte que l'idèle $\alpha.x^{-1}$ a toutes ses composantes en dehors de S inversibles, donc est dans $I_{k,S}.k^*$.

□

Terminons ce chapitre en rappelant un lemme qui est une conséquence facile du théorème 7.11 (cf. [3], exposé II, paragraphe 18), et nous sera utile plus tard :

Lemme 7.16 *Soit S un ensemble fini non vide de places de k, contenant toutes les places archimédiennes. Soit $k_S = k^* \cap I_{k,S}$ le groupe des S-unités de k. Soit V le $\mathbf{R}$-espace vectoriel des applications de S dans $\mathbf{R}$. Soit $\lambda : k_S \to V$ l'homomorphisme défini par $\lambda(a) = f_a$, où $f_a(v) = \log \mid a \mid_v$ pour toute $v \in S$. Alors λ a un noyau fini, et son image est un réseau engendrant le $\mathbf{R}$-espace vectoriel V^0 des $f \in V$ telles que $\sum_{v \in S} f(v) = 0$.*

Démonstration : On observe d'abord que si c et C sont des constantes avec $0 < c < C$, alors l'ensemble des S-unités η telles que $c \leq \mid \eta \mid_v \leq C$ est fini comme intersection d'un compact de I_k avec le sous-groupe discret (cf. proposition 7.10) k^*. En particulier les éléments x vérifiant $\mid x \mid_v = 1$ pour toute place v sont en nombre fini et forment un groupe multiplicatif, c'est donc exactement le groupe des racines de l'unité. Ceci montre que $\ker \lambda$ est fini. Pour obtenir l'assertion sur son image, on observe qu'on peut définir λ par la formule analogue sur les S-idèles $I_{k,S}$, et l'image de $I_S^0 := I_{k,S} \cap I_k^0$ engendre [36] le $\mathbf{R}$-espace vectoriel des f vérifiant $\sum_{v \in S} f(w) = 0$, qui est de dimension $s-1$. Le groupe $\lambda(k_S)$ est discret (parce qu'il

36. et même lui est égal si k est un corps de nombres et S est l'ensemble des places archimédiennes.

n'y a qu'un nombre fini de $\eta \in k_S$ avec $1/2 \leq |\ \eta\ |_v \leq 2$ pour toute place v de S) et $\lambda(I_S^0)/\lambda(k_S)$ est compact via la compacité de I_S^0/k_S qui résulte du théorème 7.11 (noter que I_S^0/k_S est un sous-groupe ouvert, donc fermé de I_k^0/k^*). Finalement $\lambda(K_S)$ est un réseau qui engendre le $\mathbf{R}$-espace vectoriel V^0.

□

On obtient en corollaire le théorème des unités de Dirichlet :

Theorème 7.17 *Le groupe des S-unités k_S est isomorphe au produit direct d'un groupe fini (les racines de l'unité de k^*) et de $\mathbf{Z}^{s-1}$, où s est le cardinal de S.*

7.4. Exercices

1. Soit k un corps global. Trouver une suite d'éléments de I_k qui converge dans $\mathbf{A}_k$ mais pas dans I_k.

2. Soit $k = \mathbf{Q}(\sqrt{2})$.

a) Montrer que le sous-groupe H de I_k engendré par $\{\pm 1\}$ et $1+\sqrt{2}$ n'est pas compact.

b) En déduire que k^* n'est pas fermé dans le produit restreint des k_v^* pour v finie (relativement aux $\mathcal{O}_v^*$), c'est-à-dire dans les "idèles finis".

3. On rappelle que le corps $\mathbf{Q}$ n'admet pas d'extension finie, non ramifiée en tout nombre premier p, autre que $\mathbf{Q}$. Soit L une extension finie et abélienne de $\mathbf{Q}$. Le but de cet exercice est de démontrer que L est une extension cyclotomique (théorème de Kronecker-Weber) par voie purement locale.

a) Soit p un nombre premier ramifié dans $L/\mathbf{Q}$. Soit L_p le complété de L en un premier au-dessus de p. Montrer qu'il existe un entier $n_p > 0$ tel que $L_p \subset \mathbf{Q}(\mu_{n_p})$, où $\mathbf{Q}(\mu_{n_p})$ est l'extension obtenue en adjoignant à $\mathbf{Q}_p$ les racines n_p-ièmes de l'unité.

Dans toute la suite, on écrit $n_p = p^{e_p}.m_p$ avec m_p premier à p, et on pose $n = \prod_p p^{e_p}$, le produit étant sur tous les nombres premiers ramifiés dans $L/\mathbf{Q}$ (dont on note R l'ensemble). On pose aussi $M = L(\mu_n)$.

b) Montrer que si un nombre premier p est ramifié dans $M/\mathbf{Q}$, alors il est ramifié dans $L/\mathbf{Q}$.

c) Soit (pour $p \in R$) $I_p \subset \mathrm{Gal}\,(M_p/\mathbf{Q}_p)$ le sous-groupe d'inertie. Montrer que I_p est isomorphe à $\mathrm{Gal}\,(\mathbf{Q}_p(\mu_{p^{e_p}})/\mathbf{Q}_p)$.

d) Soit I le sous-groupe de $\mathrm{Gal}\,(M/\mathbf{Q})$ engendré par les I_p, Montrer que le corps fixe M^I est $\mathbf{Q}$.

e) Montrer que le cardinal de I est au plus $[\mathbf{Q}(\mu_n) : \mathbf{Q}]$ et en déduire que $L \subset \mathbf{Q}(\mu_n)$.

8. Cohomologie des idèles : l'axiome du corps de classes

Dans ce chapitre, nous commençons à investiguer les propriétés cohomologiques des groupes I_k et C_k définis au chapitre précédent pour un corps global k. Le but est de démontrer un analogue global de la proposition 4.3, où le groupe des classes d'idèles va remplacer le groupe multiplicatif d'un corps local. C'est ce résultat qui (comme en théorie du corps de classes local) est la première étape dans la détermination du groupe de Brauer d'un corps global.

8.1. Cohomologie du groupe des idèles

Dans tout ce paragraphe on fixe un corps global k et une clôture séparable $\bar{k}$ de k. On considérera des extensions finies séparables K de k, qui seront toujours implicitement supposées incluses dans $\bar{k}$. Pour toute place v de k, on fixe un k-plongement $i_v : \bar{k} \to \bar{k} \otimes_k k_v$, et une place $\bar{v}$ de $\bar{k}$ au-dessus de v. Ceci permet pour tout extension algébrique séparable K de k d'avoir une place $v^\bullet$ de K privilégiée au-dessus de v ; on notera pour simplifier $K_v := i_v(K)k_v$ le corps Kk_v, qui est de plus la complétion de K en $v^\bullet$ si $[K : k]$ est fini. On notera de même $U_{K,v}$ le groupe des unités de K_v^*, et $G_v(K/k)$ (ou même G_v s'il n'y a pas d'ambigüité) le groupe de décomposition de $v^\bullet$ dans $G = \mathrm{Gal}\,(K/k)$ si K est une extension galoisienne de k.

Soit K une extension finie galoisienne de k de groupe G. On peut écrire le groupe des idèles de K comme le produit restreint des $I_K(v)$ pour v place de k par rapports aux $U_K(v)$, où on a posé

$$I_K(v) := \prod_{w|v} K_w^*; \quad U_K(v) := \prod_{w|v} U_{K,w}.$$

($U_{K,w}$ est le groupe multiplicatif de l'anneau des entiers de K_w pour w place finie de K). Chacun des $I_K(v)$ et des $U_K(v)$ est un G-module via le k_v-isomorphismes $K_w \simeq K_{\sigma w}$ induit par chaque $\sigma \in G$.

La proposition 7.5 donne facilement que $I_K(v)$ (resp. $U_K(v)$) s'identifie à l'induit $I_G^{G_v}(K_v^*)$ de K_v^* (resp. à $I_G^{G_v}(U_{K,v})$).

Proposition 8.1 *Avec les notations ci-dessus :*

a) On a $I_k = H^0(G, I_K)$.

b) Pour tout $i \in \mathbf{Z}$, *on a*

$$\widehat{H}^i(G, I_K) = \bigoplus_{v \in \Omega_k} \widehat{H}^i(G_v, K_v^*).$$

Démonstration : a) On a une injection naturelle de I_k dans I_K via la décomposition (5). Soit $\alpha \in I_k$. Pour tout $\sigma \in G$ et toute place w de K au-dessus d'une place v de k, la composante $(\sigma\alpha)_{\sigma w}$ de $\sigma\alpha$ en σw est $\sigma\alpha_w = \alpha_w = \alpha_{\sigma w}$ donc $\sigma\alpha = \alpha$. Réciproquement si $\alpha = (\alpha_w)$ est dans $H^0(G, I_K)$, alors

$$(\sigma\alpha)_{\sigma w} = \sigma\alpha_w = \alpha_{\sigma w}$$

pour tout $\sigma \in G$. Pour $\sigma \in G_w$, cela donne déjà $\alpha_w \in k_v^*$. Le fait que G opère transitivement sur les places w au-dessus de v (proposition 7.5) donne alors que les α_w pour $w \mid v$ proviennent d'un même $\alpha_v \in k_v^*$ via les plongements $k_v^* \to K_w^*$, d'où $\alpha \in I_k$.

b) Le lemme de Shapiro donne

$$\widehat{H}^i(G, I_K(v)) = \widehat{H}^i(G_v, K_v^*)$$

et par ailleurs si v est non ramifiée dans l'extension K/k, on a

$$\widehat{H}^i(G, U_K(v)) = \widehat{H}^i(G_v, U_{K,v}) = 0$$

car $U_{K,v}$ est un G_v-module cohomologiquement trivial par la proposition 4.1. Considérons les ensembles finis S de places de k, contenant les places ramifiées dans K/k et les places archimédiennes. Posons

$$I_{K,S} = \prod_{v \in S} I_K(v) \times \prod_{v \notin S} U_K(v).$$

Alors I_K est la limite inductive des $I_{K,S}$. On en déduit

$$\widehat{H}^i(G, I_K) = \varinjlim_S \widehat{H}^i(G, I_{K,S}) = \varinjlim_S (\widehat{H}^i(G, \prod_{v \in S} I_K(v)) \times \widehat{H}^i(G, \prod_{v \notin S} U_K(v))) =$$

$$\varinjlim_S ((\prod_{v \in S} \widehat{H}^i(G, I_K(v)) \times \prod_{v \notin S} \widehat{H}^i(G, U_K(v))) =$$

$$\varinjlim_S \prod_{v \in S} \widehat{H}^i(G_v, K_v^*) = \bigoplus_{v \in \Omega_k} \widehat{H}^i(G_v, K_v^*).$$

□

Corollaire 8.2 *On a* $H^1(G, I_K) = H^3(G, I_K) = 0$.

Démonstration : D'après la proposition précédente, il s'agit de voir que pour toute place v de k, on a $H^1(G_v, K_v^*) = H^3(G_v, K_v^*) = 0$. La première assertion résulte du théorème de Hilbert 90. La deuxième en résulte pour v réelle via le théorème 1.32. Pour v finie, le théorème de Tate-Nakayama (théorème 2.12) donne un isomorphisme de $H^1(G_v, \mathbf{Z}) = 0$ sur $H^3(G_v, K_v^*)$. □

On aimerait "passer à la limite" dans les assertions précédentes. Notons $I := \varinjlim_K I_K$ le *groupe des idèles de* $\bar{k}$, la limite étant prise sur les extensions finies séparables K de k (attention, ce n'est pas le produit restreint des $(\bar{k})_v^*$). On appelle aussi $C := I/\bar{k}^*$ le *groupe des classes d'idèles de* $\bar{k}$, qui est la limite inductive des C_K. La proposition 8.1 a) et le théorème de Hilbert 90 donnent :

Proposition 8.3 *On a* $H^0(k, I) = I_k$ *et* $H^0(k, C) = C_k$.

En passant à la limite dans la proposition 8.1 b), on obtient

$$H^i(k, I) = \bigoplus_{v \in \Omega_k} H^i(G_v(\bar{k}/k), (\bar{k})_v^*)$$

pour tout $i \geq 1$. On aimerait dans cet énoncé remplacer $(\bar{k})_v^*$ par $\bar{k}_v^*$ (où $\bar{k}_v$ est la clôture séparable de k_v). On a effectivement bien que $(\bar{k})_v = \bar{k}k_v$ est une clôture séparable de k_v, mais cet énoncé est non trivial ; il utilise le

Lemme 8.4 (Krasner) *Soit* F *un corps complet pour une valeur absolue ultramétrique (pas forcément associée à une valuation discrète), de clôture séparable* $\overline{F}$. *Soit* $\alpha \in \overline{F}$, *on note* $\alpha_1 = \alpha, ..., \alpha_n$ *ses conjugués sur* F. *Soit* $\beta \in \overline{F}$ *vérifiant*

$$| \alpha - \beta | < | \alpha - \alpha_i |$$

pour $i = 2, ..., n$, *où* $| \, . \, |$ *est l'unique prolongement de la valeur absolue de* F *à* $\overline{F}$. *Alors on a l'inclusion de corps* $F(\alpha) \subset F(\beta)$.

Démonstration : Soit L la clôture galoisienne sur $F(\beta)$ de l'extension de corps $F(\alpha, \beta)/F(\beta)$. Soit $\sigma \in G := \mathrm{Gal}\,(L/F(\beta))$. Alors $\sigma(\beta - \alpha) = \beta - \sigma(\alpha)$. Comme σ conserve $| \, . \, |$ (par unicité du prolongement de la valeur absolue dans le cas complet), on obtient

$$| \beta - \sigma(\alpha) | = | \beta - \alpha | < | \alpha_i - \alpha |$$

pour $i = 2, ..., n$. On en déduit

$$| \alpha - \sigma(\alpha) | < | \alpha - \alpha_i |$$

pour $i = 2, ..., n$ car $|\ .\ |$ est ultramétrique. Finalement $\sigma(\alpha) = \alpha$, i.e. $\alpha \in F(\beta)$ comme on voulait.

□

On en déduit le résultat annoncé :

Proposition 8.5 *Soit k un corps global. Soit v une place de k. Alors $(\bar{k})_v$ (avec les conventions expliquées au début du paragraphe) s'identifie à la clôture séparable $\overline{k_v}$ de la complétion k_v de k en v.*

Démonstration : On a une inclusion naturelle $(\bar{k})_v \to \overline{k_v}$. On peut supposer que v est une place finie (le cas archimédien est trivial). Soit $\alpha \in \overline{k_v}$, de polynôme minimal $f \in k_v[X]$. Comme k est dense dans k_v, on peut trouver un polynôme séparable $g \in k[X]$ très proche de f, ce qui implique que $|\ g(\alpha)\ |$ peut être rendu aussi petit qu'on veut. Écrivons $g(X) = \prod(X - \beta_j)$ avec $\beta_j \in \bar{k} \subset (\bar{k})_v$. Alors g possède une racine β qui peut être rendue aussi proche qu'on veut de α, donc en particulier qui vérifie $|\ \beta - \alpha\ | < |\ \alpha_i - \alpha\ |$ pour tous les conjugués $\alpha_i \in \overline{k_v}$ de α autre que α. Le lemme de Krasner donne alors $\alpha \in k_v(\beta) = k(\beta)_v \subset (\bar{k})_v$.

□

Corollaire 8.6 *Pour tout $i \geq 1$, on a $H^i(k, I) = \bigoplus_{v \in \Omega_k} H^i(k_v, \bar{k}_v^*)$, où $\bar{k}_v$ est la clôture séparable de k_v.*

Noter que d'après ce qu'on vient de voir, la notation $\bar{k}_v$ n'est pas ambigüe.

8.2. La deuxième inégalité

Le but de ce paragraphe est de montrer :

Theorème 8.7 *Soit k un corps global. Soit K une extension galoisienne de k de groupe de Galois G cyclique d'ordre n. Soit $h(G, C_K)$ le quotient d'Herbrand du G-module C_K, où $C_K = I_K/K^*$ est le groupe des classes d'idèles de K. Alors $h(G, C_K) = n$.*

On en déduit :

Corollaire 8.8 ("Seconde inégalité") *Sous les hypothèses du théorème précédent, le cardinal du groupe $\widehat{H}^0(G, C_K) = I_k/k^* N_{K/k} I_K$ est $\geq n$.*

Démonstration : En appliquant Hilbert 90 et la proposition 8.1 a), on a $H^0(G, C_K) = C_k$, d'où $\widehat{H}^0(G, C_K) = C_k/N_{K/k}C_K = I_k/k^*N_{K/k}I_K$.

□

Le but de ce chapitre est de démontrer qu'on a en fait $\#\widehat{H}^0(G, C_K) = n$ dans le corollaire ci-dessus. Pour cela, on aura besoin de la *première inégalité* qui, bien que pouvant se démontrer en utilisant le corollaire 8.8 (voir les paragraphes suivants), a historiquement été prouvée plus tôt par voie analytique (cf. [3], exposé VIII), d'où la terminologie que nous adoptons ici (certains auteurs adoptent la convention inverse, c'est le cas par exemple dans [3]). Le corollaire 8.8 s'utilise surtout pour démontrer que $K = k$ quand des informations arithmétiques permettent de vérifier que $I_k = k^*N_{K/k}I_K$.

La preuve du théorème 8.7 s'appuie sur le lemme suivant :

Lemme 8.9 *Soit G un groupe fini.*

a) Soient M et M' deux modules sur l'anneau $\mathbf{Q}[G]$, de dimension finie sur $\mathbf{Q}$, et tels que les $\mathbf{R}[G]$-modules $M_{\mathbf{R}} := M \otimes_{\mathbf{Q}} \mathbf{R}$ et $M'_{\mathbf{R}}$ soient isomorphes. Alors les $\mathbf{Q}[G]$-modules M et M' sont isomorphes.

b) Soit E un $\mathbf{R}$-espace vectoriel de dimension finie équipé d'une action de G. Soient L et L' deux réseaux de E, stables pour l'action de G, et engendrant le $\mathbf{R}$-espace vectoriel E. Alors si l'un des quotients d'Herbrand $h(L)$, $h(L')$ est défini, l'autre l'est aussi et on a $h(L) = h(L')$.

Démonstration : a) Tout $\mathbf{Q}[G]$-homomorphisme $\varphi : M \to M'$ induit un $\mathbf{R}[G]$-homomorphisme $\varphi \otimes 1 : M_{\mathbf{R}} \to M'_{\mathbf{R}}$ et l'application $\varphi \to \varphi \otimes 1$ induit un isomorphisme de $\mathbf{R}$-espaces vectoriels :

$$(\mathrm{Hom}_{\mathbf{Q}[G]}(M, M')) \otimes_{\mathbf{Q}} \mathbf{R} \to \mathrm{Hom}_{\mathbf{R}[G]}(M_{\mathbf{R}}, M'_{\mathbf{R}}).$$

Fixons des bases respectives des $\mathbf{Q}$-espaces vectoriels M et M', qui ont la même dimension. Le déterminant d'un élément de $\mathrm{Hom}_{\mathbf{Q}[G]}(M, M')$ ou de $\mathrm{Hom}_{\mathbf{R}[G]}(M_{\mathbf{R}}, M'_{\mathbf{R}})$ dans ces bases est alors bien défini. Soit alors (ξ_i) une base du $\mathbf{Q}$-espace vectoriel $\mathrm{Hom}_{\mathbf{Q}[G]}(M, M')$, la formule ci-dessus montre que c'est encore une base du $\mathbf{R}$-espace vectoriel $\mathrm{Hom}_{\mathbf{R}[G]}(M_{\mathbf{R}}, M'_{\mathbf{R}})$. L'hypothèse que $M_{\mathbf{R}}$ et $M'_{\mathbf{R}}$ sont isomorphes implique alors que le polynôme

$$F(t_1, ..., t_n) := \det(\sum_i t_i \xi_i) \in \mathbf{Q}[t_1, ..., t_m]$$

ne s'annule pas sur $\mathbf{R}^m$ tout entier, donc pas non plus sur $\mathbf{Q}^m$ vu que $\mathbf{Q}$ est infini. On a donc bien un $\mathbf{Q}[G]$-isomorphisme de M sur M'.

b) Posons $M = L \otimes \mathbf{Q}$ et $M' = L' \otimes \mathbf{Q}$. Alors $M_{\mathbf{R}}$ et $M'_{\mathbf{R}}$ sont tous deux $\mathbf{R}[G]$-isomorphes à E. Par a), il existe un $\mathbf{Q}[G]$-isomorphisme $\varphi : M \to M'$. Alors φ induit un homomorphisme injectif $\varphi : L \to (1/N)L'$ pour un certain entier $N > 0$. Ceci implique que $f := N\varphi$ est un homomorphisme injectif de L dans L'. Comme L et L' sont des réseaux de même rang, le conoyau de f est fini et on conclut en appliquant le théorème 1.34, c).

□

Preuve du théorème 8.7 : D'après la proposition 7.15, on peut trouver un ensemble fini non vide S de places de k (contenant les places archimédiennes et les places ramifiées dans K/k) tel que $I_K = K^* I_{K,S}$, où

$$I_{K,S} = \prod_{v \in S} I_K(v) \times \prod_{v \notin S} U_K(v) = \prod_{v \in S} (\prod_{w|v} K_w^*) \times \prod_{v \notin S} (\prod_{w|v} U_{K,w}^*).$$

Soit T l'ensemble (fini) des places de K qui sont au-dessus d'une place de S. On a alors

$$C_K = I_K / K^* = I_{K,S} / K_T$$

où $K_T := K^* \cap I_{K,S}$ est le groupe des T-unités de K. D'après le théorème 1.34, on a alors, en abrégeant $h(G, ...)$ en $h(...)$,

$$h(C_K) = h(I_{K,S}) / h(K_T)$$

dès que le membre de droite est défini (l'intérêt d'introduire S et T est précisément que cela va permettre à cette condition d'être satisfaite, alors que $h(K^*)$ n'est pas défini vu que $\widehat{H}^0(G, K^*) = K^*/NL^*$ est infini).

On calcule d'abord $h(I_{K,S})$ de façon purement "locale". Pour $v \notin S$, la place v est non ramifiée dans K/k, ce qui implique comme on l'a déjà vu (conséquence du lemme de Shapiro et de la proposition 4.1) que le G-module $U_K(v)$ est cohomologiquement trivial. Soit maintenant $v \in S$, notons $n_v := [K_v : k_v]$ le degré local de K/k en v. Le lemme de Shapiro implique que pour v dans S, on a :

$$h(I_K(v)) = h(G_v, K_v^*) = n_v$$

par l'axiome du corps de classes local (proposition 4.3) d'où finalement

$$h(I_{K,S}) = \prod_{v \in S} n_v.$$

On passe maintenant au calcul de $h(K_T)$, qui est la partie "globale" de la preuve. Il s'agit de montrer que $n.h(K_T) = \prod_{v \in S} n_v$. Pour cela on va

utiliser le lemme 8.9. Soit V l'espace vectoriel des applications de T dans $\mathbf{R}$, qui est donc isomorphe à $\mathbf{R}^t$ avec $t = \#T$. Le groupe G opère sur V par la formule $(\sigma f)(w) = f(\sigma^{-1}w)$ pour tous $f \in V$, $\sigma \in G$, $w \in T$. Soit N le réseau constitué des $f \in V$ dont l'image est incluse dans $\mathbf{Z}$. Il est clair que N engendre le $\mathbf{R}$-espace vectoriel V et est stable pour l'action de G. Le G-module N est isomorphe à $\prod_{v\in S}(\prod_{w|v}\mathbf{Z}_w)$, avec $\mathbf{Z}_w = \mathbf{Z}$ et l'action de G est par permutation des $\mathbf{Z}_w$ pour $w \mid v$ et v fixée. Le lemme de Shapiro donne alors, pour tout $q \in \mathbf{Z}$:

$$\widehat{H}^q(G, N) = \prod_{v\in S} \widehat{H}^q(G_v, \mathbf{Z})$$

ce qui implique immédiatement

$$h(N) = \prod_{v\in S} n_v.$$

Pour $a \in K_T$, notons $f_a : T \to \mathbf{R}$ l'application définie par $f_a(w) = \log \mid a \mid_w$ et appliquons le lemme 7.16. Il nous dit que l'application

$$\lambda : K_T \to V, \quad a \mapsto f_a$$

a un noyau fini, et que l'image M^0 de f est un réseau M^0 qui engendre le $\mathbf{R}$-espace vectoriel $V^0 \subset V$ constitué des f telles que $\sum_{w\in T} f(w) = 0$. On a $h(K_T) = h(M^0)$ par le théorème 1.34, c). Soit $g \in V$ défini par $g(w) = 1$ pour tout $w \in T$, posons $M = M^0 + \mathbf{Z}g$. Alors le réseau M engendre le $\mathbf{R}$-espace vectoriel $V = V^0 + \mathbf{R}g$; comme M^0 et $\mathbf{Z}.g$ sont tous deux stables par G, on peut écrire

$$h(M) = h(M^0).h(\mathbf{Z}) = nh(M^0) = nh(K_T).$$

Comme M et N engendrent le même $\mathbf{R}$-espace vectoriel, le lemme 8.9 implique que $h(N) = h(M)$. Finalement $n.h(K_T) = h(N)$, ou encore

$$n.h(K_T) = \prod_{v\in S} n_v$$

comme on voulait.

□

On en déduit :

Proposition 8.10 *Soit K une extension finie abélienne d'un corps global k. On suppose qu'il existe un sous-groupe D de I_k vérifiant : $D \subset N_{K/k}I_K$ et k^*D est dense dans I_k. Alors $K = k$.*

Démonstration : On se ramène tout de suite au cas où K/k est une extension cyclique en raisonnant par récurrence sur $[K : k]$ et en observant que si $K \supset F \supset k$ avec F/k cyclique, on a $D \subset N_{K/k}I_K \subset N_{F/k}I_F$ par transitivité des normes. Notons le

Lemme 8.11 *Un idèle $\alpha = (\alpha_v) \in I_k$ est dans $N_{K/k}$ si et seulement si pour toute place v de k, sa composante locale $\alpha_v \in k_v^*$ est une norme pour l'extension K_v/k_v (rappelons que K_v désigne le complété de K pour une place w au-dessus de v).*

Ce lemme résulte immédiatement de la proposition 8.1 b) appliquée à $i = 0$.

Maintenant, le théorème 6.17, a) dit que chaque $N_{K_v/k_v}K_v^*$ est un sous-groupe ouvert de K_v^* ; de plus $N_{K_v/k_v}K_v^*$ contient $U_v := \mathcal{O}_v^*$ pour presque toute place v puisque v non ramifiée implique $\widehat{H}^0(G_v, U_{K,v}) = 0$ avec $G_v = \mathrm{Gal}\,(K_v/k_v)$ (proposition 4.1). On en déduit, avec le lemme 8.11, que $N_{K/k}I_K$ est un sous-groupe ouvert de I_k, donc aussi $k^*N_{K/k}I_K$ (réunion d'ouverts). Ainsi $k^*N_{K/k}I_K$ est un sous-groupe fermé (car ouvert) et dense (car il contient k^*D) de I_k, d'où $k^*N_{K/k}I_K = I_k$. Le corollaire 8.8 donne alors $[K : k] = 1$, i.e. $K = k$.

□

Proposition 8.12 *Soit S un sous-ensemble fini de places de k, contenant les places archimédiennes. Soit K une extension finie abélienne de k, non ramifiée en dehors de S. Alors le groupe de Galois $G = \mathrm{Gal}\,(K/k)$ est engendré par les Frobenius $F_{K/k}(v)$ pour $v \notin S$.*

Démonstration : Notons déjà que comme ici G est abélien, le Frobenius $F_v := F_{K/k}(v)$ est bien défini comme élément de G (et pas seulement à conjugaison près). Soit G' le sous-groupe de G engendré par les F_v pour $v \notin S$ et soit E son corps fixe. Alors l'image de F_v dans $\mathrm{Gal}\,(E/k) = G/G'$ est triviale pour $v \notin S$, ce qui donne $E_v = k_v$, et donc tout élément de k_v est une norme de E_v/k_v pour $v \notin S$. Notons alors D le sous-groupe de I_k constitué des idèles (α_v) tels que $\alpha_v = 1$ pour tout $v \in S$. Alors d'après le lemme 8.11 et ce qu'on vient de voir, on a $D \subset N_{E/k}I_E$. D'autre part le théorème d'approximation forte[37] donne que k^*D est dense dans I_k. La proposition 8.10 donne alors $E = k$, ou encore $G' = G$.

□

37. Ou même sa forme "faible", c'est-à-dire sans la condition en dehors de S.

Corollaire 8.13 *Soit K une extension abélienne non triviale de k. Alors il y a une infinité de places v de k qui ne sont pas totalement décomposées dans K. Si de plus K/k est cyclique de degré ℓ^m avec ℓ premier, il existe une infinité de places de k qui sont inertes dans K/k (c'est-à-dire non ramifiées et telles que le groupe de décomposition associé soit $G := \mathrm{Gal}\,(K/k)$ tout entier).*

Notons qu'une place inerte v correspond à un Frobenius $F_{K/k}(v)$ qui engendre $\mathrm{Gal}\,(K/k)$, ou encore à une place non ramifiée telle qu'il existe une seule place w de K au-dessus de v.

Démonstration : La première assertion vient de la proposition 8.12 jointe au fait que les places v totalement décomposées dans K correspondent à $F_{K/k}(v) \neq 1$. La deuxième assertion s'obtient en appliquant la première à l'extension intermédiaire E/k de degré ℓ, qui correspond à l'unique sous-groupe d'ordre ℓ^{m-1} de $\mathrm{Gal}\,(K/k)$: on obtient une infinité de places v pour lesquelles le Frobenius $F_{K/k}(v)$ a une image non triviale dans le quotient d'ordre ℓ de G, donc engendre G.

□

Par exemple, le corollaire ci-dessus donne qu'un élément de $\mathbf{Z}$ qui n'est pas un carré ne peut pas devenir un carré modulo tous les nombres premiers à l'exception d'un nombre fini d'entre eux.

8.3. Extensions de Kummer

Dans ce paragraphe, nous établissons des résultats généraux sur les extensions de Kummer, qui seront utiles aussi bien dans le prochain paragraphe que pour le théorème d'existence global.

On fixe un corps k et un entier $n > 0$ non divisible par la caractéristique de k, tel que k **contienne une racine primitive n-ième de l'unité** ζ.

Définition 8.14 Une *extension de Kummer* de k est une extension de corps K de k de la forme $K = k(\sqrt[n]{\Delta})$, où Δ est un sous-groupe de k^*, contenant k^{*n}, et tel que Δ/k^{*n} soit fini. [38]

Noter que comme $\zeta \in k$, la notation $k(\sqrt[n]{\Delta})$ n'est pas ambigüe. Comme pour tout $a \in \Delta$, l'extension $k(\sqrt[n]{a})$ est cyclique de degré divisant n (elle correspond à l'élément de $H^1(k, \mathbf{Z}/n) = H^1(k, \mu_n) = k^*/k^{*n}$ donné par la

38. Certains auteurs ne demandent pas cette condition, mais nous n'aurons pas besoin du cas infini.

classe de a), une extension de Kummer est une extension finie abélienne de k dont le groupe de Galois est d'exposant divisant n (isomorphe à un sous-groupe de $(\mathbf{Z}/n)^r$, où r est le cardinal de Δ/k^{*n}). Réciproquement on a :

Proposition 8.15 *Soit K une extension finie abélienne de k dont le groupe de Galois G est d'exposant n. Alors $K = k(\sqrt[n]{\Delta})$ avec $\Delta = K^{*n} \cap k^*$. De plus on a un isomorphisme*

$$\Delta/k^{*n} \to \mathrm{Hom}(G, \mathbf{Z}/n).$$

Démonstration : On a clairement $k(\sqrt[n]{\Delta}) \subset K$. Réciproquement l'extension K/k est la composée de toutes ses sous-extensions E/k cycliques puisqu'elle est abélienne (vu qu'un groupe abélien fini est produit direct de groupes cycliques). Une telle extension E est de degré divisant n, donc s'écrit $E = k(\sqrt[n]{a})$ avec $a \in k^* \cap K^{*n}$, d'où $E \subset k(\sqrt[n]{\Delta})$ et finalement $K \subset k(\sqrt[n]{\Delta})$.

On définit alors un homorphisme $u : \Delta \to \mathrm{Hom}(G, \mathbf{Z}/n)$ par $u(a) = \chi_a$, où

$$\chi_a(\sigma) = \sigma(\sqrt[n]{a})/\sqrt[n]{a}.$$

(le choix de ζ permet d'identifier $\mathbf{Z}/n$ au groupe multiplicatif des racines de l'unité de k^*). Le noyau de u est k^{*n} car χ_a est trivial ssi $\sqrt[n]{a} \in k^*$. Il reste à montrer que u est surjectif. Soit $\chi \in \mathrm{Hom}(G, \mathbf{Z}/n) = \mathrm{Hom}(G, \mu_n)$, alors χ devient un 1-cocycle (par Hilbert 90) quand on le voit comme une application de G dans K^*. Ceci signifie qu'on a un $b \in K^*$ tel que $\chi(\sigma) = \sigma(b)/b$ pour tout $\sigma \in G$. Alors

$$\sigma(b^n) = (\sigma b)^n = \chi(\sigma)^n b^n = b^n$$

d'où $a := b^n \in k^* \cap K^{*n} = \Delta$, et finalement $\chi = \chi_a$.

□

On aura besoin également du résultat "local" suivant.

Lemme 8.16 *Soit K un corps local. Soit $n > 0$ un entier non divisible par la caractéristique du corps résiduel κ de K, on suppose que K contient une racine primitive n-ième de 1 (et donc n divise $q - 1$, où $q = \#\kappa$). Alors, pour $x \in K^*$, l'extension $L = K(\sqrt[n]{x})/K$ est non ramifiée si et seulement si $x \in U_K K^{*n}$.*

Démonstration : Supposons que $x = u.y^n$ avec $u \in U_K$ et $y \in K^*$. On veut montrer que $K(\sqrt[n]{u})$ est non ramifiée sur K. Par le lemme de Hensel, le polynôme $X^n - u$ se décompose en produits de facteurs linéaires sur l'extension non ramifiée K' de K dont le corps résiduel est le corps de

décomposition de la réduction $X^n - \bar{u}$ sur κ, donc ${}^n\sqrt{u} \in K'$ et on a bien $K({}^n\sqrt{u})$ non ramifiée sur K. Réciproquement si $K({}^n\sqrt{x})/K$ est non ramifiée, écrivons $x = u.\pi^r$ avec $u \in U_K$ et π uniformisante de K. Alors la valuation $v_L({}^n\sqrt{u.\pi^r})$ vaut $\frac{1}{n}v_L(\pi^r) = \frac{1}{n}v_K(\pi^r)$, ce qui montre que n divise r.

□

Enfin, les extensions de Kummer sont liées au résultat "local" suivant, que nous utiliserons au prochain paragraphe :

Proposition 8.17 *Soit k_v un complété d'un corps global k. Soit $n > 0$ un entier non divisible par la caractéristique de k (ce qui est automatique si k est un corps de nombres), et tel que $\mu_n \subset k_v$. Alors le cardinal de k_v^*/k_v^{*n} est $n^2/ \mid n \mid_v$, et si v est finie le cardinal de $\mathcal{O}_v^*/\mathcal{O}_v^{*n}$ est $n/ \mid n \mid_v$.*

Démonstration : Le cas où v est archimédienne est immédiat, en notant que pour v réelle on a forcément $n = 1$ ou $n = 2$, et pour v complexe $\mid n \mid_v = n^2$ par convention. Supposons donc v finie. Comme $k_v^* \simeq \mathbf{Z} \times \mathcal{O}_v^*$, il suffit de calculer le cardinal de $\mathcal{O}_v^*/\mathcal{O}_v^{*n}$. Pour cela, on fait opérer le groupe $\mathbf{Z}/n$ trivialement sur $\mathcal{O}_v^*$, et on considère le quotient d'Herbrand associé $h_n(\mathcal{O}_v^*)$. Comme $H^1(\mathbf{Z}/n, \mathcal{O}_v^*) = \mathrm{Hom}(\mathbf{Z}/n, \mathcal{O}_v^*)$ est de cardinal n (parce que $k_v \supset \mu_n$), on a

$$h_n(\mathcal{O}_v^*) = \frac{\#\mathcal{O}_v^*/\mathcal{O}_v^{*n}}{n}.$$

On est donc ramené à montrer que $h_n(\mathcal{O}_v^*) = \mid n \mid_v^{-1}$. Si k est un corps de fonctions de caractéristique p, l'hypothèse faite sur n implique que $\mid n \mid_v = 1$, et par ailleurs le sous-groupe d'indice fini U_v^1 de $U_v = \mathcal{O}_v^*$ est un pro-p-groupe, donc vérifie $h_n(U_v^1) = 1$ puisque p ne divise pas n. On conclut avec le théorème 1.34. Si k est un corps de nombres, le groupe U_v^1 possède un sous-groupe d'indice fini isomorphe au groupe additif $\mathcal{O}_v$ ([11], chapitre XIV, proposition 10). Comme $H^1(\mathbf{Z}/n, \mathcal{O}_v) = \mathcal{O}_v[n] = 0$, le théorème 1.34 donne alors

$$h_n(U_v) = h_n(\mathcal{O}_v) = \#(\mathcal{O}_v/n\mathcal{O}_v) = \mid n \mid_v^{-1}$$

comme on voulait.

□

8.4. Première inégalité et axiome du corps de classes

Nous revenons aux corps globaux. Dans tout ce paragraphe, k désigne un corps global et n une puissance d'un nombre premier ℓ différent de la caractéristique de k, tel que k contienne une racine primitive n-ième de l'unité ζ. Le but va d'abord être de calculer (par une méthode due à Chevalley) le

groupe de normes $N_{K/k}C_K$ pour une extension de Kummer K/k de groupe de Galois $G = (\mathbf{Z}/n)^r$. On commence par fixer un ensemble fini S de places de k, contenant toutes les places archimédiennes, les places au-dessus de ℓ, les places ramifiées dans K/k, et tel que $I_k = I_{k,S}k^*$ (cf. proposition 7.15). On note s le cardinal de S.

Proposition 8.18 *Avec les notations ci-dessus, on a $s \geq r$. De plus, il existe un ensemble T de places de k, disjoint de S et de cardinal $s - r$, tel que $K = k(\sqrt[n]{\Delta})$, où Δ est le noyau de l'application diagonale*

$$k_S \to \prod_{v \in T} k_v^*/k_v^{*^n}.$$

avec de plus $\Delta = K^{*^n} \cap k_S$.

(Rappelons que $I_{k,S}$ est le groupe des S-idèles et $k_S = k^* \cap I_{k,S}$ est le groupe des S-unités).

Démonstration : On commence par montrer que $K = k(\sqrt[n]{\Delta})$ avec $\Delta = K^{*^n} \cap k_S$. La proposition 8.15 donne $K = k(\sqrt[n]{D})$ avec $D = K^{*^n} \cap k^*$. Pour $x \in D$, le choix de S donne que $k(\sqrt[n]{x})/k$ est non ramifiée pour $v \notin S$, d'où $x = u_v y_v^n$ avec $u_v \in U_v = \mathcal{O}_v^*$ et $y_v \in k_v^*$ (lemme 8.16). Posons $y_v = 1$ pour $v \in S$, on obtient un idèle $y = (y_v)$, qu'on peut écrire (toujours par le choix de S) $y = \alpha.z$ avec $\alpha \in I_{k,S}$ et $z \in k^*$. Alors $x/z^n \in I_{k,S} \cap k^* = k_S$ donc $x/z^n \in \Delta$. Ainsi $D = \Delta.k^{*^n}$ comme on voulait.

Posons $N = k(\sqrt[n]{k_S})$, alors $N \supset K$ puisque $k_S \supset \Delta$. Comme $k_S k^{*^n}/k^{*^n} = k_S/k_S^n$ (observer que $k^{*^n} \cap k_S = k_S^n$), la proposition 8.15 donne

$$\mathrm{Gal}\,(N/k) \simeq \mathrm{Hom}(k_S/k_S^n, \mathbf{Z}/n).$$

D'autre part k_S contient les racines n-ièmes de l'unité et c'est donc un groupe abélien isomorphe à $\mathbf{Z}^{s-1} \times \mu_q$ (où q est un entier tel que n divise q) par le théorème des unités de Dirichlet ; ceci donne que k_S/k_S^n est un $\mathbf{Z}/n$-module libre de rang s, donc c'est aussi le cas de $\mathrm{Gal}\,(N/k)$. Comme son quotient $G = \mathrm{Gal}\,(K/k)$ est par hypothèse un $\mathbf{Z}/n$-module libre de rang r, on obtient déjà $r \leq s$ et $\mathrm{Gal}\,(N/K)$ est un $\mathbf{Z}/n$-module libre (pour voir ceci, on peut par exemple utiliser que tout module projectif de type fini sur l'anneau local $\mathbf{Z}/\ell^m\mathbf{Z}$ est libre) de rang $s - r$.

Choisissons alors une $\mathbf{Z}/n$-base $\sigma_1, ..., \sigma_{s-r}$ de de $\mathrm{Gal}\,(N/K)$, et appelons N_i le corps fixe de σ_i pour $i = 1, ..., s - r$. Alors $K = \bigcap_{1 \leq i \leq s-r} N_i$. D'après le corollaire 8.13, on peut trouver pour chaque i un idéal premier $\wp_i$ de

N_i, au-dessus d'une place finie v_i de k, tel que : les places v_i sont deux à deux distinctes, ne sont pas dans S, et chaque $\wp_i$ est inerte dans l'extension N/N_i (rappelons que les N/N_i sont cycliques d'ordre n, avec n puissance d'un nombre premier ℓ). Ceci signifie que le Frobenius associé à $\wp_i$ engendre $\mathrm{Gal}\,(N/N_i)$, ou encore qu'il y a un seul premier $\wp_i' = \wp_i N$ de N au-dessus de N_i. Nous allons montrer que $T = \{v_1, ..., v_{s-r}\}$ convient.

La place v_i est non ramifiée dans l'extension N/k d'après le lemme 8.16. En particulier le groupe de décomposition $\mathrm{Gal}\,(N/Z_i)$ de $\wp_i'$ dans N/k est cyclique, engendŕe par le Frobenius $F_{N/k}(v_i)$. D'autre part $\mathrm{Gal}\,(N/Z_i) \supset \mathrm{Gal}\,(N/N_i)$ car tout élément de $\mathrm{Gal}\,(N/k)$ qui induit l'identité sur N_i laisse fixe $\wp_i$, donc $\wp_i'$. Comme $\mathrm{Gal}\,(N/N_i)$ est d'ordre n et $\mathrm{Gal}\,(N/Z_i)$ cyclique d'exposant $\leq n$, la seule possibilité est finalement $N_i = Z_i$. On en conclut que $\mathrm{Gal}\,(N/N_i)$ est le groupe de décomposition de v_i dans N/k. Comme $\mathrm{Gal}\,(N/K)$ est le produit direct des $\mathrm{Gal}\,(N/N_i)$, on obtient que K/k est la sous-extension maximale de N/k dans laquelle toutes les places v_i sont totalement décomposées : en effet cette propriété revient à dire que K est la sous-extension maximale de N/k telle que tous les $F_{N/k}(v)$ soient dans $\mathrm{Gal}\,(N/K)$. Soit alors $x \in k_S$. On obtient :

$$x \in \Delta \Leftrightarrow k(\sqrt[n]{x}) \subset K \Leftrightarrow k_{v_i}(\sqrt[n]{x}) = k_{v_i}, \forall i = 1, ..., s-r$$

ce qui signifie exactement que Δ est le noyau de $k_S \to \prod_{i=1}^{s-r} k_{v_i}^*/k_{v_i}^{*n}$.

□

On en vient au résultat le plus compliqué de ce paragraphe, qui inclut en particulier la "première inégalité" dans le cas d'une extension de Kummer :

Theorème 8.19 *Soient Δ et T comme dans la conclusion de la proposition 8.18. On pose*

$$I_k(S,T) := \prod_{v \in S} k_v^{*n} \times \prod_{v \in T} k_v^* \times \prod_{v \notin S \cup T} U_v.$$

Soit $C_k(S,T) = I_k(S,T).k^*/k^*$. Alors on a

$$N_{K/k} C_K \supset C_k(S,T)$$

et $[C_k : C_k(S,T)] = [K : k]$. Si de plus l'extension K/k est cyclique (de groupe $\mathbf{Z}/\ell$ donc), on a $C_k(S,T) = N_{K/k} C_K$.

On commence par un lemme :

Lemme 8.20 *On a $I_k(S,T) \cap k^* = k_{S \cup T}^n$.*

Démonstration : Il est immédiat qu'on a l'inclusion $k_{S\cup T}^n \subset I_k(S,T)\cap k^*$. Soit réciproquement $y \in I_k(S,T) \cap k^*$, posons $M = k(\sqrt[n]{y})$. Pour montrer que $M = k$, il suffit d'après le corollaire 8.8 de voir que $C_k = N_{M/k}C_M$. Soit donc $\alpha \in I_{k,S}$, d'image $[\alpha] \in C_k = I_{k,S}k^*/k^*$. Montrons que l'application diagonale $f : k_S \to \prod_{v\in T} U_v/U_v^n$ est surjective, où U_v^n est le sous-groupe des puissances n-ièmes dans U_v. Son noyau est Δ d'après la proposition 8.18, et on a

$$\#(k_S/\Delta) = \frac{\#k_S/k_S^n}{\#\Delta/k_S^n}.$$

Comme on l'a vu dans la preuve de la proposition 8.18 (conséquence du théorème des unités de Dirichlet), le cardinal de k_S/k_S^n est n^s ; d'autre part le cardinal de $\Delta/k_S^n = \Delta k^{*^n}/k^{*^n}$ est celui de $G = \mathrm{Gal}\,(K/k)$ par la proposition 8.15, c'est donc n^r. Finalement le cardinal de k_S/Δ est n^{s-r}, et il suffit pour obtenir la surjectivité voulue de voir que c'est aussi celui de $\prod_{v\in T} U_v/U_v^n$. Or c'est bien le cas d'après la proposition 8.17, vu que v ne divise pas ℓ si $v \in T$ et n est une puissance de ℓ.

La surjectivité de f permet de trouver $x \in k_S$ tel que pour toute place v de T, on ait $\alpha_v = x.u_v^n$ avec $u_v \in U_v$. Posons $\alpha' = \alpha/x$, il suffit de voir que α' est dans $N_{M/k}I_M$, ce qu'on peut vérifier composante par composante d'après le lemme 8.11. Pour $v \in S$, on a $y \in k_v^{*^n}$ donc $M_v = k_v$, ce qui implique évidemment que α'_v est une norme de l'extension M_v/k_v. Pour $v \in T$, cela marche aussi parce que $\alpha'_v = u_v^n$ est une puissance n-ième. Enfin pour $v \notin S\cup T$, on a M_v/k_v non ramifiée et $\alpha'_v \in U_v$, ce qui suffit à assurer que α'_v est une norme locale d'après la proposition 4.1. Finalement on a bien $M = k$, soit $y \in k^{*^n} \cap I_k(S,T) \subset k_{S\cup T}^n$ comme on voulait.

□

Preuve du théorème 8.19 : On utilise la suite exacte :

$$1 \to I_{k,S\cup T} \cap k^*/I_k(S,T)\cap k^* \to I_{k,S\cup T}/I_k(S,T) \to I_{k,S\cup T}.k^*/I_k(S,T)k^* \to 1$$

et on calcule les cardinaux des différents termes. Comme $I_k = I_{k,S\cup T}.k^*$, l'ordre du groupe de droite est $[C_k : C_k(S,T)]$. D'après le lemme 8.20, l'ordre du groupe de gauche est $[k_{S\cup T} : k_{S\cup T}^n] = n^{2s-r}$ comme on l'a déjà vu (car le cardinal de $S\cup T$ est $2s-r$). Enfin le cardinal du groupe du milieu est celui de $\prod_{v\in S}[k_v^* : k_v^{*^n}]$, soit $\prod_{v\in S} n^2/\mid n\mid_v = n^{2s}$ d'après la proposition 8.17. On obtient donc

$$[C_k : C_k(S,T)] = n^r = [K : k].$$

comme voulu.

Montrons maintenant que $C_k(S,T) \subset N_{K/k}C_K$. Soit $\alpha \in I_k(S,T)$, on doit vérifier (lemme 8.11) que chaque composante α_v de α est une norme locale.

Pour $v \in S$, on a $\alpha_v \in k_v^{*n}$, qui est une norme locale via l'isomorphisme de réciprocité local $k_v^*/NK_v^* \simeq \mathrm{Gal}\,(K_v/k_v)$ et le fait que $\mathrm{Gal}\,(K/k)$ soit d'exposant n. Pour $v \in T$, on a $K_v = k_v$ car $\Delta \subset k_v^{*n}$ donc pas de problème. Enfin pour $v \notin S \cup T$, α_v est une unité et K_v/k_v est non ramifiée par le lemme 8.16 donc cela marche encore (proposition 4.1).

Enfin, si K/k est cyclique, on a $r = 1$ et le corollaire 8.8 donne

$$[K : k] \leq [C_k : N_{K/k}C_K] \leq [C_k : C_k(S,T)] = [K : k]$$

ce qui prouve l'égalité $N_{K/k}C_K = C_k(S,T)$.

□

On en déduit enfin :

Theorème 8.21 (Axiome du corps de classes global) *Soit k un corps global. Soit K une extension finie galoisienne de k de groupe de Galois G cyclique. Alors $\widehat{H}^0(G, C_K)$ est de cardinal $[K : k]$, et $H^1(G, C_K) = 0$.*

On verra un peu plus loin que la nullité de $H^1(G, C_K)$ est encore valable si G est un groupe fini quelconque. L'assertion sur $\widehat{H}^0(G, C_K)$ est également valable (sous une forme plus précise) dès que G est fini abélien, comme conséquence de résultats que nous verrons dans les prochains chapitres. On en déduira aussi que dans le théorème 8.19, l'égalité $C_k(S,T) = N_{K/k}C_K$ est encore vraie si on suppose seulement que l'extension K/k est abélienne.

Démonstration : On va se limiter à donner la preuve si la caractéristique de k ne divise pas $[K : k]$. Le cas où k est un corps de fonctions de caractéristique $p > 0$ divisant $[K : k]$ doit se traiter à part (cf. [1], chapitre 6).

Comme on sait que le quotient d'Herbrand $h(G, C_K)$ est $n := [K : k]$ par le théorème 8.7, il suffit de voir que $\widehat{H}^{-1}(G, C_K)$ (qui est aussi $H^1(G, C_K)$) est de cardinal 1. On raisonne par récurrence sur n. Considérons une sous extension M/k de K/k de degré ℓ premier. Si $\ell < n$, l'hypothèse de récurrence et la suite exacte de restriction-inflation donnent $H^1(G, C_K) = 0$. Supposons donc que $n = \ell$ est premier et posons $k' = k(\mu_\ell)$, $K' = K(\mu_\ell)$. Alors K'/k' est une extension de Kummer cyclique et le théorème précédent donne $\widehat{H}^0(\mathrm{Gal}\,(K'/k'), C_{K'})$ de cardinal $[K' : k']$, donc $H^1(\mathrm{Gal}\,(K'/k'), C_{K'}) = 0$ (toujours avec le théorème 8.7). Comme $[k' : k] \leq \ell - 1$, l'hypothèse de récurrence donne aussi $H^1(\mathrm{Gal}\,(k'/k), C_{k'}) = 0$ d'où $H^1(\mathrm{Gal}\,(K'/k), C_{K'}) = 0$ par la suite de restriction-inflation, et a fortiori $H^1(G, C_K) = 0$ par la même suite.

□

Corollaire 8.22 (Principe de Hasse normique) *Soit k un corps global. Soit K une extension finie cyclique de k. Alors un élément $x \in k^*$ est une norme de l'extension K/k ssi son image x_v dans k_v^* est une norme de K_v/k_v pour toute place v de k.*

Attention, ce résultat n'est pas vrai pour une extension abélienne quelconque (voir par exemple l'exercice 5 de [3]).

Démonstration : Soit $G = \mathrm{Gal}\,(K/k)$. Comme $\widehat{H}^{-1}(G, C_K) = 0$, la suite exacte de cohomologie modifiée donne une injection $\widehat{H}^0(G, K^*) \to \widehat{H}^0(G, I_K)$, ce qui permet de conclure avec la proposition 8.1, b).

□

Theorème 8.23 *Soit K/k une extension finie galoisienne de corps globaux de groupe G. Alors $H^1(G, C_K) = 0$.*

Démonstration : Pour G cyclique, le résultat fait partie de l'axiome du corps de classes (théorème 8.21). Le cas où G est un p-groupe avec p premier se traite par récurrence sur le cardinal de G, en prenant une sous-extension E/k galoisienne de degré p (rappelons que l'abélianisé d'un p-groupe est un p-groupe non trivial, donc G a un quotient d'ordre p) et en utilisant la suite exacte de restriction-inflation

$$0 \to H^1(\mathrm{Gal}\,(E/k), C_E) \to H^1(G, C_K) \to H^1(\mathrm{Gal}\,(K/E), C_K).$$

Finalement, pour G quelconque, on considère, pour tout p divisant $\#G$, un p-Sylow G_p de G et son corps fixe K_p. Alors, comme $H^1(G, C_K)$ est la somme directe des $H^1(G, C_K)\{p\}$, l'application

$$H^1(G, C_K) \to \prod_p H^1(\mathrm{Gal}\,(K/K_p), C_K)$$

obtenue via les restrictions est injective par le lemme 2.2, ce qui donne le résultat d'après le cas où G est un p-groupe.

□

Corollaire 8.24 *Soit $C = \varinjlim_K C_K = I_{\bar{k}}/\bar{k}^*$. Alors $H^1(k, C) = 0$.*

8.5. Exercices

1. Soit K un corps local. Soit n un entier premier à la caractéristique de K, et tel que K contienne les racines n-ièmes de l'unité. On pose $L = K(\sqrt[n]{K^*})$. Montrer que L est une extension finie abélienne de K et que le groupe des normes $N_{L/K}L*$ est exactement ${K^*}^n$.

2. Soit k un corps global. Soit K une extension finie galoisienne de k. Montrer qu'on a une injection

$$\mathrm{Br}\,(K/k) \to \bigoplus_{v\in\Omega_k} \mathrm{Br}\,(K_v/k_v).$$

3. Soit k un corps global. Soit K une extension finie galoisienne de k (pas forcément abélienne). Montrer qu'il existe une infinité de places v de k telles que l'extension K/k ne soit pas totalement décomposée en v. Le résultat vaut-il encore si K/k est une extension finie séparable qui n'est pas galoisienne ?

9. Loi de réciprocité et théorème de Brauer-Hasse-Noether

Dans ce chapitre, on va calculer le groupe de Brauer d'un corps global, par une méthode assez similaire à celle du cas local, à ceci près que le rôle joué par les extensions non ramifiées sera ici tenu par des extensions **cycliques** d'un type particulier, dites *cyclotomiques* (i.e. engendrées par des racines de l'unité). Un point très important sera de démontrer la *loi de réciprocité globale* associée au symbole normique (dont un cas très particulier est la classique loi de réciprocité quadratique). Pour cela, nous utiliserons les calculs locaux provenant de la construction de Lubin-Tate pour $\mathbf{Q}_p$.

Dans tout le chapitre, on désigne par k un corps global, par I_k le groupe des idèles de k, et par $C_k = I_k/k^*$ son groupe des classes d'idèles. On utilisera également les groupes $I = I_{\bar{k}} := \varinjlim_K I_K$ et $C = C_{\bar{k}} := \varinjlim_K C_K = I/\bar{k}^*$, la limite étant prise sur les extensions finies (galoisiennes) K de k. On note Ω_k (resp. Ω_f, $\Omega_{\mathbf{R}}$) l'ensemble des places (resp. des places finies, des places réelles) de k.

9.1. Existence d'une extension cyclique neutralisante

Dans ce paragraphe, on va montrer que pour tout élément α du groupe de Brauer $\mathrm{Br}\,k$ d'un corps global, il existe une extension finie cyclique K/k

de k telle que la restriction de α à $\mathrm{Br}\, K$ soit nulle.

Proposition 9.1 *Soit p un nombre premier. Soit L/k une extension galoisienne (infinie) de k. On suppose que L est totalement imaginaire (i.e. n'a pas de plongements réels) si $p = 2$ et k est un corps de nombres. On fait l'hypothèse que pour toute place finie v de k, l'extension L_v/k_v est de degré divisible par p^∞. Alors on a*

$$H^2(L, I)\{p\} = 0. \quad H^2(\mathrm{Gal}\,(L/k), I_L)\{p\} \simeq H^2(k, I)\{p\}.$$

où $I_L = I^{\mathrm{Gal}\,(\bar{k}/L)}$ est la limite inductive des I_K pour les sous-extensions K/k finies galoisiennes de L/k.

Rappelons qu'ici L_v désigne le corps Lk_v, qui est aussi la réunion des K_v pour K extension finie de k incluse dans L (avec les conventions rappelées au début du paragraphe 8.1.).

Démonstration : Comme $H^1(K, I) = 0$ (corollaire 8.2) pour toute extension finie K de k incluse dans L, on a $H^1(L, I) = 0$ en passant à la limite (proposition 3.7). On a donc une suite exacte de restriction-inflation

$$0 \to H^2(\mathrm{Gal}\,(L/k), I_L) \to H^2(k, I) \to H^2(L, I)$$

qui permet de se ramener à montrer que $H^2(L, I)\{p\} = 0$. Le corollaire 8.6 donne (toujours par passage à la limite)

$$H^2(L, I)\{p\} = \bigoplus_{v \in \Omega_k} H^2(L_v, \overline{L}_v^*)\{p\}.$$

Supposons d'abord que v est une place finie de k. Alors l'hypothèse que p^∞ divise le degré de L_v sur k_v donne $H^2(L_v, \overline{L}_v^*)\{p\} = (\mathrm{Br}\, L_v)\{p\} = 0$ par le théorème 4.10, a). Si v est une place archimédienne, on a encore $H^2(L_v, \overline{L}_v^*)\{p\} = 0$: c'est immédiat si $p \neq 2$, et résulte de l'hypothèse pour $p = 2$.

□

Soit $k(\mu)$ l'extension de k qui est obtenue en rajoutant toutes les racines de l'unité. Si k est le corps des fonctions d'une courbe sur $\mathbf{F}_q$, avec $\mathbf{F}_q$ algébriquement fermé dans k (rappelons qu'on peut toujours se ramener à cette situation, quitte à remplacer $\mathbf{F}_q$ par sa fermeture algébrique dans k) le corps $k(\mu)$ s'obtient simplement en prenant le corps des fonctions $\overline{\mathbf{F}_q}(C) = k\overline{\mathbf{F}_q}$. On pose alors $\tilde{k} = k(\mu)$, et on observe que $\mathrm{Gal}\,(\tilde{k}/k)$ est isomorphe à $\widehat{\mathbf{Z}}$. Dans le cas d'un corps de nombres, le groupe $\Gamma = \mathrm{Gal}\,(k(\mu)/k)$

est le produit pour p premier des $\Gamma_p \times \Delta_p$, avec $\Gamma_p \simeq \mathbf{Z}_p$ et $\Delta_p \subset \mathbf{Z}/(p-1)\mathbf{Z}$ pour $p \neq 2$ (resp. $\Delta_2 \subset \mathbf{Z}/2\mathbf{Z}$). On appelle alors T le sous-groupe de torsion de Γ et on note $\tilde{k}$ son corps fixe. On a donc $\mathrm{Gal}\,(\tilde{k}/k) \simeq \widehat{\mathbf{Z}}$.

Définition 9.2 On dit que $\tilde{k}$ est la $\widehat{\mathbf{Z}}$-*extension cyclotomique* de k.

Noter qu'ici on sait que toutes les places archimédiennes de k sont totalement décomposées dans $\tilde{k}$, vu que $\widehat{\mathbf{Z}}$ est sans torsion.

Par ailleurs, on a le

Lemme 9.3 *Soit v une place finie de k. Alors le groupe de décomposition $D_v := G_v(\tilde{k}/k)$ est isomorphe à $\widehat{\mathbf{Z}}$.*

Démonstration : Le corps local k_v ne contient qu'un nombre fini de racines de l'unité, et en particulier il n'y a qu'un nombre fini de nombres premiers ℓ tels que $\zeta_\ell \in k_v$. Ceci implique que D_v contient un sous-groupe de $\widehat{\mathbf{Z}} = \prod_\ell \mathbf{Z}_l$ de la forme $\prod_{\ell \in S} U_\ell \times \prod_{\ell \notin S} \mathbf{Z}_l$, où S est un ensemble fini et U_ℓ est un sous-groupe non réduit à $\{0\}$ (donc de la forme $l^r\mathbf{Z}_l$ avec $r \geq 0$) de $\mathbf{Z}_\ell$, d'où le résultat.

□

Proposition 9.4 *Le groupe $H^2(k, I)$ est la réunion des $H^2(\mathrm{Gal}\,(K/k), I_K)$ où $K \subset \bar{k}$ parcourt les extensions finies cycliques de k. On peut de plus se restreindre aux sous-extensions K de $\tilde{k}$ si k n'a pas de places réelles (resp. de $\tilde{k}_1$, où k_1 est une extension quadratique totalement imaginaire quelconque de k, si k a au moins une place réelle).*

En particulier, en prenant $k_1 = k(\sqrt{-1})$, on voit qu'on peut toujours choisir pour K une extension cyclique cyclotomique (i.e. engendrée par des racines de l'unité) de k.

Démonstration : Soit K une extension finie et galoisienne de k de groupe G. Comme $H^1(K, I) = 0$ (corollaire 8.2), on a une suite exacte

$$0 \to H^2(G, I_K) \to H^2(k, I) \to H^2(K, I)$$

ce qui permet d'identifier $H^2(G, I_K)$ au sous-groupe de $H^2(k, I)$ constitué des éléments dont la restriction à $H^2(K, I)$ est nulle. Soit $x \in H^2(k, I)$. D'après le corollaire 8.6, on peut décomposer x en $x = x_a + x_f$ avec $x_a \in \bigoplus_{v \in \Omega_\mathbf{R}} H^2(k_v, \bar{k}_v^*)$ et $x_f \in \bigoplus_{v \in \Omega_f} H^2(k_v, \bar{k}_v^*)$. La proposition 9.1 (ou plutôt sa preuve) jointe au lemme précédent dit que la restriction de x_f à $H^2(\tilde{k}, I)$ est nulle, d'où une extension finie $K \subset \tilde{k}$ telle que la restriction de x_f à $H^2(K, I)$ soit nulle, ce qui termine la preuve si k n'a pas de places réelles.

Dans le cas où k est un corps de nombres possédant au moins une place réelle et k_1 est une extension quadratique totalement imaginaire de k, notons K_1 l'extension cyclique de degré $2[K : k]$ de k incluse dans $\tilde{k}$; en particulier K_1 est une extension quadratique de K, et elle est disjointe de k_1 sur k (car totalement décomposée aux places réelles de k alors que k_1 n'a pas de places réelles). On a donc $K_1 = K(\sqrt{a})$ et $k_1 = k(\sqrt{b})$ avec a, b dans K. On a aussi $\mathrm{Gal}\,(K_1/k) \simeq \mathbf{Z}/2n$ (où $n := [K : k]$) et $\mathrm{Gal}\,(k_1K_1/k)$ est isomorphe à $\mathbf{Z}/2n \times \mathbf{Z}/2$. Si on pose $L = K(\sqrt{ab})$, l'extension L de k est cyclique (car isomorphe au quotient de $\mathbf{Z}/2n \times \mathbf{Z}/2$ par le sous-groupe constitué des (x, x) avec $x \in \mathbf{Z}/2$) de k, totalement imaginaire (car pour toute place réelle v de K, on a $a_v > 0$ et $b_v < 0$ vu que K_1 est totalement décomposées aux places réelles de k et k_1 totalement imaginaire). Ceci implique que la restriction de x à $H^2(L, I)$ est nulle.

□

On en déduit la première étape dans le calcul de $\mathrm{Br}\,k$:

Proposition 9.5 *Le groupe de Brauer* $\mathrm{Br}\,k$ *est la réunion des* $\mathrm{Br}\,(K/k)$ *pour les extensions* K/k *finies cycliques (et on peut même se restreindre aux* K *comme dans la proposition 9.4).*

Démonstration : Soit K une extension finie galoisienne de k de groupe G. Comme les groupes $H^1(K, C)$, $H^1(k, C)$, $H^1(G, C_K)$ sont nuls ainsi que $H^1(K, \bar{k}^*)$ et $H^1(K, I)$, on a un diagramme commutatif exact :

$$\begin{array}{ccccc}
0 & \longrightarrow & \mathrm{Br}\,K & \longrightarrow & H^2(K, I) \\
 & & \uparrow & & \uparrow \\
0 & \longrightarrow & \mathrm{Br}\,k & \longrightarrow & H^2(k, I) \\
 & & \uparrow & & \uparrow \\
0 & \longrightarrow & H^2(G, K^*) & \longrightarrow & H^2(G, I_K) \\
 & & \uparrow & & \uparrow \\
 & & 0 & & 0
\end{array}$$

On conclut alors avec la proposition 9.4.

9.2. Invariant global et symbole de reste normique

On va fabriquer ici les analogues de l'invariant local et de l'application de réciprocité locale dans le contexte global.

Définition 9.6 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

$$\mathrm{inv}_{K/k} : H^2(G, I_K) \to \frac{1}{[K:k]}\mathbf{Z}/\mathbf{Z} \subset \mathbf{Q}/\mathbf{Z}$$

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 $\mathrm{inv}_v : \mathrm{Br}\, k_v \to \mathbf{Q}/\mathbf{Z}$ (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 $(.,K_v/k_v) : k_v^* \to G_v^{\mathrm{ab}} \subset G^{\mathrm{ab}}$ (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 le *symbole de reste normique* associé à l'extension K/k par

$$(.,K/k) : I_k \to G^{\mathrm{ab}}$$
$$(\alpha,K/k) = \prod_{v\in\Omega_k} (\alpha_v, K_v/k_v) \qquad (6)$$

Le produit est bien défini car si v est non ramifiée dans K/k et $\alpha_v \in U_v = \mathcal{O}_v^*$, alors $(\alpha_v, K_v/k_v) = 1$ (en effet $\widehat{H}^0(G_v, U_{K_v}) = 0$ pour une telle v via la proposition 4.1, donc tous les éléments de U_v sont des normes de K_v/k_v).

La proposition 5.4 donne facilement :

Proposition 9.7 *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 $H^2(G, \mathbf{Z})$.

Les propriétés de l'invariant local (théorème 4.8) donnent aussi :

Proposition 9.8 *Soit L une extension finie galoisienne de k. Soit K une sous-extension. Alors on a des diagrammes commutatifs :*

$$\begin{array}{ccc} H^2(\mathrm{Gal}\,(L/K), I_L) & \xrightarrow{\mathrm{inv}_{L/K}} & \frac{1}{[L:K]}\mathbf{Z}/\mathbf{Z} \\ {\scriptstyle \mathrm{Res}}\uparrow & & \uparrow{\scriptstyle .[K:k]} \\ H^2(\mathrm{Gal}\,(L/k), I_L) & \xrightarrow{\mathrm{inv}_{L/k}} & \frac{1}{[L:k]}\mathbf{Z}/\mathbf{Z} \end{array}$$

et

$$\begin{array}{ccc} H^2(\mathrm{Gal}\,(L/K), I_L) & \xrightarrow{\mathrm{inv}_{L/K}} & \frac{1}{[L:K]}\mathbf{Z}/\mathbf{Z} \\ {\scriptstyle \mathrm{Cor}}\downarrow & & \downarrow{\scriptstyle j} \\ H^2(\mathrm{Gal}\,(L/k), I_L) & \xrightarrow{\mathrm{inv}_{L/k}} & \frac{1}{[L:k]}\mathbf{Z}/\mathbf{Z} \end{array}$$

où l'application

$$j : \frac{1}{[L:K]}\mathbf{Z}/\mathbf{Z} \to \frac{1}{[L:k]}\mathbf{Z}/\mathbf{Z}$$

est l'inclusion. Si de plus K/k est galoisienne, alors $\mathrm{inv}_{L/k}$ *prolonge* $\mathrm{inv}_{K/k}$ *via l'inclusion* $H^2(\mathrm{Gal}\,(K/k), I_K) \to H^2(\mathrm{Gal}\,(L/k), I_L)$.

On a aussi, en passant à la limite sur les extensions finies galoisiennes K de k, une application

$$\mathrm{inv} : H^2(k, I) \to \mathbf{Q}/\mathbf{Z}.$$

Une propriété essentielle pour toute la théorie est le théorème suivant :

Theorème 9.9 (Loi de réciprocité globale) *Soit K une extension finie de k de groupe de Galois G abélien. Alors :*

a) L'application $\mathrm{inv}_{K/k} : H^2(G, I_K) \to \mathbf{Q}/\mathbf{Z}$ *est nulle sur l'image de* $H^2(G, K^*)$ *dans* $H^2(G, I_K)$.

b) Soit $a \in k^*$ un idèle principal. Alors on a $(a, K/k) = 1$.

Pour une extension quadratique $K = k(\sqrt{b})$, le théorème donne que la somme des symboles de Hilbert locaux $(a, b)_v$ (cf. exercice 7 du chapitre 5) sur toutes les places de v est triviale, ce qui redonne pour $k = \mathbf{Q}$ la classique loi de réciprocité quadratique.

Démonstration : Notons déjà que a) implique b) via la proposition 9.7 et le fait qu'un élément du groupe abélien G est trivial si et seulement si son image par tout caractère de G est trivial. Pour démontrer a), il suffit de démontrer que l'application inv : $H^2(k, I) \to \mathbf{Q}/\mathbf{Z}$ est triviale sur l'image de $\mathrm{Br}\,k = H^2(k, \bar{k}^*)$ via la dernière assertion de la proposition 9.8.

Soit donc $\alpha \in \mathrm{Br}\,k$. D'après la proposition 9.5, on peut supposer dans le cas d'un corps de fonctions que $\alpha \in \mathrm{Br}\,(K/k)$ avec $K = k(\zeta_n)$, où n est premier à la caractéristique de k. Dans le cas d'un corps de nombres, on se ramène d'abord à $k = \mathbf{Q}$ en observant que si $\alpha \in \mathrm{Br}\,(L/k)$ avec L finie galoisienne sur k, alors $\mathrm{inv}(\alpha) = \mathrm{inv}_{L/\mathbf{Q}}(\mathrm{Cor}\,\alpha)$, où Cor désigne la corestriction de $\mathrm{Br}\,k$ vers $\mathrm{Br}\,\mathbf{Q}$ (ceci résulte de la proposition 9.8). La proposition 9.5 permet

de plus de supposer que $\alpha \in \mathrm{Br}\,(K/\mathbf{Q})$, où K est une sous-extension cyclique de $\mathbf{Q}(\zeta_n/\mathbf{Q})$ pour un certain n.

Soit alors $G = \mathrm{Gal}\,(K/k)$ et soit χ un générateur du groupe $H^1(G, \mathbf{Q}/\mathbf{Z})$. Le cup-produit par $\delta_\chi \in H^2(G, \mathbf{Z})$ est un isomorphisme de $\widehat{H}^0(G, K^*)$ sur $H^2(G, K^*)$, ce qui permet d'écrire tout élément de $H^2(G, K^*)$ sous la forme $\bar{a} \cup \delta_\chi$ avec $a \in k^*$. D'après la proposition 9.7, on est donc ramené à prouver l'assertion b) du théorème dans les deux cas particuliers :

i) k corps de fonctions sur $\mathbf{F}_q$ et $K = \tilde{k} = k(\zeta_n)$ avec n premier à la caractéristique de k.

ii) $k = \mathbf{Q}$ et $K = k(\zeta)$, où ζ est une racine de l'unité (noter que si E est une sous-extension de $k(\zeta)$, alors $(a, E/k)$ est l'image de $(a, k(\zeta)/k)$ dans le quotient $\mathrm{Gal}\,(E/k)$ de $\mathrm{Gal}\,(k(\zeta)/k)$).

Le cas i) est plus simple : en effet pour toute place v de k, l'extension $\tilde{k}_v/k_v$ est non ramifiée et le lemme 6.11 s'applique ; on obtient que $(a, \tilde{k}_v/k_v)$ est $F(v)^{v(a)}$, où $F(v)$ est le Frobenius en v (qui agit sur ζ_n par l'élévation à la puissance $n(v)$, où $n(v)$ est le cardinal du corps résiduel en v). On a donc

$$(a, \tilde{k}_v/k_v).\zeta_n = \zeta_n^{n(v)^{v(a)}}$$

d'où

$$(a, \tilde{k}/k).\zeta_n = \zeta_n^{\prod_{v \in \Omega_k} n(v)^{v(a)}} = \zeta_n$$

par la formule du produit car $n(v)^{v(a)} = \mid a \mid_v^{-1}$ ce qui conclut la preuve dans ce cas-là.

Dans le cas ii), on doit utiliser les calculs locaux explicites provenant de la théorie de Lubin-Tate. Soit $\theta_p : \mathbf{Q}_p^* \to \mathrm{Gal}\,(K_p/\mathbf{Q}_p)$ l'application de réciprocité locale définie pour p premier ou $p = \infty$ (on convient que $\mathbf{Q}_\infty = \mathbf{R}$). On a déjà

$$\theta_\infty(x).\zeta = \zeta^{\varepsilon(x)}$$

où $\varepsilon(x)$ est le signe de x. Pour p premier, soit $x = p^m u$ avec $u \in \mathbf{Z}_p^*$ et $m \in \mathbf{Z}$. Le théorème 6.14 donne :

$$\theta_p(x).\zeta = \zeta^{p^m}, \quad \forall \zeta \in U_p'$$

$$\theta_p(x).\zeta = \zeta^{u^{-1}}, \quad \forall \zeta \in U_{p^\infty}$$

où U_p' (resp. U_{p^∞}) est l'ensemble des racines de l'unité d'ordre premier à p (resp. d'ordre une puissance de p). Pour montrer la formule $\prod_p \theta_p(a) = 1$ ($a \in \mathbf{Q}^*$) dans le groupe $\mathrm{Gal}\,(K/k)$ (où le produit correspond à la composition des automorphismes), il suffit de traiter le cas $a = -1$ et le cas $a = q$ avec q premier, et de regarder l'action de $\prod_p \theta_p(a) = 1$ sur une racine de l'unité

$\zeta \in U_{\ell^\infty}$ avec ℓ premier. Or, ceci résulte des formules (pour p premier ou $p = \infty$) :

$$\theta_\infty(-1).\zeta = \zeta^{-1}; \quad \theta_\ell(-1).\zeta = \zeta^{-1}; \quad \theta_p(-1).\zeta = \zeta, \forall p \neq l, \infty.$$

Pour $q \neq \ell$:

$$\theta_p(q).\zeta = \zeta, \forall p \neq \ell, q; \quad \theta_\ell(q).\zeta = \zeta^{q^{-1}}; \quad \theta_q(q).\zeta = \zeta^q.$$

Et enfin :

$$\theta_p(\ell).\zeta = \zeta; \quad \forall p.$$

□

Corollaire 9.10 *Soit K une extension finie cyclique de k de groupe G. Alors on a une suite exacte*

$$0 \to H^2(G, K^*) \to H^2(G, I_K) \overset{\text{inv}_{K/k}}{\to} \frac{1}{[K:k]}\mathbf{Z}/\mathbf{Z} \to 0. \tag{7}$$

Démonstration : Montrons d'abord la surjectivité de $\text{inv}_{K/k}$ dans le cas où $[K : k] = p^m$ avec p premier. D'après le corollaire 8.13, il existe une place finie v de k qui est inerte dans K. Comme on a alors $[K_v : k_v] = [K : k]$, le fait que l'invariant local inv_{K_v/k_v} soit un isomorphisme de $H^2(G_v, K_v^*)$ sur $\frac{1}{[K_v:k_v]}\mathbf{Z}/\mathbf{Z}$ implique que $\text{inv}_{K/k}$ est surjectif sur $\frac{1}{[K:k]}\mathbf{Z}/\mathbf{Z}$. On en déduit immédiatement la même surjectivité pour G cyclique quelconque via la proposition 9.8.

Maintenant, les égalités $H^1(G, C_K) = 0$ et $H^3(G, C_K) = H^1(G, C_K) = 0$ (rappelons que G est cyclique) donnent une suite exacte

$$0 \to H^2(G, K^*) \to H^2(G, I_K) \to H^2(G, C_K) \to 0.$$

Ainsi le conoyau de la flèche $H^2(G, K^*) \to H^2(G, I_K)$ a pour cardinal celui de $H^2(G, C_K) = \widehat{H}^0(G, C_K)$, soit $[K : k]$ d'après l'axiome du corps de classes. Comme le théorème 9.9 donne que la suite (7) est un complexe et qu'on a de plus vu que sa dernière flèche était surjective, on en déduit finalement que cette suite est exacte.

□

En passant à la limite sur les extensions cycliques K de k, et en utilisant les propositions 9.4 et 9.5, on obtient alors (avec la proposition 8.1) le théorème principal de ce chapitre :

Theorème 9.11 (Brauer-Hasse-Noether) *Soit k un corps global. Alors on a une suite exacte*

$$0 \to \operatorname{Br} k \to \bigoplus_{v \in \Omega_k} \operatorname{Br} k_v \stackrel{\operatorname{inv}_k}{\to} \mathbf{Q}/\mathbf{Z} \to 0.$$

où l'application inv_k *est définie comme la somme des invariants locaux* $\operatorname{inv}_v : \operatorname{Br} k_v \to \mathbf{Q}/\mathbf{Z}$.

Corollaire 9.12 *Soit p un nombre premier. Soit L une extension algébrique (infinie) séparable de k, supposée totalement imaginaire si $p = 2$. Supposons que p^∞ divise $[L_v : k_v]$ pour toute place finie v de k. Alors* $\operatorname{cd}_p(L) \leq 1$.

Rappelons qu'ici on note $L_v := Lk_v$.

Démonstration : Il suffit de vérifier que $(\operatorname{Br} L')\{p\} = 0$ pour toute extension algébrique séparable L' de L via le théorème 3.27. Comme L' vérifie les mêmes hypothèses que L, on est ramené à montrer que $(\operatorname{Br} L)\{p\} = 0$. Or $\operatorname{Br} L$ s'injecte dans la somme directe (pour v place de k) des $\operatorname{Br} L_v$ (passer à la limite dans le théorème de Brauer-Hasse-Noether). On conclut alors avec le théorème 4.10.

□

9.3. Exercices

1. Soit k un corps de nombres. Soit p un nombre premier. On suppose que $p \neq 2$ ou que k est totalement imaginaire. Montrer que la dimension cohomologique $\operatorname{cd}_p(k)$ est au plus 2 (utiliser la $\widehat{\mathbf{Z}}$-extension cyclotomique de k).

2. Soit k un corps global. Soit S un ensemble de places de k. Donner une condition nécessaire et suffisante sur S pour que l'application diagonale

$$\operatorname{Br} k \to \bigoplus_{v \in S} \operatorname{Br} k_v$$

soit surjective. Même question en remplaçant "surjective" par "injective".

10. Le groupe de Galois abélien d'un corps global

Nous continuons avec les notations du chapitre précédent. En particulier k désigne toujours un corps global dont on note I_k le groupe des idèles et C_k

le groupe des classes d'idèles. On note $G_k = \mathrm{Gal}\,(\bar{k}/k)$ le groupe de Galois absolu de k. On note aussi $I = I_{\bar{k}}$ la limite inductive des I_K pour K extension finie galoisienne de k, et $C = I/\bar{k}^*$ celle des C_K.

10.1. Application de réciprocité et groupe des classes d'idèles

On a défini au chapitre précédent une application $\mathrm{inv}_k : H^2(k, I) \to \mathbf{Q}/\mathbf{Z}$ en passant à la limite sur les applications $\mathrm{inv}_{K/k} : H^2(\mathrm{Gal}\,(K/k), I_K) \to \mathbf{Q}/\mathbf{Z}$. On aimerait en déduire des applications analogues sur $H^2(k, C)$. Une difficulté est qu'en général le groupe $H^2(\mathrm{Gal}\,(K/k), I_K)$ ne se surjecte pas sur $H^2(\mathrm{Gal}\,(K/k), C_K)$, mais nous allons voir que le problème disparaît si on passe à la limite.

Lemme 10.1 *Soit K une extension finie galoisienne de k de groupe G. Alors le cardinal de $H^2(G, C_K)$ divise $[K : k]$.*

Démonstration : C'est tout à fait analogue à l'énoncé local correspondant (lemme 4.6). Le cas d'une extension cyclique fait partie de l'axiome du corps de classes. On en déduit le cas où G est un p-groupe par récurrence sur $[K : k]$, en utilisant la suite exacte (valable parce que $H^1(\mathrm{Gal}\,(K/E), C_K) = 0$ pour toute sous-extension galoisienne E de k) :

$$0 \to H^2(\mathrm{Gal}\,(E/k), C_E) \to H^2(G, C_K) \to H^2(\mathrm{Gal}\,(K/E), C_K).$$

Enfin le cas général se traite en considérant (pour p divisant $\#G$) un p-Sylow $G_p = \mathrm{Gal}\,(K/K_p)$ de G, et en utilisant l'injectivité de la flèche de restriction

$$H^2(G, C_K) \to \bigoplus_p H^2(\mathrm{Gal}\,(K/K_p), C_K).$$

□

Soit maintenant $\tilde{k}$ la $\widehat{\mathbf{Z}}$-extension cyclotomique de k définie comme au chapitre précédent. Posons $\widetilde{G} = \mathrm{Gal}\,(\tilde{k}/k)$. Comme $\mathrm{scd}\,\widehat{\mathbf{Z}} = 2$, on a $H^3(\widetilde{G}, \tilde{k}^*) = 0$, d'où une suite exacte

$$0 \to H^2(\widetilde{G}, \tilde{k}^*) \to H^2(\widetilde{G}, I_{\tilde{k}}) \to H^2(\widetilde{G}, C_{\tilde{k}}) \to 0.$$

Mais d'autre part, en passant à la limite dans le corollaire 9.10, on a aussi une suite exacte

$$0 \to H^2(\widetilde{G}, \tilde{k}^*) \to H^2(\widetilde{G}, I_{\tilde{k}}) \to \mathbf{Q}/\mathbf{Z} \to 0.$$

où la dernière flèche est induite par inv_k. Rappelons que si $K \subset \tilde{k}$ est une extension finie de k, la flèche $H^2(\mathrm{Gal}\,(K/k), C_K) \to H^2(k, C)$ est injective car $H^1(K, C) - 0$. On obtient un isomorphisme

$$\mathrm{inv}_{\tilde{k}/k} : H^2(\widetilde{G}, C_{\tilde{k}}) \simeq \mathbf{Q}/\mathbf{Z}.$$

La proposition suivante est l'analogue global du théorème 4.5 dans le cas local :

Proposition 10.2 *La suite*

$$0 \to \mathrm{Br}\, k \to H^2(k, I) \to H^2(k, C) \to 0$$

est exacte.

Démonstration : Soit K une extension finie galoisienne de k de degré n, dont on note $G := \mathrm{Gal}\,(K/k)$ le groupe de Galois. Soit k_n l'unique sous-extension de $\tilde{k}$ de degré n sur k. On va montrer exactement comme dans le lemme 4.7 que les sous-groupes $H^2(G, C_K)$ et $H^2(\mathrm{Gal}\,(k_n/k), C_{k_n})$ de $H^2(k, C)$ coïncident. Le lemme 10.1 et l'axiome du corps de classes donnent que le cardinal de $H^2(\mathrm{Gal}\,(K/k), C_K)$ divise celui de $H^2(\mathrm{Gal}\,(k_n/k), C_{k_n})$. Mais par ailleurs $H^2(\mathrm{Gal}\,(k_n/k), C_{k_n})$ est inclus dans $H^2(G, C_K)$ via le diagramme commutatif

$$\begin{array}{ccccccc}
0 & \longrightarrow & H^2(G, C_K) & \longrightarrow & H^2(k, C) & \xrightarrow{\mathrm{Res}} & H^2(K, C) \\
 & & & & \uparrow & & \uparrow \\
 & & & & H^2(\widetilde{G}, C_{\tilde{k}}) & \xrightarrow{\mathrm{Res}} & H^2(\mathrm{Gal}\,(\widetilde{K}/K, C_{\widetilde{K}}) \\
 & & & & \downarrow{\scriptstyle \mathrm{inv}_{\tilde{k}/k}} & & \downarrow{\scriptstyle \mathrm{inv}_{\widetilde{K}/K}} \\
 & & & & \mathbf{Q}/\mathbf{Z} & \xrightarrow{.n} & \mathbf{Q}/\mathbf{Z}
\end{array}$$

et le fait que les flèches $\mathrm{inv}_{\tilde{k}/k}$ et $\mathrm{inv}_{\widetilde{K}/K}$ sont des isomorphismes. Finalement on obtient que $H^2(k, C)$ est la réunion des $H^2(\mathrm{Gal}\,(k_n/k), C_{k_n})$, et en particulier la réunion des $H^2(\mathrm{Gal}\,(K/k), C_K)$ pour K cyclique. Par ailleurs, on a l'énoncé analogue avec K^* et I_K (propositions 9.4 et 9.5). On obtient alors le résultat voulu en passant à la limite la suite exacte

$$0 \to \mathrm{Br}\,(K/k) \to H^2(G, I_K) \to H^2(G, C_K) \to 0$$

qui est valable pour toute extension cyclique K de k.

□

Corollaire 10.3 *On a un isomorphisme* $\mathrm{inv}_k : H^2(k, C) \to \mathbf{Q}/\mathbf{Z}$.

Comme de plus la restriction $H^2(k, C) \to H^2(K, C)$ correspond[39] à la multiplication par $[K : k]$ dans $\mathbf{Q}/\mathbf{Z}$, on en déduit pour toute extension finie galoisienne K de k un isomorphisme

$$\mathrm{inv}_{K/k} : H^2(\mathrm{Gal}\,(K/k), C_K) \to \frac{1}{[K : k]}\mathbf{Z}/\mathbf{Z}.$$

Soit K une extension finie galoisienne de k de groupe G. Comme dans le cas local, nous pouvons maintenant appliquer le théorème de Tate-Nakayama en considérant le cup-produit par la classe fondamentale de $H^2(G, C_K)$ (i.e. l'élément qui s'envoie sur $1/[K : k]$ par $\mathrm{inv}_{K/k}$). On obtient

Theorème 10.4 *Soit K une extension finie galoisienne de k de groupe G. Alors on a un isomorphisme*

$$\omega_{K/k} = (., K/k) : C_k/N_{K/k}C_K \to G^{\mathrm{ab}}$$

appelé isomorphisme de réciprocité.

Notons que par construction cet isomorphisme est obtenu par passage au quotient à partir du symbole de reste normique $(., K/k) : I_k \to G^{\mathrm{ab}}$, ce qui justifie l'emploi de la même notation pour l'isomorphisme de réciprocité. On a donc (via la formule 9.7) la même compatibilité que dans le cas local entre les applications $\omega_{K/k}$ et $\omega_{L/k}$ si L est une extension finie galoisienne de k contenant K. On en déduit un *homomorphisme de réciprocité*

$$\mathrm{rec}_k = \mathrm{rec} : C_k \to G_k^{\mathrm{ab}}$$

dont l'image est dense et le noyau $\bigcap_K N_{K/k}C_K$ est le *groupe des normes universelles.*

Corollaire 10.5 *Pour toute extension finie abélienne de k de groupe G, le cardinal de $\widehat{H}^0(G, C_K)$ est $[K : k]$.*

Ainsi l'énoncé de l'axiome du corps de classes global se généralise à toute extension abélienne (pas forcément cyclique). On en déduit aussi un lemme qui sera utile au paragraphe suivant :

39. Avec la propriété $H^1(k, C) = 0$, ceci correspond, comme dans le cas local, aux axiomes d'une *formation de classes.*

Lemme 10.6 *Avec les hypothèses et notations du théorème 8.19, l'égalité*

$$C_k(S,T) = N_{K/k}C_K$$

est valable sans l'hypothèse que K/k est cyclique.

En effet le théorème dit que $[C_k : C_k(S,T)] = [K : k]$ et $C_k(S,T) \subset N_{K/k}C_K$, mais on sait maintenant que $[C_k : N_{K/k}C_K] = [K : k]$ dès que K est une extension finie abélienne de k.

10.2. Le théorème d'existence global

Le théorème suivant est le pendant global du théorème local 6.17.

Theorème 10.7 (Théorème d'existence global) *Soit k un corps global. Alors les sous-groupes ouverts d'indice fini de C_k sont exactement les sous-groupes de normes, i.e. les sous-groupes de la forme $N_{K/k}C_K$ où K est une extension finie abélienne de k. De plus, tout sous-groupe de normes N est associé à une unique extension finie abélienne $K \subset \overline{k}$ de k, qu'on appelle le corps de classes de N.*

Démonstration : Soit K une extension finie et abélienne de k. Alors $N_{K/k}C_K$ est d'indice fini dans C_k d'après le théorème 10.4. Montrons que $N_{K/k}C_K$ est un sous-groupe fermé de C_k. L'application $N_{K/k}$ est continue sur C_K, ce qui fait que l'image du sous-groupe compact C_K^0 est compacte ; par ailleurs dans le cas d'un corps de nombres, le groupe C_k est isomorphe à $C_k^0 \times \mathbf{R}_+^*$: plus précisément on obtient un sous-groupe Γ de représentants de C_k/C_k^0 isomorphe à $\mathbf{R}_+^*$ en considérant une place archimédienne v_0 de k, puis en définissant Γ comme l'image dans C_k des idèles de la forme $(x, 1, 1, ..., 1, ...)$, avec x dans $\mathbf{R}_+^*$, où la première composante est celle en v_0. L'image de Γ dans C_K est alors aussi un sous-groupe de représentants de C_K/C_K^0 et on a

$$N_{K/k}C_K = N_{K/k}C_K^0 \times N_{K/k}\Gamma = N_{K/k}C_K^0 \times \Gamma^n = N_{K/k}C_K^0 \times \Gamma$$

avec $n := [K : k]$, vu que Γ est divisible. Comme $N_{K/k}C_K^0$ est compact, $N_{K/k}C_K^0 \times \Gamma$ est fermé dans $C_k = C_k^0 \times \Gamma$. L'argument est analogue dans le cas d'un corps de fonctions (en remplaçant Γ par un sous-groupe isomorphe à $\mathbf{Z}$). D'autre part, si N est un groupe de normes, l'unicité de l'extension K telle que $N = N_{K/k}C_K$ se montre exactement comme dans le cas local (théorème 6.17, c).

Pour montrer que tout sous-groupe ouvert d'indice fini de C_k est un groupe de normes, on note d'abord que par la meme preuve que dans le cas

local (cf. lemme 6.16), tout sous-groupe qui contient un groupe de normes est un groupe de normes. D'autre part si K et L sont deux extensions finies abéliennes de K et $E = KL$ le corps composé, alors on a

$$N_{K/k}C_K \cap N_{L/k}C_L = N_{E/k}C_E.$$

En effet les deux membres de l'égalité correspondent au noyau de l'application de réciprocité $\omega_{E/k}$ vu la compatiblité des applications de réciprocité et la trivialité du noyau de $\mathrm{Gal}\,(E/k) \to \mathrm{Gal}\,(K/k) \times \mathrm{Gal}\,(L/k)$. On en déduit qu'une intersection finie de groupes de normes est encore un groupe de normes.

Soit alors N un sous-groupe ouvert d'indice fini de C_k. Nous nous limiterons au cas où l'indice $[C_k : N]$ n'est pas divisible par la caractéristique de k (ce qui est toujours le cas pour un corps de nombres ; pour le cas général, voir le chapitre 8 de [1]) Il reste seulement à montrer que N contient un groupe de normes. On se ramène d'abord au cas où n est une puissance d'un nombre premier ℓ (différent de $\mathrm{Car}\,k$), en décomposant n sous la forme $n = \prod_i p_i^{m_i}$ (avec p_i premier), puis en observant que si $N_i \subset C_k$ est le sous-groupe d'indice p^{n_i} qui contient N, alors N est l'intersection de la famille (finie) des N_i (et chaque N_i contient N, donc est ouvert), donc par la remarque ci-dessus il suffit de savoir que chaque N_i est un groupe de normes.

Soit alors $J \subset I_k$ l'image réciproque de N, c'est un sous-groupe ouvert de I_k ; ceci implique que J contient un sous-groupe de la forme

$$U_k^S := \prod_{v \in S} \{1\} \times \prod_{v \notin S} U_v$$

où S est un ensemble fini de places de k, contenant les places archimédiennes. On peut de plus supposer que S contient les places divisant ℓ et que $I_k = I_{k,S}k^*$. Par ailleurs comme J est d'indice n dans I_k, il contient aussi le groupe $\prod_{v\in S} k_v^{*n} \times \prod_{v\notin S}\{1\}$, et donc finalement J contient le groupe

$$I_k(S) = \prod_{v \in S} k_v^{*n} \prod_{v \notin S} U_v.$$

Il suffit donc de montrer que $C_k(S) := I_k(S).k^*/k^*$ contient un groupe de normes.

On commence par le cas où k contient les racines n-ièmes de 1. Posons alors $K = k(\sqrt[n]{k_S})$. C'est une extension de Kummer de degré $[k_S : k_S^n] = n^s$, où s est le cardinal de S (cf. proposition 8.18). Le théorème 8.19, et sa conséquence (lemme 10.6) s'appliquent avec ici $r = s$, c'est-à-dire $T = \emptyset$. On obtient donc $C_k(S) = N_{K/k}C_K$.

Dans le cas général, on note k' l'extension cyclotomique de k obtenue en adjoignant à k les racines n-ièmes de 1. D'après le cas où $\mu_n \subset k$, on peut supposer (quitte à augmenter S) que $I_{k'} = I_{k',S'}k'^{*}$ et $C_{k'}(S') = N_{K'/k'}C_{K'}$, où S' est l'ensemble des places de k' au-dessus d'une place de S et $K' := k'(\sqrt[n]{k'_{S'}})$. La formule (facile à vérifier), valable pour $\beta \in I_{k'}$:

$$(N_{k'/k}(\beta))_v = \prod_{w|v} N_{k'_w/k_v}\beta_w$$

donne $N_{k'/k}(I_{k'}(S')) \subset I_k(S)$ d'où

$$N_{K'/k}(C_{K'}) \subset N_{k'/k}(N_{K'/k'}C_{K'}) = N_{k'/k}(C_{k'}(S')) \subset C_k(S).$$

Ainsi $C_k(S)$ contient $N_{K'/k}(C_{K'})$. Il reste à se ramener à une extension abélienne de k (ici on ne sait même pas si K' est galoisienne sur k) pour conclure. Pour cela, on applique le lemme suivant à $E = K'$ (cf. aussi exercice 1 du chapitre 6) :

Lemme 10.8 *Soit E une extension finie de k, de clôture galoisienne L. Soit M l'extension abélienne maximale de k incluse dans E. Posons $G = \mathrm{Gal}\,(L/k)$ et $H = \mathrm{Gal}\,(L/E)$. Alors on a un diagramme commutatif :*

$$\begin{array}{ccccccc}
\widehat{H}^{-2}(H,\mathbf{Z}) & \xrightarrow{\simeq} & H^{\mathrm{ab}} & \xrightarrow{\simeq} & C_E/N_{L/E}C_L & \xrightarrow{\simeq} & \widehat{H}^{0}(H,C_L) \\
\Big\downarrow{\scriptstyle \mathrm{Cor}} & & \Big\downarrow{\scriptstyle \theta} & & \Big\downarrow{\scriptstyle N_{E/k}} & & \Big\downarrow{\scriptstyle \mathrm{Cor}} \\
\widehat{H}^{-2}(G,\mathbf{Z}) & \xrightarrow{\simeq} & G^{\mathrm{ab}} & \xrightarrow{\simeq} & C_k/N_{L/k}C_L & \xrightarrow{\simeq} & \widehat{H}^{0}(G,C_L)
\end{array}$$

et $N_{E/k}C_E = N_{M/k}C_M$.

Preuve du lemme : La commutativité du diagramme résulte facilement de la compatibilité du cup-produit avec la cohomologie modifiée. On observe alors que $\mathrm{Gal}\,(M/k)$ est le quotient de G par le sous-groupe engendré par $D(G)$ et H : en effet le sous-groupe $\mathrm{Gal}\,(L/M)$ de G est, par définition de M, le plus petit sous-groupe contenant $D(G)$ et H. On en déduit que $\mathrm{Gal}\,(M/k) = G^{\mathrm{ab}}/\pi(H)$, où π est la surjection canonique $G \to G^{\mathrm{ab}} = G/D(G)$, soit finalement $G^{\mathrm{ab}}/\theta(H^{\mathrm{ab}}) = \mathrm{Gal}\,(M/k)$. L'inclusion $N_{E/k}C_E \subset N_{M/k}C_M$ résulte de la transitivité des normes. Réciproquement tout élément α de $N_{M/k}C_M$ vérifie $\omega_{M/k}(\alpha) = 1$, donc l'image de α dans G^{ab} est dans $\mathrm{Im}\,\theta$; le diagramme donne alors que $\alpha \in N_{E/k}C_E$.

□

On va en déduire une description du groupe de Galois abélien d'un corps de nombres :

Theorème 10.9 *Soit k un corps de nombres de groupe de Galois G_k. Alors on a une suite exacte*

$$0 \to D_k \to C_k \stackrel{\text{rec}}{\to} G_k^{\text{ab}} \to 0$$

où D_k est la composante connexe neutre de C_k. Le groupe D_k est aussi le groupe des normes universelles

$$N_{G_k} C = \bigcap_K N_{K/k} C_K$$

où K décrit les extensions finies abéliennes de k, et c'est aussi le noyau du morphisme de complétion profinie $C_k \to C_k^\wedge$, i.e. l'intersection des sous-groupes ouverts d'indice fini de C_k.

Démonstration : Comme $\mathbf{R}_+^*$ n'a pas de quotient fini non trivial, l'image de $C_k = C_k^0 \times \mathbf{R}_+^*$ par l'application de réciprocité rec est la même que celle de C_k. Cette image est donc dense et compacte, i.e. c'est G_k tout entier. On sait par ailleurs déjà que le noyau de rec est $N_{G_k} C$.

Définissons D_k comme la composante connexe neutre de C_k. On observe que dans une décomposition $C_k = C_k^0 \times \mathbf{R}_+^*$, on a $\mathbf{R}_+^* \subset D_k$ (car $\mathbf{R}_+^*$ est connexe) d'où une décomposition $D_k = D_k^0 \times \mathbf{R}_+^*$, où D_k^0 est la composante connexe neutre de D_k. Le groupe C_k/D_k est compact car isomorphe à C_k^0/D_k^0. Tous ses sous-groupes ouverts $\widetilde{U}_i$ sont donc d'indice fini (le quotient est compact et discret) et leur intersection est triviale car C_k/D_k est totalement discontinu. Ainsi l'intersection de leurs images réciproques U_i dans C_k est D_k, et par ailleurs tout sous-groupe ouvert de C_k contient D_k (son intersection avec D_k est non vide, ouverte, et fermée dans D_k, donc cette intersection est D_k). Finalement D_k est bien l'intersection de tous les sous-groupes ouverts d'indice fini de C_k. Le théorème 10.7 donne alors que D_k est aussi l'intersection des sous-groupes de normes, i.e. $D_k = N_{G_k} C$.

□

Remarque : Pour $k = \mathbf{Q}$, on a $D_{\mathbf{Q}} = \mathbf{R}_+^*$ et pour k quadratique imaginaire on a $D_k = \mathbf{C}^*$ (il n'y a qu'une place archimédienne, qui est complexe), mais en général la structure de D_k peut être très compliquée. Pour d'autres propriétés de D_k, voir [10], chapitre VIII, paragraphe 2. ce

Le cas d'un corps de fonctions est, en un sens, plus simple ; la situation est totalement analogue au cas local :

Theorème 10.10 *Soit k le corps des fonctions d'une courbe (projective et lisse) C sur un corps fini $\kappa = \mathbf{F}_q$. Alors, on a une suite exacte*

$$0 \to C_k \stackrel{\text{rec}}{\to} G_k^{\text{ab}} \to \widehat{\mathbf{Z}}/\mathbf{Z} \to 0.$$

Démonstration : Ici C_k est déjà totalement discontinu et C_k^0 est donc profini. On peut supposer κ algébriquement fermé dans k (i.e. la courbe C géométriquement intègre sur κ). Pour toute place v de k, correspondant à un point fermé de C, notons $\kappa(v)$ le corps résiduel de v ; c'est une extension finie de κ. Alors l'application

$$\deg : I_k \to \mathbf{Z}, \quad (\alpha) \mapsto \sum_{v \in \Omega_k} v(\alpha_v).[\kappa(v) : \kappa]$$

se factorise en $\deg : C_k \to \mathbf{Z}$ (le degré d'une fonction $f \in k^*$ est nul), et deg est de plus surjective : c'est par exemple une conséquence de ce que C a des points sur $\mathbf{F}_{q^n}$ pour n assez grand (corollaire du théorème de Lang-Weil), ou encore du fait que la projection $\pi : G_k^{\mathrm{ab}} \to \mathrm{Gal}\,(\bar{\kappa}/\kappa) \simeq \widehat{\mathbf{Z}}$ est surjective et envoie (par le lemme 6.11 et la définition des symboles de reste normique comme produit des symboles locaux) $\mathrm{rec}(\alpha)$ sur $x \mapsto x^{q.\deg \alpha}$, ce qui permet de conclure avec le fait que l'image de rec dans G_k^{ab} est dense.

On en déduit une suite exacte (scindée)

$$0 \to C_k^0 \to C_k \stackrel{\deg}{\to} \mathbf{Z} \to 0.$$

De plus le groupe C_k s'injecte dans sa complétion profinie $C_k^\wedge$ (car C_k^0 est profini), qui est la limite des $C_k/N_{K/k}C_K$ (pour K extension finie abélienne de k) d'après le théorème d'existence, donc est isomorphe à G_k^{ab} via rec. On peut alors étendre deg en une application surjective $C_k^\wedge \to \widehat{\mathbf{Z}}$ de noyau C_k^0, ce qui donne un diagramme commutatif exact :

$$\begin{array}{ccccccccc} 0 & \longrightarrow & C_k^0 & \longrightarrow & C_k & \xrightarrow{\deg} & \mathbf{Z} & \longrightarrow & 0 \\ & & {\scriptstyle =}\downarrow & & \downarrow & & \downarrow{\scriptstyle i} & & \\ 0 & \longrightarrow & C_k^0 & \longrightarrow & C_k^\wedge & \xrightarrow{\deg} & \widehat{\mathbf{Z}} & \longrightarrow & 0 \end{array}$$

d'où on tire immédiatement la suite voulue.

□

10.3. Corps de classes de rayons ; corps de classes de Hilbert

Dans ce paragraphe, on va utiliser le théorème d'existence pour relier les extensions abéliennes de k aux *corps de classes de rayon* qui sont historiquement apparus avant la formulation idèlique de la théorie. Pour simplifier les notations, nous supposerons que k est un corps de nombres. Les résultats

sont analogues pour le corps des fonctions d'une courbe projective lisse C sur $\mathbf{F}_q$ avec quelques changements (notamment en remplaçant les cycles par les cycles de degré 0, le groupe des classes d'idéaux de $\mathcal{O}_k$ par $\mathrm{Pic}^0 C$ etc.).

Définition 10.11 Soit k un corps de nombres. Un *cycle* $\mathcal{M}$ de k est un produit formel $\mathcal{M} = \prod_{v\in\Omega_k} v^{n_v}$, où $n_v \in \mathbf{N}$, n_v est nul pour presque toute v, et $n_v \in \{0,1\}$ si v est archimédienne.

Pour v finie et $n_v \geq 1$, on note $U_v^{n_v}$ le groupe multiplicatif des x tels que $v(x-1) \geq n_v$, ainsi que $U_v^0 = U_v = \mathcal{O}_v^*$. Pour v complexe, on pose $U_v^{n_v} = k_v^* \simeq \mathbf{C}^*$. Pour v réelle, on pose $U_v^1 = \mathbf{R}_+^* \subset k_v^*$ et $U_v^0 = k_v^* \simeq \mathbf{R}^*$. La notation $\alpha_v \equiv 1 \bmod. v^{n_v}$ signifiera $v(\alpha_v - 1) \geq n_v$ si v est finie et $n_v \geq 1$ (et on convient que pour $n_v = 0$ la condition est toujours vérifiée). Pour v complexe ou v réelle avec $n_v = 0$, cette condition sera par définition toujours vérifiée et pour v réelle avec $n_v = 1$, elle signifiera juste $\alpha_v > 0$. Soit $\mathcal{M} = \prod_v v^{n_v}$ un cycle et soit $\alpha \in I_k$. On notera $\alpha \equiv 1 \bmod. \mathcal{M}$ pour la condition : $\alpha_v \equiv 1 \bmod. v^{n_v}$ pour toute place v de k.

Définition 10.12 Soit $\mathcal{M}$ un cycle de k. Posons

$$I_k^{\mathcal{M}} = \{\alpha \in I_k, \alpha \equiv 1 \bmod. \mathcal{M}\} = \prod_{v\in\Omega_k} U_v^{n_v}.$$

L'image $C_k^{\mathcal{M}} = I_k^{\mathcal{M}}.k^*/k^*$ du groupe $I_k^{\mathcal{M}}$ dans C_k s'appelle le *sous-groupe de congruence mod.* $\mathcal{M}$ de C_k. Le quotient $C_k/C_k^{\mathcal{M}}$ est le *groupe de classes de rayon* mod. $\mathcal{M}$.

Le cas où $\mathcal{M} = 1$ est le cycle trivial est particulièrement intéressant : on a alors $I_k^1 = \prod_{v\in\Omega_\infty} k_v^* \times \prod_{v\in\Omega_f} U_v$, d'où on tire que $C_k/C_k^1 = \mathcal{I}_k/\mathcal{P}_k$ est le groupe des classes d'idéaux de $\mathcal{O}_k$. Son cardinal est le nombre de classes $h(k)$.

Theorème 10.13 *Un sous-groupe de C_k est un groupe de normes si et seulement s'il contient un sous-groupe de congruence $C_k^{\mathcal{M}}$.*

Démonstration : Soit $\mathcal{M} = \prod_v v^{n_v}$ un cycle. Le groupe $C_k^{\mathcal{M}}$ est un sous-groupe ouvert de C_k car $I_k^{\mathcal{M}} = \prod_{v\in\Omega_k} U_v^{n_v}$ est un ouvert de I_k. Par ailleurs $C_k^{\mathcal{M}}$ est d'indice fini dans C_k car $[C_k : C_k^1] = h(k)$ est fini et $[C_k^1 : C_k^{\mathcal{M}}]$ est majoré par l'ordre de $I_k^1/I_k^{\mathcal{M}} = \prod_v U_v/U_v^{n_v}$ qui est bien fini (rappelons que $n_v = 0$ pour presque toute place v et $U_v^0 := U_v$). Finalement $C_k^{\mathcal{M}}$ est un groupe de normes par le théorème 10.7.

Soit réciproquement N un groupe de normes, alors son image réciproque J dans I_k est ouverte, donc J contient un sous-ensemble de la forme $\prod_{v\in S} W_v \times \prod_{v\notin S} U_v$, où $S \supset \Omega_\infty$ est un ensemble fini de places et W_v est un voisinage ouvert de 1 dans k_v^*. Pour $v \in S$ finie, on peut supposer que $W_v = U_v^{n_v}$ avec $n_v \in \mathbf{N}$ car les $U_v^m, m \geq 0$ forment une base de voisinages de 1. Pour v archimédienne, les seuls sous-groupes de k_v^* engendrés par un voisinage ouvert de 1 sont k_v^* ou $\mathbf{R}_+^*$ si v est réelle. On en déduit que J contient un sous-groupe de la forme $I_k^{\mathcal{M}}$, et donc que N contient un sous-groupe de congruence $C_k^{\mathcal{M}}$. □

Définition 10.14 Le corps de classes $k^{\mathcal{M}}$ qui est associé au sous-groupe de congruence $C_k^{\mathcal{M}}$ s'appelle le *corps de classes de rayon* mod. $\mathcal{M}$. Le corps k^1 s'appelle le *corps de classes de Hilbert* de k.

On a donc $\mathrm{Gal}\,(k^{\mathcal{M}}/k) \simeq C_k/C_k^{\mathcal{M}}$, et toute extension finie abélienne de k est contenue dans un corps de classes de rayon. On a aussi $\mathcal{M} \mid \mathcal{M}' \Rightarrow k^{\mathcal{M}} \subset k^{\mathcal{M}'} \Rightarrow C_k^{\mathcal{M}} \supset C_k^{\mathcal{M}'}$. On a en particulier $\mathrm{Gal}\,(k^1/k) \simeq \mathcal{I}_k/\mathcal{P}_k$, ce qui fait que le degré $[k^1 : k]$ est le nombre de classes $h(k)$ de k.

Définition 10.15 Soit K un corps local et soit L une extension finie galoisienne de K de groupe G. Le *conducteur* $f(L/K)$ de l'extension L/K est le plus petit entier $n \geq 0$ tel que l'application de réciprocité $\omega_{L/K} : K^* \to G^{\mathrm{ab}}$ soit triviale sur U_K^n (toujours avec la convention $U_K^0 = U_K$).

Notons que comme le noyau de $\omega_{L/K}$ est un sous-groupe ouvert de K^*, ce sous-groupe contient U_K^n pour n assez grand et le conducteur est bien défini. Par ailleurs, le calcul de l'application de réciprocité via Lubin-Tate (théorème 6.14) montre que $f(L/K)$ est nul si et seulement si l'extension est non ramifiée. On généralise cette notion à $K = \mathbf{R}$ ou $K = \mathbf{C}$, en prenant $f(L/K) = 0$ ou $f(L/K) = 1$ suivant que l'extension L est égale à K ou non.

Définition 10.16 Soit k un corps de nombres. Soit K une extension finie et abélienne de k, associée au groupe de normes $N_K := N_{K/k}C_K$. Le *conducteur* $\mathcal{F}$ de l'extension K/k (ou de N_K) est le p.g.c.d. des cycles $\mathcal{M}$ tels que $K \subset k^{\mathcal{M}}$ (ou encore $C_k^{\mathcal{M}} \subset N_{K/k}C_K$).

Autrement dit $k^{\mathcal{F}}$ est le plus petit corps de classes de rayon qui contient K (attention, ceci n'implique pas que le conducteur de $k^{\mathcal{M}}$ est $\mathcal{M}$ car $\mathcal{M} \mapsto C_K^{\mathcal{M}}$ est décroissante, mais pas injective en général).

Proposition 10.17 *Soit K une extension finie et abélienne d'un corps de nombres k, de conducteur $\mathcal{F}$. Alors on a*

$$\mathcal{F} = \prod_{v\in\Omega_k} v^{f(K_v/k_v)}.$$

Démonstration : On commence par un lemme :

Lemme 10.18 *Pour $x_v \in k_v^*$, notons $[x_v]$ l'idèle $(1, ..., 1, x_v, 1...,)$. Soit K une extension finie abélienne de k. Alors la classe de $[x_v]$ dans C_k est dans $N_{K/k}C_K$ si et seulement si $x_v \in N_{K_v/k_v}K_v^*$. De plus la classe d'un idèle α est dans $N_{K/k}C_K$ si et seulement si la classe de $[\alpha_v]$ est dans $N_{K/k}C_K$ pour toute place v de k.*

Preuve du lemme : Supposons $x_v \in N_{K_v/k_v}K_v^*$. Alors on a par définition du symbole de reste normique :

$$([x_v], K/k) = (x_v, K_v/k_v) = 1$$

ce qui montre que la classe de $[x_v]$ appartient à $N_{K/k}C_K$ par le théorème 10.4. Réciproquement supposons que la classe de $[x_v]$ soit dans $N_{K/k}C_K$. Cela signifie qu'il existe $\beta \in I_K$ et $a \in k^*$ tels que $[x_v].a = N_{K/k}\beta$. Ceci implique que a est une norme de K_u/k_u pour toute place u de k autre que v. Mais alors, on obtient que a est aussi une norme de K_v/k_v grâce à la loi de réciprocité (théorème 9.9, b), ce qui prouve que $x_v \in N_{K_v/k_v}K_v^*$.

Pour la deuxième assertion, soit $\alpha \in N_{K/k}I_K$. Alors $\alpha_v \in N_{K_v/k_v}K_v^*$ donc $[\alpha_v] \in N_{K/k}I_K$ par le lemme 8.11. Réciproquement si $[\alpha_v] \in N_{K/k}I_K$, pour toute place v, alors $\alpha_v \in N_{K_v/k_v}K_v^*$ pour toute place v, et donc $\alpha \in N_{K/k}I_K$ par (loc. cit.). Le résultat correspondant pour C_K au lieu de I_K s'en déduit immédiatement.

□

On peut maintenant démontrer la proposition 10.17. Soit $N = N_{K/k}C_K$ et soit $\mathcal{M} = \prod_v v^{n_v}$ un cycle. La condition $C_k^{\mathcal{M}} \subset N$ signifie : pour tout $\alpha \in I_k$, on a que $\alpha \equiv 1$ mod. $\mathcal{M}$ implique $\bar{\alpha} \in N$ (où $\bar{\alpha}$ est la classe de α dans C_k). Cette dernière propriété s'écrit, avec le lemme : $\alpha_v \equiv 1$ mod. v^{n_v} pour toute place v implique $\alpha_v \in N_{K_v/k_v}K_v^*$, ou encore : $U_v^{n_v} \subset N_{K_v/k_v}K_v^*$. Finalement on a montré que $C_k^{\mathcal{M}} \subset N$ équivaut à $f(K_v/k_v) \leq n_v$ pour toute place v, ce qui signifie exactement que $\mathcal{F} = \prod_v v^{f(K_v/k_v)}$.

□

Corollaire 10.19 *Soit K une extension finie et abélienne d'un corps de nombres k, de conducteur $\mathcal{F}$. Alors une place v est ramifiée dans K/k si et seulement si v divise $\mathcal{F}$ (on convient que pour une place archimédienne, non ramifiée signifie totalement décomposée). Le corps de classes de Hilbert est l'extension abélienne maximale de k qui est non ramifiée en toute place de k (y compris les places archimédiennes).*

On conclut avec le célèbre théorème de Kronecker-Weber (qu'on peut aussi déduire de sa version sur $\mathbf{Q}_p$, cf. exercice 3 du chapitre 7).

Theorème 10.20 *L'extension abélienne maximale du corps* $\mathbf{Q}$ *est l'extension* $\mathbf{Q}(\mu_\infty)$ *engendrée par toutes les racines de l'unité.*

Soit ζ_m une racine primitive m-ième de l'unité. On sait déjà que toute extension cyclotomique $\mathbf{Q}(\zeta_m)$ est abélienne, il suffit donc de montrer que toute extension finie abélienne de $\mathbf{Q}$ est contenue dans $\mathbf{Q}(\zeta_m)$ pour un certain m. Pour cela, on va montrer la forme plus précise suivante :

Theorème 10.21 *Soit* $m = \prod p^{n_p} \in \mathbf{N}^*$. *Soit* p_∞ *la place réelle de* $\mathbf{Q}$. *Soit* $\mathcal{M}$ *le cycle* $m.p_\infty$. *Alors le corps de classes de rayon mod.* $\mathcal{M}$ *de* $\mathbf{Q}$ *est* $\mathbf{Q}(\zeta_m)$.

Démonstration : Posons $m = m'.p$ (pour p fixé). Alors $U_p^{n_p}$ est inclus dans le groupe de normes de l'extension non ramifiée $\mathbf{Q}_p(\zeta_{m'})/\mathbf{Q}_p$, et aussi dans celui de $\mathbf{Q}_p(\zeta_{p^{n_p}})/\mathbf{Q}_p$ par Lubin-Tate (cf. exemple à la fin du chapitre 6.). On en déduit que $U_p^{n_p}$ est inclus dans le groupe de normes de $\mathbf{Q}_p(\zeta_m)/\mathbf{Q}_p$, car par compatiblité des applications de réciprocité, son image par $\omega_{\mathbf{Q}_p(\zeta_m)/\mathbf{Q}_p}$ est triviale. Comme $I_{\mathbf{Q}}^{\mathcal{M}} = \prod_{p \neq p_\infty} U_p^{n_p} \times \mathbf{R}_+^*$, on obtient $C_{\mathbf{Q}}^{\mathcal{M}} \subset NC_{\mathbf{Q}(\zeta_m)}$ par le lemme 8.11.

Par ailleurs on a

$$[C_{\mathbf{Q}} : C_{\mathbf{Q}}^{\mathcal{M}}] = [I_{\mathbf{Q}}^1.\mathbf{Q}^* : I_{\mathbf{Q}}^{\mathcal{M}}.\mathbf{Q}^*] = [I_{\mathbf{Q}}^1 : I_{\mathbf{Q}}^{\mathcal{M}}]/[I_{\mathbf{Q}}^1 \cap \mathbf{Q}^* : I_{\mathbf{Q}}^{\mathcal{M}} \cap \mathbf{Q}^*]$$

car $[C_{\mathbf{Q}} : C_{\mathbf{Q}}^1] = 1$ vu que $\mathbf{Z} = \mathcal{O}_{\mathbf{Q}}$ est principal. Or $I_{\mathbf{Q}}^{\mathcal{M}} \cap \mathbf{Q}^* = \{1\}$ et $I_{\mathbf{Q}}^1 \cap \mathbf{Q}^* = \{\pm 1\}$ d'où

$$[C_{\mathbf{Q}} : C_{\mathbf{Q}}^{\mathcal{M}}] = 1/2. \prod_{p \neq p_\infty} [U_p : U_p^{n_p}].2 = \prod_{p \neq p_\infty} \varphi(p^{n_p}) = \varphi(m)$$

soit finalement $[C_{\mathbf{Q}} : C_{\mathbf{Q}}^{\mathcal{M}}] = [\mathbf{Q}(\zeta_m) : \mathbf{Q}] = [C_{\mathbf{Q}} : NC_{\mathbf{Q}(\zeta_m)}]$ ce qui conclut.

□

10.4. Exercices

1. Soit k un corps de nombres. On note D_k la composante connexe neutre de son groupe des classes d'idèles C_k. On note aussi C_k^0 le sous-groupe de C_k constitué des classes d'idèles α telles que $\mid \alpha \mid = 1$, et D_k^0 la composante connexe neutre de C_k^0. Montrer que pour toute extension finie K de k, les applications norme $N_{K/k} : D_K^0 \to D_k^0$ et $N_{K/k} : D_K \to D_k$ sont surjectives (utiliser la compacité de C_k^0).

2. On garde les notations de l'exercice précédent.

a) Soit x un élément divisible de C_k (i.e. pour tout $n > 0$, il existe $y \in C_k$ tel que $y^n = x$). Montrer que $x \in D_k$.

Dans la suite, on fixe un nombre premier ℓ.

b) Soit K une extension finie de k, contenant les racines ℓ-ièmes de l'unité. Montrer que pour S ensemble fini de places de K suffisamment grand (contenant les places archimédiennes et les places divisant ℓ), on a

$$D_K \subset (C_K)^\ell \overline{U}_{K,S}$$

où $U_{K,S} \subset I_K$ est l'ensemble des idèles de la forme $\prod_{v \in S} 1 \times \prod_{v \notin S} U_v$, et $\overline{U}_{K,S}$ est l'image de $U_{K,S}$ dans C_K.

c) En déduire que $D_K^0 \subset (C_K^0)^\ell$, puis que $D_k^0 \subset (N_{K/k} C_K^0)^\ell$ (utiliser l'exercice précédent).

d) Soit $a \in D_k^0$. Montrer que pour tout extension finie K de k, l'ensemble $(N_{K/k} C_K^0) \cap \ell(a)$ est non vide, où $\ell(a)$ est l'ensemble des racines ℓ-ièmes de a dans C_k^0.

e) En déduire que D_k^0 et D_k sont des groupes abéliens divisibles.

Références

[1] E. Artin, J. Tate : *Class field theory*, W. A. Benjamin, Inc., New York-Amsterdam 1968.

[2] N. Bourbaki : *Algèbre*, chapitre V, Hermann, Paris, 1959.

[3] J.W.S. Cassels, A. Fröhlich : *Algebraic number theory*, Academic press, London and New-York, 1967.

[4] D. Harari : Cours de M2 "Cohomologie galoisienne et théorie des nombres",
http ://www.math.u-psud.fr/~harari/enseignement/cogal/poly.pdf

[5] P. Gille, T. Szamuely : *Central Simple Algebras and Galois Cohomology*, Cambridge Studies in Advanced Mathematics **101**, Cambridge University Press, 2006.

[6] S. Lang : *On quasi-algebraic closure*, Ann. Math. **55**, 373-390 (1952).

[7] J. S. Milne : *Arithmetic duality theorems* (Second edition), BookSurge, LLC, Charleston, SC, 2006.

[8] J. Neukirch : *Class field Theory*, Grundlehren der Mathematischen Wissenschaften **280**, Springer-Verlag 1986.

[9] J. Neukirch : *Algebraic Number Theory*, Springer-Verlag, 1999.

[10] J. Neukirch, A. Schmidt, K. Wingberg : *Cohomology of number fields* (Second edition), Grundlehren der Mathematischen Wissenschaften **323**, Springer-Verlag 2008.

[11] J-P. Serre : *Corps locaux* (seconde édition), Hermann, Paris, 1968.

[12] J-P. Serre : *Cohomologie galoisienne* (cinquième édition, révisée et complétée), Lecture Notes in Mathematics **5**, Springer-Verlag, Berlin, 1994.

[13] S. Shatz : *Profinite groups, arithmetic, and geometry*, Annals of Mathematics Studies **67**, Princeton University Press, 1972.

[14] C. Weibel : *An introduction to homological algebra*, Cambridge University Press, 1994.