Projet de semestre

Eté 2005-2006

Vers un Enoncé de la Conjecture de Milnor

CAROLINE LASSUEUR

Encadré par :

DAVID BORNAND

Professeur responsable :

Prof. J. THÉVENAZ
IGAT

Ecole Polytechnique Fédérale de Lausanne
Section de mathématiques
CH-1015 Lausanne
caroline.lassueur@epfl.ch

Resumé

Le but premier de ce travail est de donner les outils et le vocabulaire nécessaires pour comprendre l'énoncé de la conjecture de Milnor. Cette compréhension se fait au travers de notions élémentaires concernant les groupes profinis, la cohomologie des groupes, dont en particulier la cohomologie galoisienne pour finir avec la définition de la K-théorie de Milnor.

To Pinky and The Brain,
Whom I share the plans of !

Pinky : "Gee, Brain, what do you want to do tonight ?"
Brain : "The same thing we do every night, Pinky.
Try to take over the world !"

Table des matières

Table des notations 6

Introduction 7

Chapitre 1. Groupes Profinis 9
1. La notion de limite projective 9
2. Groupe de Galois d'une extension galoisienne 12

Chapitre 2. Cohomologie des groupes profinis 15
1. L'anneau de groupe 15
2. G-modules 16
3. Définition des groupes de cohomologie 17
4. Suite exacte longue en cohomologie 19

Chapitre 3. Un minimum de Cohomologie Galoisienne 25
1. Clôture séparable d'un corps 25
2. Notations 26
3. Calcul de $H^1(\mathbb{K}, \mu_n)$ 27

Chapitre 4. Approche de la conjecture de Milnor 29
1. Définition de la K-théorie de Milnor 29
2. Lemme de Bass-Tate et Conjecture de Milnor 31

Bibliographie 35

Index 37

Table des notations

$\mathrm{Aut}(\mathbb{K})$	Groupe des automorphismes du corps $\mathbb{K}$
$B^n(G, A)$	Groupe des n-cobords du groupe G
$C^n(G, A)$	Groupe des n-cochaînes du groupe G
C_d	Groupe cyclique d'ordre d
$\mathrm{car}(A)$	Caractéristique de l'anneau A
$\mathbb{E}/\mathbb{K}$	Extension de corps $\mathbb{E} \supseteq \mathbb{K}$
$\mathrm{Gal}(\mathbb{E}, \mathbb{K})$	Groupe de Galois de l'extension $\mathbb{E}/\mathbb{K}$
$H^n(G, A)$	n-ème groupe de cohomologie du groupe G à coefficient dans A
Id_S	Application identité de l'ensemble S
Im	Image d'une application
Ker	Noyau
$K_*\mathbb{F}$	K-théorie de Milnor du corps $\mathbb{F}$
$\overline{\mathbb{K}}$	Clôture algébrique du corps $\mathbb{K}$
$\mathbb{K}_s$	Clôture séparable du corps $\mathbb{K}$
$\mathbb{K}[\alpha]$	Extension du corps K par l'élément α
$\varprojlim$	Limite projective
$M^{\otimes n}$	$M \otimes \cdots \otimes M$ n fois
$\mathbb{N}$	Les nombres naturels, 0 compris
$\mathbb{N}_n$	$\{1, 2, 3, \ldots, n\}$
R^*	Groupe des unités de l'anneau R
$res_X(f)$	Restriction de l'application f à l'ensemble X
$T(M)$	Algébre tensorielle sur le module M
$\mathbb{Z}$	Les nombres entiers
$\mathbb{Z}G$	Anneau de groupe de G
$Z^n(G, A)$	Groupe des n-cocycles du groupe G
$< f >$	Idéal principal engendré par l'élément f
$\otimes$	Le produit tensoriel
$\sum$	Symbole de sommation
$\prod$	Produit cartésien
$\subseteq$	L'inclusion
$\hookrightarrow$	Flèche injective
$\twoheadrightarrow$	Flèche surjective
$\forall$	Symbole universel "pour tout"
$\exists$	Symbole universel "il existe"

Introduction

L'idée du thème de ce travail de semestre vient d'un projet de David Kohler de monter un séminaire d'étudiants qui aurait consisté à étudier la conjecture de Milnor ; ceci à l'image d'un projet de l'an passé intitulé *Projet de l'Index* (http ://ima.epfl.ch/ dekohler/index.php). Malheureusement, par manque d'intérêt des étudiants ce projet est quelque peu tombé à l'eau pour se transformer en deux projets de semestres ordinaires dont le but est devenu d'expliquer l'énoncé de la conjecture de Milnor, qui lie la K-théorie algébrique définie par Milnor aux formes quadratiques ainsi qu'à la cohomologie galoisienne.

Pour dire les choses brièvement, la conjecture de Milnor est une proposition de John Milnor qui décrit la K-théorie de Milnor modulo 2 d'un corps $\mathbb{F}$ de caractéristique différente de 2 en utilisant les groupes de cohomologie galoisienne de $\mathbb{F}$ à coefficient dans $\mathbb{Z}/2\mathbb{Z}$. De façon plus symbolique, cette conjecture affirme que $K_*\mathbb{F}/2K_*\mathbb{F}$ est canoniquement isomorphe à $H^*(\mathrm{Gal}(\mathbb{F}_s/\mathbb{F}), \mathbb{Z}/2\mathbb{Z})$. Milnor expose tout ceci dans son article [2] publié en 1970, où il expose aussi plus principalement la conjecture que $K_*\mathbb{F}/2K_*\mathbb{F}$ est canoniquement isomorphe à l'anneau gradué $(W/I, I/I^2, I^2/I^3, \ldots)$ où W est l'anneau de Witt des modules quadratiques anisotropes sur $\mathbb{F}$ et I l'idéal maximal de W constitué des modules de rang pair. J'avoue ouvertement ne pas comprendre cette partie de l'énoncé, mais je m'en remets au travail d'Olivier Isely, *Formes quadratiques et conjecture de Milnor*, aussi disponible sur la bibliothèque du site http://cqfd.epfl.ch, pour expliquer le vocabulaire et les notions nécessaires à la compréhension de cette partie de l'énoncé.

Cette conjecture a été prouvée autour de 1996 par Vladimir Voevodsky, alors qu'elle était restée ouverte pendant plus de 20 ans. L'article original écrit par Voevodsky n'a jamais été publié, mais on peut le trouver sur le site http://www.math.uiuc.edu/K-theory/0170/ . En 2002, il reçoit la médaille Fields avec Laurent Lafforgue pour ses travaux sur la cohomologie motivique grâce à laquelle il démontre la conjecture de Milnor. On trouve ceci dans son article *Motivic cohomology with Z/2 coefficient* [7] publié en 2003. En outre, pour les nombres premiers différents de 2, il existe un résultat analogue, connu sous le nom de conjecture de Bloch-Kato. Des travaux menés par Voevodsky toujours, mènent à une preuve complète de ce résultat, mais apparemment elle attend encore d'être publiée.

Mon travail tentera d'expliquer la partie de l'énoncé qui lie la K-théorie de Milnor à la cohomologie galoisienne et pour être honnête consiste essentiellement à expliquer les pages 83 et 84 du livre de Serre *Cohomologie Galoisienne* [5]. Pour ce faire, le chapitre 1 introduit la notion de groupe profini et montre que le groupe de Galois d'une extension de corps galoisienne est profini. Le chapitre 2 introduit les groupes de cohomolgie d'un groupe profini et développe l'outil essentiel qu'est la suite exacte longue en cohomologie associée à une suite exacte courte de modules

sur un groupe profini. Cette suite exacte longue est alors exploitée au chapitre 3 pour établir l'isomorphisme entre $K_1\mathbb{F}/2K_1\mathbb{F}$ et $H^1(\mathrm{Gal}(\mathbb{F}_s/\mathbb{F}), \mathbb{Z}/2\mathbb{Z})$. Au chapitre 4, on s'intéresse de plus prés à la construction de la K-théorie de Milnor, pour terminer avec l'énoncé de la conjecture de Milnor.

Un tel travail, par son but d'explication d'un énoncé, ne peut pas être self-contained, cependant, dans cette optique, il est écrit pour aller droit au but sans se perdre dans les développements des théories concernant les notions introduites, préliminaires à la conjecture. Il est aussi écrit pour être accessible aisément à un niveau de première année de master, ainsi les seuls pré-requis supposés sont quelques notions élémentaires d'algèbre, de topologie et de théorie de Galois.

CHAPITRE 1

Groupes Profinis

1. La notion de limite projective

Dans cette section, I désignera un pré-ordre filtrant à droite, i.e. l'ensemble I est muni d'une relation binaire $\leq$ réflexive et transitive avec la propriété supplémentaire que pour toute paire d'éléments $i, j \in I$, il existe un élément $k \in I$ tel que $i \leq k$ et $j \leq k$. Un tel ensemble est appelé *directif*.

Définition 1.1.
Soit I un ensemble directif. Un *système projectif* $(X_i, f_{ij})_I$ d'espaces topologiques indexés par I consiste en une famille $\{X_i \mid i \in I\}$ d'espaces topologiques et en une famille $\{f_{ij} : X_j \longrightarrow X_i \mid i, j \in I,\ i \leq j\}$ d'applications continues telles que

(1) f_{ii} est l'identité sur X_i pour tout $i \in I$;

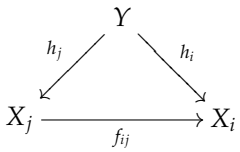
(2) $f_{ij} \circ f_{jk} = f_{ik}$ pour tout $i \leq j \leq k \in I$.

Remarques.

(1) Si aucune topologie n'est spécifée sur une famille d'ensembles, on peut toujours les topologiser en les munissant de la topologie discrète.

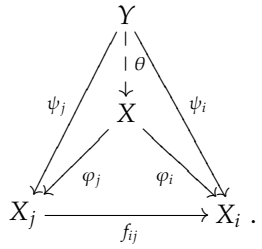
(2) La définition ci-dessus de système projectif, tout comme la définition suivante de limite projective n'est pas valable uniquement dans la catégorie des espaces topologiques, mais peut être généralisée à une catégorie arbitraire.

Si Y est un espace topologique, on appelle une famille d'applications continues $\{h_i : Y \longrightarrow X_i\}_{i \in I}$ *compatible*, si $f_{ij} h_j = h_i$ pour tout $i \leq j$, i.e si le diagramme suivant commute :



Nous pouvons maintenant définir la notion de limite projective par une propriété universelle.

Définition 1.2.
Une *limite projective* (X, φ_i) d'un système projectif $(X_i, f_{ij})_I$ d'espaces topologiques est un espace topologique X muni d'une famille compatible $\{\varphi_i : X \longrightarrow X_i\}_{i\in I}$ d'applications continues satisfaisant la propriété universelle suivante :
pour toute espace topologique Y et pour toute famille compatible $\{\psi_i : Y \longrightarrow X_i\}_{i\in I}$ d'applications continues, il existe une unique application continue $\theta : Y \longrightarrow X$ telle que le diagramme suivant commute pour tout $i \leq j \in I$.



On s'intéresse dans ce travail plus particulièrement au cas où la famille $\{X_i \,|\, i \in I\}$ est constituée de groupes topologiques et la famille $\{f_{ij} \,|\, i, j \in I\}$ d'homomorphismes continus. On remplace alors dans la définition ci-dessus les mots *espace topologique* par les mots *groupe topologique* et les mots *application continue* par les mots *homomorphisme continu*.

Existence et unicité de la limite projective.

On montre d'abord que si la limite projective existe, elle est unique à un unique isomorphisme (au sens catégoriel) près .

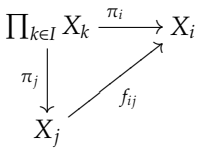
Proposition 1.3 (Unicité).
Soit $(X_i, f_{ij})_I$ un sytème projectif d'espaces topologiques. Si $(X, \varphi_i)_I$ et $(Y, \psi_j)_I$ sont deux limites projectives de $(X_i, f_{ij})_I$, alors il existe un homéomorphisme $\Phi : X \longrightarrow Y$ tel que $\varphi_i\Phi = \psi_i$ pour tout $i \in I$.

Démonstration. La propriété universelle de $(Y, \psi_j)_I$ appliquée à X et à la famille compatible $\{\varphi_i\}_{i\in I}$ fournit une unique application continue $\Phi : X \longrightarrow Y$ telle que $\psi_i\Phi = \varphi_i$ pour tout $i \in I$.
De même, la propriété universelle de $(X, \varphi_i)_I$ appliquée à Y et à la famille compatible $\{\psi_j\}_{j\in I}$ fournit une unique application continue $\Psi : Y \longrightarrow X$ telle que $\varphi_i\Psi = \psi_i$ pour tout $i \in I$.
Ainsi, $\varphi_i\Psi\Phi = \varphi_i$ et pour tout $i \in I$, de plus, $\varphi_i \,\mathrm{id}_X = \varphi_i$ banalement, ainsi, et $\Psi\Phi$ et id_X font commuter le diagramme de la définition et par unicité on a $\Psi\Phi = \mathrm{id}_X$. Similairement, $\Phi\Psi = \mathrm{id}_Y$. Par conséquent $\Phi : X \longrightarrow Y$ est un homéomorphisme (unique). □

On prouve ensuite l'existence de la limite projective en donnant une construction explicite. La preuve est intéressante dans le sens où elle permet de voir la

toplogie que l'on met sur cette construction et motive le choix de définir les limites projectives en particulier pour les espaces topologiques, plutôt que sur une catégorie quelconque.

PROPOSITION 1.4 (Existence).
Soit $(X_i, f_{ij})_I$ un sytème projectif d'espaces topologiques. Notons X l'ensemble des éléments $x \in \prod_{k\in I} X_k$ qui font commuter le diagramme



i.e. tels que $f_{ij}\pi_j(x) = \pi_i(x)$ pour tout $i \leq j \in I$. (Où les π_i sont les projections canoniques.)
Posons $\varphi_i := \pi_i|_X$ pour tout $i \in I$.
Alors $(X, \varphi_i)_I$ est une limite projective de $(X_i, f_{ij})_I$.

DÉMONSTRATION. On munit $\prod_{k\in I} X_k$ de la topologie produit (la vraie !) et X de la topologie induite de sous-espace. Ainsi les applications φ_i sont continues par définition de la topologie produit et $f_{ij}\varphi_j = \varphi_i$ par définition de l'ensemble X. Autrement dit, la famille $\{\varphi_i : X \longrightarrow X_i \,|\, i \in I\}$ est compatible.
Considérons donc une autre famille compatible $\{\psi_i : Y \longrightarrow X_i \,|\, i \in I\}$. Il faut montrer qu'il existe une unique application continue $\theta : Y \longrightarrow X$ telle que $\varphi_i\theta = \psi_i$ pour tout $i \in I$. Posons alors

$$\begin{array}{rccc} \overline{\theta}: & Y & \longrightarrow & \prod_{k\in I} X_k \\ & y & \longmapsto & \{\psi_k(y)\}_{k\in I}\,. \end{array}$$

On a alors $\pi_i\overline{\theta} = \psi_i$ qui est continue pour tout $i \in I$, ce qui équivaut à la continuité de $\overline{\theta}$. En outre, l'image de $\overline{\theta}$ est contenue dans X puisque

$$f_{ij}\pi_j(\overline{\theta}(y)) = f_{ij}\psi_j(y) = \psi_i(y) = \pi_i(\overline{\theta}(y)) \qquad \forall\, i \leq j \in I,\ \forall\, y \in Y\,.$$

On peut donc poser l'application (bien-définie)

$$\begin{array}{rccc} \theta: & Y & \longrightarrow & X \\ & y & \longmapsto & \overline{\theta}(y)\,. \end{array}$$

qui est continue puisque $\overline{\theta}$ l'est ; satisfaisant aussi les relations $\phi_i\theta = \psi_i$ pour tout $i \in I$. L'unicité de θ est immédiate par construction. □

Désormais, on note $\varprojlim X_i$ la limite projective d'un système projectif $(X_i, f_{ij})_I$ au lieu de $(X, \varphi_i)_I$, et $s\varprojlim X_i$ pour la construction particulière de la preuve ci-dessus.

PROPRIÉTÉ 1.5.
La limite projective $s\varprojlim G_i$ d'un système projectif de groupes topologiques $(G_i, f_{ij})_I$ est un groupe topologique.

Démonstration. Le produit cartésien $\prod_{k\in I} G_k$ est un groupe topologique. Le sous-ensemble

$$G = \{g \in \prod_{k\in I} G_k \,|\, f_{ij}\pi_j(g) = \pi_i(g)\ \forall i \leq j\}$$

est clairement non-vide ($1_{\prod_{i\in I} G_i} \in G$) et stable par composition et par inversion puisque tous les f_{ij} et π_k ($i, j, k \in I$) sont des homomorphismes de groupes. De ce fait, G est un sous-groupe de $\prod_{k\in I} G_k$, et donc un groupe topologique pour la topologie induite (en tant que sous-groupe d'un groupe topologique).
Les applications φ_i sont des homomorphismes par définition, puisque les projections le sont. L'application θ de la preuve précédente est aussi un homomorphisme. □

Définition 1.6.
Un *groupe profini* G est un groupe topologique qui est limite projective d'un système projectif $(G_i, f_{ij})_I$ de groupes finis, chacun muni de la topologie discrète.

Dans cette définition chacun des G_i est compact, donc leur produit cartésien sur I l'est aussi et par conséquent $G \cong s\varprojlim G_i$ aussi. Le même argument montre qu'un groupe profini est aussi de Hausdorff et totalement discontinu.
De plus, comme G est en particulier localement compact et totalement discontinu, les sous-groupes ouverts de G forment une base de voisinages de l'élément neutre.

Exemples 1.7.

(1) Les groupes finis munis de la topologie discrète sont profinis.

(2) En théorie algébrique des nombres, si $p \in \mathbb{Z}$ est un nombre premier on peut voir $\mathbb{Z}_p$ comme la limite projective du système projectif $(\mathbb{Z}/p^i\mathbb{Z})$ d'anneaux, indexé sur $\mathbb{N}\setminus\{0\}$, via la bijection

$$\begin{array}{rccc} \theta: & \mathbb{Z}_p & \longrightarrow & s\varprojlim \mathbb{Z}/p^i\mathbb{Z} \\ & x & \longmapsto & \{\varphi_i(x)\}_{i\geq 1} \end{array}$$

où $\varphi_i(x) := \sum_{k=0}^{i-1} a_k p^k + p^i\mathbb{Z}$ si $x = \sum_{k=0}^{\infty} a_k p^k$.
On donne alors à $\mathbb{Z}_p$ une structure d'anneau topologique par transport de la structure d'anneau topologique profini de $s\varprojlim \mathbb{Z}/p^i\mathbb{Z}$ via la bijection θ.

(3) Le groupe de Galois d'une extension galoisienne, développé dans la section suivante.

2. Groupe de Galois d'une extension galoisienne

Une source concrète de groupes profinis est constituée par les groupes de Galois des extensions de corps galoisiennes.
La notation $\mathbb{E}/\mathbb{K}$ désigne dans cette section une extension de corps galoisienne de groupe de Galois $\mathrm{Gal}(\mathbb{E}, \mathbb{K}) = \{\sigma \in \mathrm{Aut}(\mathbb{E}) \,|\, \sigma|_{\mathbb{K}} = \mathrm{id}_{\mathbb{K}}\}$.

On muni $\mathrm{Gal}(\mathbb{E},\mathbb{K})$ de la topologie de Krull, c'est-à-dire la topologie obtenue en prenant pour base de voisinages ouverts de l'identité la famille de sous-groupes

$$\mathcal{N} := \{\mathrm{Gal}(\mathbb{E},\mathbb{L}) \,|\, \mathbb{L} \in F\}$$

où F est la famille de toutes les extensions intermédiaires $\mathbb{L}$ de $\mathbb{E}/\mathbb{K}$ telles que $\mathbb{L}$ est une extension galoisienne finie sur $\mathbb{K}$.

Proposition 1.8.
Le groupe de Galois d'une extension galoisienne $\mathbb{E}/\mathbb{K}$ est profini.

Démonstration. Si l'extension $\mathbb{E}/\mathbb{K}$ est finie, c'est banal car son groupe de Galois est fini.
Supposons donc que $\mathbb{E}/\mathbb{K}$ est une extension infinie. Pour montrer que $\mathrm{Gal}(\mathbb{E},\mathbb{K})$ est profini, il faut montrer qu'il est limite projective de groupe finis.
L'ensemble F est partiellement ordonné par l'inclusion, et le corps composé $\mathbb{F}_1\mathbb{F}_2$ de deux de ses éléments $\mathbb{F}_1$ et $\mathbb{F}_2$ est une extension galoisienne finie de $\mathbb{K}$, donc appartient à F, qui est de ce fait un ensemble directif.
De plus, si $\mathbb{L}_i, \mathbb{L}_j \in F$ avec $\mathbb{L}_i \subseteq \mathbb{L}_j$, on peut considérer les restrictions

$$\begin{array}{rccc} res_{i,j}: & \mathrm{Gal}(\mathbb{L}_j,\mathbb{K}) & \longrightarrow & \mathrm{Gal}(\mathbb{L}_i,\mathbb{K}) \\ & \sigma & \longmapsto & res_{\mathbb{L}_i}(\sigma) \end{array}$$

qui sont des homomorphismes de groupes surjectifs. Alors pour tous $\mathbb{L}_i, \mathbb{L}_j, \mathbb{L}_k \in F$ avec $\mathbb{L}_i \subseteq \mathbb{L}_j \subseteq \mathbb{L}_k$ on a $res_{ij}res_{jk} = res_{ik}$. Ainsi $(\mathrm{Gal}(\mathbb{L}_i,\mathbb{K}), res_{ij})_F$ indexé sur F est un système projectif.
Remarquons que le groupe de Galois de chacun des éléments de F est fini. On a un homomorphisme de groupes

$$\begin{array}{rccc} \theta: & \mathrm{Gal}(\mathbb{E},\mathbb{K}) & \longrightarrow & \prod_{\mathbb{L}\in F}\mathrm{Gal}(\mathbb{L},\mathbb{K}) \\ & \sigma & \longmapsto & \{res_{\mathbb{L}}(\sigma)\}_{\mathbb{L}\in F} \end{array}$$

dont l'image est incluse dans $s\varprojlim_{\mathbb{L}\in F}\mathrm{Gal}(\mathbb{L},\mathbb{K})$. En effet, pour tous $\mathbb{L}_i, \mathbb{L}_j \in F$ avec $\mathbb{L}_i \subseteq \mathbb{L}_j$ et pour tout $\sigma \in \mathrm{Gal}(\mathbb{E},\mathbb{K})$ on a

$$res_{ij}\pi_j(\{res_{\mathbb{L}}(\sigma)\}_{\mathbb{L}\in F}) = res_{ij}(res_{\mathbb{L}_j}(\sigma)) = res_{\mathbb{L}_i}(\sigma) = \pi_i(\{res_{\mathbb{L}}(\sigma)\}_{\mathbb{L}\in F})\ .$$

Il reste à prouver que l'image de θ contient la limite projective $s\varprojlim_{\mathbb{L}\in F}\mathrm{Gal}(\mathbb{L},\mathbb{K})$.
Définissons une application $\varphi : s\varprojlim_{\mathbb{L}\in F}\mathrm{Gal}(\mathbb{L},\mathbb{K}) \longrightarrow \mathrm{Gal}(\mathbb{E},\mathbb{K})$ par

$$\begin{array}{rccc} \varphi(\{\sigma_{\mathbb{L}}\}_{\mathbb{L}\in F}): & \mathbb{E} & \longrightarrow & \mathbb{E} \\ & \alpha & \longmapsto & \sigma_{\mathbb{F}}(\alpha) \end{array}$$

où $\mathbb{F}$ est une extension galoisienne intermédiaire contenant α. (Une telle extension existe toujours dans F, car par exemple $\mathbb{K}[\alpha, x_1, \ldots, x_n]$ où $x_1, \ldots, x_n$ sont les autres racines de $\min(\alpha,\mathbb{K})$ est galoisienne finie sur $\mathbb{K}$.) Cette définition est indépendante du choix de $\mathbb{F}$ car si α appartient à deux extensions galoisiennes intermédiares $\mathbb{F}_1$ et $\mathbb{F}_2$ alors $\alpha \in \mathbb{F}_1\mathbb{F}_2 \in F$. Ainsi

$$res_{\mathbb{F}_1,\mathbb{F}_1\mathbb{F}_2}(\sigma_{\mathbb{F}_1\mathbb{F}_2}(\alpha)) = \sigma_{\mathbb{F}_1}(\alpha)$$

par construction de $s\varprojlim_{\mathbb{L}\in F}\mathrm{Gal}(\mathbb{L},\mathbb{K})$. De même,

$$res_{\mathbb{F}_2,\mathbb{F}_1\mathbb{F}_2}(\sigma_{\mathbb{F}_1\mathbb{F}_2}(\alpha)) = \sigma_{\mathbb{F}_2}(\alpha)\,.$$

Par le même type d'argument, on montre que $\varphi(\{\sigma_{\mathbb{L}}\}_{\mathbb{L}\in F})$ est un homomorphisme de corps, donc injectif et surjectif par normalité de $\mathbb{E}$ et donc un élément de $\mathrm{Gal}(\mathbb{E},\mathbb{K})$.

On vérifie encore que θ et φ sont inverses l'un de l'autre. Pour tout $\sigma \in \mathrm{Gal}(\mathbb{E}, \mathbb{K})$ et pour tout $\alpha \in \mathbb{E}$ on a $\varphi\theta(\sigma)(\alpha) = \varphi(\{res_{\mathbb{L}}\}_{\mathbb{L}\in F})(\alpha) = \sigma(\alpha)$ car il n'y a que des restrictions de σ dans la famille $\{res_{\mathbb{L}}\}_{\mathbb{L}\in F}$. Inversement, pour tout $\{\sigma_{\mathbb{L}}\}_{\mathbb{L}\in F} \in s\varprojlim_{\mathbb{L}\in F} \mathrm{Gal}(\mathbb{L}, \mathbb{K})$ on a $\theta\varphi(\{\sigma_{\mathbb{L}}\}_{\mathbb{L}\in F}) = \{res_{\mathbb{L}}(\varphi(\{\sigma_{\mathbb{L}}\}_{\mathbb{L}\in F}))\}_{\mathbb{L}\in F} = \{\sigma_{\mathbb{L}}\}_{\mathbb{L}\in F}$. Il suit que θ et φ sont des isomorphismes de groupes.
On constate finalement que pour tout $\mathbb{L} \in F$, $\theta(\mathrm{Gal}(\mathbb{E}, \mathbb{L})$ est constitué des éléments de $s\varprojlim_{\mathbb{F}\in F} \mathrm{Gal}(\mathbb{F}, \mathbb{K})$ dont la projection sur $\mathrm{Gal}(\mathbb{L}, \mathbb{K})$ est triviale, autrement dit θ envoie la base de voisinages ouverts de l'identité $\mathcal{N}$ dans $\mathrm{Gal}(\mathbb{E}, \mathbb{K})$ sur une base de voisinages ouverts de l'identité dans $s\varprojlim_{\mathbb{L}\in F} \mathrm{Gal}(\mathbb{L}, \mathbb{K})$. Par suite, θ est un isomorphisme topologique. □

La preuve ci-dessus étant constructive, nous obtenons en corollaire une construction explicite comme limite projective du groupe de Galois d'une extension galoisienne.

Scholie 1.9.
Le groupe $\mathrm{Gal}(\mathbb{E}, \mathbb{K})$ *est limite projective de la famille de groupes finis* $\mathrm{Gal}(\mathbb{L}, \mathbb{K})$ *où* $\mathbb{L}$ *parcourt la famille des extensions galoisiennes finies de* $\mathbb{K}$.

Un résultat plus profond et étonnant est que la proposition ci-dessus admet une réciproque dans le sens où tous les groupes profinis sont des groupes de Galois.

Théorème 1.10.
Tout groupe profini peut se réaliser comme groupe de Galois d'une extension galoisienne, c'est-à-dire, est topologiquement isomorphe à un groupe de Galois d'une extension galoisienne.

Pour une preuve de ce résultat, on peut se référer à [8], Chap. 3, § 3.

CHAPITRE 2

Cohomologie des groupes profinis

Le présent chapitre introduit la notion de groupes de cohomologie d'un groupe profini et développe ensuite la notion de suite exacte longue en cohomologie qui nous sera très utile dans le chapitre suivant. Cette approche de la cohomologie est donnée directement pour les groupes profinis, les définitions et propriétés de base étant essentiellement les mêmes qu'en cohomologie des groupes générale, mais pour les groupe profinis, on s'intéresse aussi à la structure topologique supplémentaire.

1. L'anneau de groupe

Fixons un groupe $(G, \cdot)$, i.e. noté multiplicativement.

Définition 2.1.
L'*anneau de groupe* $\mathbb{Z}G$ (ou $\mathbb{Z}[G]$) est l'ensemble des sommes formelles finies

$$\sum_{g \in G} m_g \cdot g$$

où $m_g \in \mathbb{Z}$ pour tout $g \in G$ et m_g est nul sauf pour un nombre fini d'éléments de G, muni de l'addition

$$(\sum_{g \in G} m_g \cdot g) + (\sum_{g \in G} n_g \cdot g) := \sum_{g \in G} (m_g + n_g) \cdot g$$

et de la multiplication qui est l'unique extension $\mathbb{Z}$-bilinéaire qui prolonge la multiplication de G.

Remarques.

(1) L'anneau $\mathbb{Z}G$ est en fait le groupe libre-abélien de base les éléments de G.

(2) Plus précisément, la multiplication dans $\mathbb{Z}G$ est donnée sur les sommes à un élément par

$$(m_g \cdot g) \cdot (n_h \cdot h) := (m_g n_h) \cdot (gh)$$

pour tout $g, h \in G$ et pour tous $m_g, n_h \in \mathbb{Z}$. On étend alors par $\mathbb{Z}$-bilinéarité pour obtenir l'expression générale

$$(\sum_{g\in G} m_g \cdot g) \cdot (\sum_{h\in G} n_h \cdot h) = \sum_{g,h\in G} (m_g n_h) \cdot gh\,.$$

(3) Pour simplifier les notations on identifie $\mathbb{Z}$ avec $\mathbb{Z} \cdot 1_G$ et par conséquent, si G est le groupe trivial alors $\mathbb{Z}G$ est identifié à $\mathbb{Z}$.
On identifie aussi $1_{\mathbb{Z}G}$ avec 1_G et G à une partie de $\mathbb{Z}G$ en écrivant $g = 1_{\mathbb{Z}} \cdot g$.

Exemples 2.2.

(1) Si $G = C_n =< x \mid x^n = 1 >$ le groupe cyclique d'ordre n, alors $\mathbb{Z}G$ s'dentifie à l'anneau quotient

$$\mathbb{Z}[C^n] \cong \mathbb{Z}[x]/ < x^n - 1 > \ .$$

(2) Si $G = \mathbb{Z}^n$, on l'écrit multiplicativement à l'aide de la présentation

$$< x_1, \ldots, x_n \mid [x_i, x_j] = 1 \ \forall i \neq j \in \mathbb{N}_n > \ .$$

Ainsi $\mathbb{Z}[\mathbb{Z}^n]$ s'identifie avec l'anneau des polynômes de Laurent sur $\mathbb{Z}$ avec n variables

$$\mathbb{Z}[\mathbb{Z}^n] \cong \mathbb{Z}[x_1, x_1^{-1}, \ldots, x_n, x_n^{-1}].$$

2. G-modules

Soit G un groupe quelconque.

Définition 2.3.
Un *G-module* (à gauche) A est un $\mathbb{Z}G$-module (à gauche), i.e. un groupe abélien A muni d'une action de $\mathbb{Z}G$ sur A.
Un G-module A est dit *trivial* si l'action de G sur A est triviale, c'est-à-dire $g \cdot a = a$ pour tout $g \in G$ et $a \in A$, donc $(\sum_{g\in G} m_g g) \cdot a = (\sum_{g\in G} m_g) \cdot a$ pour tout $g \in G$ et $a \in A$.

Sachant qu'étant donné un anneau R ainsi qu'un homomorphisme de groupes $\varphi : G \longrightarrow R^*$, il existe une unique extension de φ en un homomorphisme d'anneaux $\mathbb{Z}G \longrightarrow R$, on obtient une correspondance bijective

$$\mathrm{Hom}_{(anneaux)}(\mathbb{Z}G, R) \approx \mathrm{Hom}_{(groupes)}(G, R^*)\,.$$

Alors, l'action de $\mathbb{Z}G$ sur A étant un homomorphisme de $\mathbb{Z}G$ dans l'anneau des endomorphismes de A, elle correspond à un homomorphisme de G dans le groupe des automorphisme de A. Par conséquent, on peut simplement voir un G-module comme un groupe abélien A muni d'une action de G sur A.

Définition 2.4.
Si G est un groupe topologique et A un G-module qui est aussi un groupe topologique, alors on dit que A est un *G-module topologique* si l'action $G \times A \longrightarrow A$ de G sur A est une application continue.
Si G est un groupe profini, un *G-module profini* est une limite projective de G-modules finis et d'homomorphismes de G-modules.

Remarques.

(1) On peut voir n'importe quel groupe abélien topologique A comme un G-module topologique en définissant l'action de G sur A comme étant triviale.

(2) On montre assez facilement que tout G-module profini est un G-module topologique. En effet, écrivons $A = \varprojlim_{i\in I} A_i$ comme limite projective avec la famille associée d'homomorphismes continus $\{\varphi_i : A \longrightarrow A_i\}_{i\in I}$. On muni alors A d'une structure de G-module en posant pour tout $\{a_i\}_{i\in I} \in s\varprojlim_{i\in I} A_i$ et tout $g \in G$ l'action $g\cdot\{a_i\} := \{ga_i\}$. Cette application est continue puisque le produit avec chacune des applications φ_i est continu. Pour tout $i \in I$, $\varphi_i(ga) = g\varphi_i(a)$ pour tout $g \in G$ et tout $a \in A$. Ainsi, les applications φ_i sont des homomorphismes continus. Et l'application $G \times A \longrightarrow A$ est continue puisque son produit avec chacun des φ_i est continu. Ainsi A est un G-module topologique.

Si G est un groupe profini, un G-module A muni de la topologie discrète est appelé un G-module *discret* si A est un G-module topologique, i.e. si l'action de G sur A est continue.

Les exemples de G-modules discrets qui nous intéressent pour accéder à l'énoncé de la conjecture de Milnor proviennent de façon naturelle de la théorie de Galois. Si $\mathbb{E}/\mathbb{K}$ est une extension de corps galoisienne et $G = \mathrm{Gal}(\mathbb{E}, \mathbb{K})$, alors G agit à gauche sur $\mathbb{E}$ par $\sigma \cdot \alpha := \sigma(\alpha)$ pour tout $\sigma \in G$ et pour tout $\alpha \in \mathbb{E}$. Plus précisément, par cette action, les groupes suivants constitués d'éléments de $\mathbb{E}$ sont des G-modules discrets :

(1) le groupe additif $(\mathbb{E}, +)$;

(2) le groupe multiplicatif des unités $(\mathbb{E}^*, \cdot)$;

(3) le groupe des racines n-ièmes de l'unité dans $\mathbb{E}$.

3. Définition des groupes de cohomologie

Soit G un groupe profini et A un G-module topologique. Pour simplifier, dans le reste du chapitre *module* signifiera *module topologique*.
Pour tout entier $n > 0$ on munit $G^{(n)} = G \times \cdots \times G$ (n fois) de la topologie produit et on pose

$$C^0(G, A) := A\,;$$

$C^n(G,A) :=$ ensemble des applications continues de $G^{(n)}$ vers A, $\forall\ n > 0$.
Les éléments de $C^n(G,A)$ sont appelés les *n-cochaînes*. On donne, de plus, à $C^n(G,A)$ une structure de groupe abélien en additionnant les applications composante par composante. En fait, pour $n = 0$, $G^{(n)} = 0$ le groupe trivial et donc $C^0(G,A)$ est canoniquement isomorphe au groupe des applications de 0 dans A.

Définissons maintenant pour tout $n \geq 1$ un homomorphisme de groupes $d^n : C^n(G,A) \longrightarrow C^{n+1}(G,A)$ par

$$(d^n g)(x_1, \cdots, x_{n+1}) := x_1 g(x_2, \cdots, x_{n+1}) + \sum_{k=1}^{n} (-1)^k g(x_1, \ldots, x_k x_{k+1}, \ldots, x_{n+1}) + (-1)^{n+1} g(x_1, \cdots, x_n)$$

pour tout $g \in C^n(G,A)$ et tout $(x_1, \cdots, x_{n+1}) \in G^{(n+1)}$. Pour $n = 0$, on définit l'homomorphisme $d^0 : C^0(G,A) = A \longrightarrow C^1(G,A)$ par $d^0(a)(x) := x \cdot a - a$ pour tout $a \in A$ et tout $x \in G$, qui est compatible avec la définition de d^n ci-dessus.

Lemme 2.5.
Pour tout $n \geq 0$, d^n est effectivement un homomorphisme de groupes et de plus $d^{n+1} d^n = 0$.

Démonstration. Le fait que chaque d^n est un homomorphisme de groupes est claire et le fait que $d^{n+1} d^n = 0$ est un long calcul peu intéressant, omis ici car il se trouve dans tout bon livre d'introduction à la cohomologie des groupes. □

En conséquence de ce lemme on obtient que les d^n sont les différentielles d'un complexe de cochaînes $(C^n(G,A), d^n)$, où l'on considère les termes et les différentielles de degré négatif comme étant égaux à 0. On va donc pouvoir prendre ses groupes de cohomologie au sens de l'algèbre homologique.

Définition 2.6.

(1) On appelle groupe des *n-cocycles* de G, le groupe[1] $Z^n(G,A) := \operatorname{Ker} d^n$ et on appelle groupe des *n-cobords* de G le groupe $B^n(G,A) := \operatorname{Im} d^{n-1}$. Le lemme précédent entraîne que $B^n(G,A)$ est un sous-groupe de $Z^n(G,A)$.
(2) On définit le *n-ième groupe de cohomologie de G à coefficients dans A* comme étant le groupe quotient

$$H^n(G,A) := Z^n(G,A)/B^n(G,A) = \operatorname{Ker} d^n / \operatorname{Im} d^{n-1} .$$

Pour $n = 0$, on obtient

$$H^0(G,A) \cong Z^0(G,A) = \{a \in A \mid d^0(a) = 0\} = \{a \in A \mid x \cdot a - a = 0\ \forall\ x \in G\} .$$

Par conséquent, $H^0(G,A)$ est canoniquement isomorphe au groupe A^G des points fixes de A sous l'action de G.

[1] De l'allemand "Zykel".

4. Suite exacte longue en cohomologie

Dans cette section, nous développons un outil très utilisé en cohomologie des groupes : la suite exacte longue induite en cohomologie par une suite exacte courte de G-modules. Il s'agit de l'outil crucial pour comprendre l'isomorphisme du corollaire 3.5 qui nous donnera accès à l'énoncé de la conjecture de Milnor, c'est pourquoi nous prenons le temps d'examiner les détails des preuves. Fixons donc G un groupe profini.

On dira qu'une suite exacte courte de G-modules $0 \longrightarrow A \xrightarrow{i} B \xrightarrow{j} C \longrightarrow 0$ est *bien-ajustée* si l'application i est un homéomorphisme de A dans son image et s'il existe une application continue $\tau : C \longrightarrow B$ telle que $j\tau = \mathrm{id}_C$. Nous allons voir que cette hypothèse supplémentaire sur les suites exactes courtes va nous permettre de prouver l'existence de la suite exacte longue en cohomologie.
Notons que dans le chapitre suivant les suites exactes considérées seront composées uniquement de G-modules discrets, alors la condition d'être bien-ajustée est automatiquement vérifiée. Le fait que i est un homéomorphisme sur son image est clair si les topologies de A et de B sont discrètes. Quant à l'existence de l'application continue τ, on peut par exemple se référer à N. Bourbaki au chapitre concernant les groupes topologiques.

Théorème 2.7.
Soit $0 \longrightarrow A \xrightarrow{i} B \xrightarrow{j} C \longrightarrow 0$ *une suite exacte courte bien-ajustée de G-modules. Alors il existe une suite exacte longue en cohomologie :*

$$0 \longrightarrow A^G \xrightarrow{i^*} B^G \xrightarrow{j^*} C^G \xrightarrow{\partial^0} H^1(G,A) \xrightarrow{i^*} H^1(G,B) \longrightarrow \cdots$$

$$\cdots \longrightarrow H^n(G,B) \xrightarrow{j^*} H^n(G,C) \xrightarrow{\partial^n} H^{n+1}(G,A) \longrightarrow \cdots$$

La preuve de ce théorème se fait aux travers de plusieurs petits lemmes constructifs. Mais pour commencer, on explique la notion d'homomorphisme induit (par un homomorphisme continu de G-modules) sur les groupes de cochaînes et sur les groupes de cohomologie, ce qui expliquera en particulier les notations i^* et j^* dans le théorème.

Soit $f : B \longrightarrow A$ un homomorphisme continu de G-modules. Pour tout entier $n \geq 0$, f induit un homomorphisme de groupes

$$f^{\#} : C^n(G,B) \longrightarrow C^n(G,A)$$

défini par $(f^{\#}g)(x_1,\ldots,x_n) := fg(x_1,\ldots,x_n)$ pour tout $(x_1,\ldots,x_n) \in G^n$ et tout $g \in C^n(G,B)$. Il est clair qu'il s'agit bien d'un homomorphisme et la continuité pour tout $g \in C^n(G,B)$ de l'application $f^{\#}(g)$ vient du fait que f et g sont des applications continues. De plus, cet homomorphisme induit commute avec les différentielles.

LEMME 2.8.
Pour tout entier $n \geq 0$, le diagramme

$$\begin{array}{ccc} C^n(G,B) & \xrightarrow{d^n} & C^{n+1}(G,B) \\ \downarrow{\scriptstyle f^\#} & & \downarrow{\scriptstyle f^\#} \\ C^n(G,A) & \xrightarrow{d^n} & C^{n+1}(G,A) \end{array}$$

commute.

DÉMONSTRATION. Soit $g \in C^n(G,B)$ et $(x_1,\dots,x_{n+1}) \in G^{n+1}$, alors

$$\begin{aligned}(d^n f^\# g)(x_1,\dots,x_{n+1}) &= x_1[(f^\# g)(x_2,\dots,x_{n+1})] + \dots + (-1)^{n+1}(f^\# g)(x_1,\dots,x_n) \\ &= x_1[fg(x_2,\dots,x_{n+1})] + \dots + (-1)^{n+1} fg(x_1,\dots,x_n) \\ &= f[x_1 g(x_2,\dots,x_{n+1}) + \dots + (-1)^{n+1} g(x_1,\dots,x_n)] \\ &= f d^n g(x_1,\dots,x_{n+1}) = (f^\# d^n g)(x_1,\dots,x_{n+1})\end{aligned}$$

□

Cette propriété de l'homomorphisme induit de commuter avec les différentielles nous permet de définir un autre homomorphisme induit sur les groupes de cohomologie. Soit $n \geq 0$ et $g \in Z^n(G,B)$, alors $d^n f^\# g = f^\# d^n g = 0$ donc $f^\# g \in Z^n(G,A)$ ainsi on obtient une application

$$Z^n(G,B) \longrightarrow Z^n(G,A) \xrightarrow{can} H^n(G,A)\,,$$

dont le noyau contient $B^n(G,B)$. En effet si $h \in B^n(G,B)$, il existe $k \in C^{n-1}(G,B)$ tel que $h = d_{n-1}k$ et donc $f^\# h = f^\# d_{n-1}k = d_{n-1} f^\# k \in B_n(G,A)$ et donc en passant au quotient, $f^\# h$ est nul. Par conséquent il existe un homomorphisme induit en cohomologie (par la propriété universelle du quotient) :

$$\begin{array}{rccc} f^* : & H^n(G,B) & \longrightarrow & H^n(G,A) \\ & g + B^n(G,B) & \longmapsto & f^\# g + B^n(G,B)\,. \end{array}$$

REMARQUE 2.9.
Il est clair par définitions que si $f_2 : C \longrightarrow B$ et $f_1 : B \longrightarrow A$ sont des homomorphismes continus de G-modules, alors $(f_1 f_2)^\# = f_1^\# f_2^\#$ et donc $(f_1 f_2)^* = f_1^* f_2^*$. De plus, id^* est l'identité en cohomologie. Par conséquent $H^n(G,-)$ est un foncteur covariant de la catégorie des G-modules à gauche dans la catégorie des groupes abéliens.

LEMME 2.10.
Soit $0 \longrightarrow A \xrightarrow{i} B \xrightarrow{j} C \longrightarrow 0$ une suite exacte courte bien-ajustée de G-modules. Alors la suite induite sur les cochaînes

$$0 \longrightarrow C^n(G,A) \xrightarrow{i^\#} C^n(G,B) \xrightarrow{j^\#} C^n(G,C) \longrightarrow 0$$

est exacte pour tout $n \geq 0$.

DÉMONSTRATION. Le noyau de $i^\#$ est trivial car si $g \in C^n(G,A)$ avec $i^\# g = 0$ alors $ig = 0$ et donc $g = 0$ par injectivité de i.

Pour l'exactitude en $C^n(G,B)$ on a d'abord $j^\# i^\# = (ji)^\# = 0$ donc $\operatorname{Im} i^\# \leq \operatorname{Ker} j^\#$. Pour l'autre inclusion on utilise le fait que la suite est bien-ajustée et on écrit $\tilde{\imath}$ l'inverse de l'homéomorphisme de A dans $\operatorname{Im} i$, ainsi $i\tilde{\imath}$ est l'identité sur $\operatorname{Im} i$. Si $g \in \operatorname{Ker} j^\#$, i.e. $jg = 0$, ainsi $\operatorname{Im} g \leq \operatorname{Ker} j = \operatorname{Im} i$ dans B et on peut considérer g comme une application à image dans $\operatorname{Im} i$ par restriction de son codomaine. Par suite, $\tilde{\imath} g \in C^n(G,A)$ et $i^\#(\tilde{\imath} g) = i\tilde{\imath} g = \mathrm{id}\, g = g$ et donc $\operatorname{Ker} j^\# \leq \operatorname{Im} i^\#$.
La surjectivité de $j^\#$ découle de l'existence de l'application continue $\tau : C \longrightarrow B$ telle que $j\tau = \mathrm{id}_C$. En effet, pour tout $g \in C^n(G,C)$, $\tau g \in C^n(G,B)$ et $j^\#(\tau g) = j\tau g = g$. □

Avec cette suite exacte sur les groupes de cochaînes en mains, on peut passer à la preuve du théorème 2.7 à proprement parler. On commence par montrer l'exactitude en $H^n(G,B)$ pour tout $n \geq 0$.

Lemme 2.11.
Le morceau de suite $H^n(G,A) \xrightarrow{i^*} H^n(G,B) \xrightarrow{j^*} H^n(G,C)$ *est exact pour tout* $n \geq 0$.

Démonstration. Premièrement, $j^* i^* = (ji)^* = 0$ donc $\operatorname{Im} i^* \leq \operatorname{Ker} j^*$. Il reste à montrer l'inclusion inverse. Soit $g \in Z^n(G,B)$ tel que $g + B^n(G,B) \in \operatorname{Ker} j^*$. Alors $j^\# g \in B^n(G,C)$ donc il existe $f \in C^{n-1}(G,C)$ tel que $j^\# g = d^{n-1} f$. Par exactitude de la suite du lemme précédent, il existe $h \in C^{n-1}(G,B)$ tel que $f = j^\# h$. Donc

$$j^\# g = d^{n-1} f = d^{n-1} j^\# h = j^\# d^{n-1} h\,,$$

d'où $j^\#(g - d^{n-1}h) = 0$. Ainsi $(g - d^{n-1}h) \in \operatorname{Ker} j^\# = \operatorname{Im} i^\#$ et donc il existe $k \in C^n(G,A)$ avec $i^\# k = g - d^{n-1}h$. Il vient

$$i^\# d^n k = d^n i^\# k = d^n(g - d^{n-1}h) = d^n g = 0$$

puisque $g \in Z^n(G,B)$ et par injectivité de $i^\#$ on obtient $d^n k = 0$. Par conséquent, $k + B^n(G,A) \in H^n(G,A)$ et finalement

$$g + B^n(G,B) = i^\# k + d^{n-1}h + B^n(G,B) = i^\# k + B^n(G,B) = i^*(k + B^n(G,A)) \in \operatorname{Im} i^*\,.$$

□

Il reste à montrer que l'on peut lier de manière exacte $H^n(G,C)$ à $H^{n+1}(G,A)$.

Lemme 2.12.
Il existe pour tout $n \geq 0$ *un homomorphisme*

$$\partial^n : H^n(G,C) \longrightarrow H^{n+1}(G,A)\,,$$

appelé homomorphisme connectant, qui rend exacte la suite

$$H^n(G,B) \xrightarrow{j_n} H^n(G,C) \xrightarrow{\partial^n} H^{n+1}(G,A) \xrightarrow{i_{n+1}} H^{n+1}(G,B)\,.$$

Démonstration. Cette preuve est une grande chasse au diagramme dans le diagramme commutatif suivant :

$$\begin{array}{ccccccc}
0 & & 0 & & 0 & & 0 \\
\downarrow & & \downarrow & & \downarrow & & \downarrow \\
C^{n-1}(G,A) & \xrightarrow{d^{n-1}} & C^n(G,A) & \xrightarrow{d^n} & C^{n+1}(G,A) & \xrightarrow{d^{n+1}} & C^{n+2}(G,A) \\
\downarrow{\scriptstyle i^\#} & & \downarrow{\scriptstyle i^\#} & & \downarrow{\scriptstyle i^\#} & & \downarrow{\scriptstyle i^\#} \\
C^{n-1}(G,B) & \xrightarrow{d^{n-1}} & C^n(G,B) & \xrightarrow{d^n} & C^{n+1}(G,B) & \xrightarrow{d^{n+1}} & C^{n+2}(G,B) \\
\downarrow{\scriptstyle j^\#} & & \downarrow{\scriptstyle j^\#} & & \downarrow{\scriptstyle j^\#} & & \downarrow{\scriptstyle j^\#} \\
C^{n-1}(G,C) & \xrightarrow{d^{n-1}} & C^n(G,C) & \xrightarrow{d^n} & C^{n+1}(G,C) & \xrightarrow{d^{n+1}} & C^{n+2}(G,C) \\
\downarrow & & \downarrow & & \downarrow & & \downarrow \\
0 & & 0 & & 0 & & 0
\end{array}$$

Soit $c_n \in Z^n(G,C)$. Par exactitude de la deuxième colonne, il existe $b_n \in C^n(G,B)$ tel que $c_n = j^\# b_n$ et $0 = d^n(c_n) = d^n j^\# b_n = j^\# d^n b_n$, donc $d^n b_n \in \operatorname{Ker} j^\# = \operatorname{Im} i^\#$. Ainsi il existe $a_{n+1} \in C^{n+1}(G,A)$ tel que $d^n b_n = i^\# a_{n+1}$. D'où

$$i^\# d^{n+1} a_{n+1} = d^{n+1} i^\# a_{n+1} = d^{n+1} d^n b_n = 0$$

et par injectivité de $i^\#$, $d^{n+1} a_{n+1} = 0$, ainsi $a_{n+1} \in Z^{n+1}(G,A)$. On a donc trouvé un moyen de définir une application

$$\begin{array}{rccc}
\partial^n : & H^n(G,C) & \longrightarrow & H^{n+1}(G,A) \\
& c_n + B^n(G,C) & \longmapsto & a_{n+1} + B^{n+1}(G,A)\,.
\end{array}$$

Il faut vérifier que ∂^n est bien définie. Supposons que $c'_n \in (c_n + B^n(G,C))$ et que $b'_n \in C^n(G,B)$ tel que $c'_n = j^\# b'_n$, alors il existe $a'_{n+1} \in C^{n+1}(G,A)$ tel que $d^n b'_n = i^\# a'_{n+1}$. Il existe $c_{n-1} C^{n-1}(G,C)$ tel que $c'_n - c_n = d^{n-1} c_{n-1}$ et par exactitude de la première colonne, il existe $b_{n-1} C^{n-1}(G,B)$ tel que $c_{n-1} = j^\# b_{n-1}$ et donc

$$j^\# d^{n-1} b_{n-1} = d^{n-1} j^\# b_{n-1} = d^{n-1} c_{n-1} = c - n' - c_n = j^\# b'_n - j^\# b_n = j^\#(b'_n - b_n)\,.$$

Donc $b'_n - b_n - d^{n-1} b_{n-1} \in \operatorname{Ker} j^\# = \operatorname{Im} i^\#$ et il existe $a_n \in C^n(G,A)$ tel que

$$b'_n - b_n - d^{n-1} b_{n-1} = i^\# a_n\,.$$

Il vient

$$i^\# d^n a_n = d^n i^\# a_n = d^n(b'_n - b_n - d^{n-1} b_{n-1}) = d^n b'_n - d^n b_n = i^\# a'_{n+1} - i^\# a_{n+1}\ .$$

Par injectivité de $i^\#$ on a $d^n a_n = a'_{n+1} - a_{n+1}$ et donc $a'_{n+1} - a_{n+1} \in B^{n+1}(G,A)$, d'où $a'_{n+1} + B^{n+1}(G,A) = a_{n+1} + B^{n+1}(G,A)$, ce qui prouve que ∂^n est bien défini.
Que ∂^n est un homomorphisme de groupes découle du fait que toutes les flèches du diagramme sont des homomorphismes. En effet, si $c_n, c'_n \in Z^n(G,C)$, alors par le processus de construction de ∂_n, il existe $b_n, b'_n \in C^n(G,B)$ tels que $c_n = j^\# b_n$ et $c'_n = j^\# b'_n$, d'où $c_n + c'_n = j^\#(b_n + b'_n)$. Il existe $a_{n+1}, a'_{n+1} \in C^{n+1}(G,A)$ tel que $d^n b_n = i^\# a_{n+1}$

et $d^n b'_n = i^\# a'_{n+1}$, ainsi $d^n(b_n + b'_n) = i^\#(a_{n+1} + a'_{n+1})$. On obtient donc

$$\begin{aligned}\partial^n(c_n + B^n(G,C)) + \partial^n(c'_n + B^n(G,C)) &= a_{n+1} + B^{n+1}(G,A) + a'_{n+1} + B^{n+1}(G,A)\\ &= (a_{n+1} + a'_{n+1}) + B^{n+1}(G,A)\\ &= \partial^n((c_n + c'_n) + B^n(G,C))\,.\end{aligned}$$

Il reste encore à montrer l'exactitude de la suite en $H^n(G,C)$ et $H^{n+1}(G,A)$.
Soit $c_n + B^n(G,C) \in \operatorname{Ker}\partial^n$, alors

$$\partial^n(c_n + B^n(G,C)) = a_{n+1} + B^{n+1}(G,A)$$

avec $a_{n+1} \in B^{n+1}(G,A)$. Il existe donc $a_n \in C^n(G,A)$ tel que $d^n a_n = a_{n+1}$. Par la construction ci-dessus, il existe aussi $b_n \in C^n(G,B)$ tel que

$$d^n b_n = i^\# a_{n+1} = i^\# d^n a_n = d^n i^\# a_n\,,$$

autrement dit $b_n - i^\# a_n \in Z^n(G,B)$ et donc $j^\#(b_n - i^\# a_n) = j^\# b_n = c_n$. On a donc en cohomologie

$$c_n + B^n(G,C) = j^\#(b_n - i^\# a_n) + B^n(G,C) = j^*(b_n - i^\# a_n + B^n(G,C))\,.$$

Par conséquent, $\operatorname{Ker}\partial^n \leq \operatorname{Im} j^*$. Soit maintenant $c_n + B^n(G,C) \in \operatorname{Im} j^*$, il existe $b_n \in Z^n(G,B)$ tel que $j^\# b_n = c_n$, alors $d^n b_n = 0$ et de ce fait, on peut choisir $a_{n+1} = 0$ dans la définition ci-dessus de ∂^n et donc $\operatorname{Im} j^* \leq \operatorname{Ker}\partial^n$.
Passons à l'exactitude en $H^{n+1}(G,A)$. Soit $c_n + B^n(G,C) \in H^n(G,C)$ ainsi que b_n et a_{n+1} comme dans la construction ci-dessus de $\partial^n(c_n + B^n(G,C))$. On veut voir que ce dernier est dans le noyau de i^*. On a

$$i^*\partial^n(c_n + B^n(G,C)) = i^\# a_{n+1} + B^{n+1}(G,B) = d^n b_n + B^{n+1}(G,B) = B^{n+1}(G,A),$$

d'où $\operatorname{Im}\partial^n \leq \operatorname{Ker} i^*$. Soit maintenant $a_{n+1} + B^{n+1}(G,A) \in \operatorname{Ker} i^*$, alors $i^\# a_{n+1} \in B^{n+1}(G,B)$ et donc il existe $b_n \in C^n(G,B)$ tel que $i^\# a_{n+1} = d^n b_n$. Toujours par la construction de ∂^n, on obtient

$$a_{n+1} + B^{n+1}(G,A) = \partial^n(j^\# b_n + B^{n+1}(G,C)) \in \operatorname{Im}\partial^n\ .$$

Ainsi, finalement $\operatorname{Ker} i^* \in \operatorname{Im}\partial^n$. □

Ceci termine en même temps la preuve du théorème 2.7.

CHAPITRE 3

Un minimum de Cohomologie Galoisienne

Fixons un corps $\mathbb{K}$ et soit $\mathbb{E}/\mathbb{K}$ est une extension de corps galoisienne. Nous avons vu au chapitre précédent que le groupe de Galois $\mathrm{Gal}(\mathbb{E}, \mathbb{K})$ de cette extension est un groupe profini. Nous pouvons donc lui appliquer les notions de cohomologie des groupes profinis développées précédemment.

1. Clôture séparable d'un corps

Définition 3.1.
Soit $\mathbb{E}$ une extension algébrique d'un corps $\mathbb{K}$. Le sous-ensemble

$$\mathbb{E}_0 := \{\alpha \in \mathbb{E} \mid \alpha \text{ est séparable sur } \mathbb{K}\}$$

de $\mathbb{E}$ s'appelle la *clôture séparable* de $\mathbb{K}$ dans $\mathbb{E}$.
Plus particulièrement, si $\mathbb{E} = \overline{\mathbb{K}}$, une clôture algébrique de $\mathbb{K}$, alors on appelle $\mathbb{E}_0$ une *clôture séparable de* $\mathbb{K}$, que l'on notera par la suite $\mathbb{K}_s$.

Une clôture séparable $\mathbb{K}_s$ d'un corps $\mathbb{K}$ est plus précisément un sous-corps de sa clôture algébrique $\overline{\mathbb{K}}$ (contenant tous les éléments séparables sur $\mathbb{K}$). En effet, pour tout $\alpha, \beta \in \mathbb{K}_s$, alors $\mathbb{K}[\alpha, \beta]$ est une extension séparable, puisqu'engendrée par des éléments séparables. Ainsi $\alpha \pm \beta, \alpha \cdot \beta, \alpha^{-1} \in \mathbb{K}[\alpha, \beta]$. Par conséquent, $\mathbb{K}_s$ est un sous-corps de $\overline{\mathbb{K}}$ puisqu'il est stable par addition, multiplication, inversion et contient $1_{\mathbb{K}}$.
Par définition $\mathbb{K}_s/\mathbb{K}$ est une extension séparable. De plus, tout polynôme irréductible de $\mathbb{K}[X]$ ayant une racine dans $\mathbb{K}_s$ est séparable et donc a toutes ses racines dans $\mathbb{K}_s$. Ainsi $\mathbb{K}_s/\mathbb{K}$ est aussi une extension normale, donc galoisienne.
En outre, le corps $\mathbb{K}_s$ est, par définition, une extension séparable maximale de $\mathbb{K}$, ainsi, par transitivité de la séparabilité, toute extension séparable de $\mathbb{K}_s$ est une extension séparable de $\mathbb{K}$ et donc égal à $\mathbb{K}_s$. En d'autres termes, $\mathbb{K}_s$ est un corps séparablement clos.
Notons aussi que l'unicité à isomorphisme près de la clôture algébrique de $\mathbb{K}$ entraîne l'unicité à isomorphisme près de la clôture séparable de $\mathbb{K}$. Ceci justifie la notation $\mathbb{K}_s$.

Remarque 3.2.
Considérons un entier $n \geq 1$, alors, si la caractéristique de $\mathbb{K}$ est nulle ou première

à n, il y a n racines n-ième de l'unité distinctes dans $\overline{\mathbb{K}}$, en fait toutes contenues dans la clôture séparable $\mathbb{K}_s$.

En effet, une racine n-ième de l'unité est une racine du polynôme $X^n - 1$, dont la dérivée est $D(X^n - 1) = nX^{n-1} \neq 0$ en caractéristique nulle ou première à n ; elle n'est ainsi pas racine de la dérivée et, de ce fait, simple, i.e contenue dans $\mathbb{K}_s$.

Lemme 3.3.
Soit $n \geq 1$ un entier. Si $\mathbb{K}$ est un corps de caractéristique 0 ou première à n. Alors l'endomorphisme

$$\begin{array}{ccc} (\mathbb{K}_s)^* & \xrightarrow{n} & (\mathbb{K}_s)^* \\ x & \longmapsto & x^n \end{array}$$

est surjectif.

Démonstration. Montrer la surjectivité de cet endomorphisme revient à montrer que que le polynôme $X^n - a \in \mathbb{K}_s[X]$ possède une racine dans $\mathbb{K}_s$ pour tout $a \in (\mathbb{K}_s)^*$.
Il s'agit exactement du même argument que ci-dessus, la dérivée est $D(X^n - a) = nX^{n-1} \neq 0$ vu l'hypothèse sur la caractéristique. Il en découle que toutes les racines de $X^n - a$ sont simples, vu qu'elles ne sont pas racines de $D(X^n - a)$. Par conséquent, $X^n - a$ a toutes ses racines dans $\mathbb{K}_s$, d'où surjectivité. □

2. Notations

On considère de manière générale une extension galoisienne $\mathbb{E}/\mathbb{K}$, finie ou infinie. Le but de la cohomologie galoisienne est d'étudier les groupes de cohomologie du groupe de Galois $\mathrm{Gal}(\mathbb{E}, \mathbb{K})$ de l'extension $\mathbb{E}/\mathbb{K}$ à coefficient dans un $\mathrm{Gal}(\mathbb{E}, \mathbb{K})$-module, appelés *groupes de cohomologie galoisienne* de l'extension $\mathbb{E}/\mathbb{K}$.

On adopte alors les quelques notations suivantes : on note $H^q(\mathbb{E}/\mathbb{K}, A)$ au lieu de $H^q(\mathrm{Gal}(\mathbb{E}, \mathbb{K}), A)$ le q-ième groupe de cohomologie à coefficients dans A du groupe de Galois de l'extension $\mathbb{E}/\mathbb{K}$.

En particulier, on peut montrer que deux clôtures séparables de $\mathbb{K}$ définissent des groupes de cohomologie galoisienne en correspondance bijective. Dans ce cas, les notations en usage veulent que l'on laisse tomber la spécification de l'extension, pour noter simplement $H^n(\mathbb{K}, A)$ au lieu de $H^n(\mathbb{K}_s/\mathbb{K}, A)$.

De plus on note G_m pour le groupe multiplicatif $\mathbb{E}^*$ ainsi que G_a pour le groupe additif $(\mathbb{E}, +)$.

3. Calcul de $H^1(\mathbb{K}, \mu_n)$

La clé du calcul annoncé dans le titre ci-dessus réside dans la proposition suivante, souvent appelée *Théorème 90 de Hilbert cohomologique*.

Proposition 3.4.
Soit $\mathbb{E}/\mathbb{K}$ *une extension galoisienne , alors* $H^1(\mathbb{E}/\mathbb{K}, G_m) = 0$ *et* $H^q(\mathbb{E}/\mathbb{K}, G_a) = 0$ *pour tout* $q \geq 1$.

Démonstration. On démontre ici seulement la première partie de la proposition, concernant le groupe multiplicatif G_m de $\mathbb{E}$, que nous utilisons dans le corollaire suivant. Pour la partie $H^q(\mathbb{E}/\mathbb{K}, G_a) = 0$ pour tout $q \geq 1$ on se réfère par exemple à [6], Chap. IV, §1.
Montrer que $H^1(\mathbb{E}/\mathbb{K}, G_m)$ est trivial revient à montrer que

$$Z^1(\mathbb{E}/\mathbb{K}, G_m) \subseteq B^1(\mathbb{E}/\mathbb{K}, G_m)\,,$$

l'inclusion inverse étant vérifiée automatiquement.
Soit $f \in B^1(\mathbb{E}/\mathbb{K}, G_m)$ un 1-cobord, alors il existe $a \in \mathbb{E}^*$ tel que $f = d^0(a)$, ainsi f est une application de $G \longrightarrow \mathbb{E}^*$ définie par $f(\sigma) = \sigma(a) \cdot a^{-1}$ pour tout $\sigma \in \mathrm{Gal}(\mathbb{E}, \mathbb{K})$.
Soit $g \in Z^1(\mathbb{E}/\mathbb{K}, G_m)$ un 1-cocycle, i.e. $d^1(g) = 0$ dans $C^2(\mathbb{E}/\mathbb{K}, G_m)$. Ainsi, pour tous $\sigma, \tau \in \mathrm{Gal}(\mathbb{E}, \mathbb{K})$ on a

$$1_{\mathbb{E}} = d^1(g)(\sigma, \tau) = \sigma g(\tau) \cdot g(\sigma\tau)^{-1} \cdot g(\sigma)\,.$$

D'où

$$g(\sigma\tau) = \sigma g(\tau) \cdot g(\sigma) \tag{1}$$

pour tous $\sigma, \tau \in \mathrm{Gal}(\mathbb{E}, \mathbb{K})$. Cette propriété nous permet de montrer que tout 1-cocycle est un 1-cobord. Le lemme de Dedekind sur l'indépendance linéaire des automorphismes entraîne qu'il existe $\alpha \in \mathbb{E}^*$ tel que

$$0 \neq \sum_{\tau \in \mathrm{Gal}(\mathbb{E}, \mathbb{K})} g(\tau)\tau(\alpha) =: \beta$$

Ainsi, pour tout $\sigma \in \mathrm{Gal}(\mathbb{E}, \mathbb{K})$ on a

$$\sigma(\beta) = \sum_{\tau \in \mathrm{Gal}(\mathbb{E}, \mathbb{K})} \sigma g(\tau) \cdot \sigma\tau(\alpha)\,.$$

Et donc en multipliant par $g(\sigma) \in \mathbb{E}^*$ il vient

$$\begin{aligned} g(\sigma) \cdot \sigma(\beta) &= \sum_{\tau \in \mathrm{Gal}(\mathbb{E}, \mathbb{K})} g(\sigma) \cdot \sigma g(\tau) \cdot \sigma\tau(\alpha) \\ &\overset{(1)}{=} \sum_{\tau \in \mathrm{Gal}(\mathbb{E}, \mathbb{K})} g(\sigma\tau)\sigma\tau(\alpha) = \beta \end{aligned}$$

Par conséquent $g(\sigma)$ s'écrit comme $g(\sigma) = \sigma(\beta^{-1})(\beta^{-1})^{-1}$ pour tout $\sigma \in \mathrm{Gal}(\mathbb{E}, \mathbb{K})$. Ceci démontre que tout 1-cocycle est un 1-cobord. □

Considérons maintenant une clôture algébrique $\overline{\mathbb{K}}$ de $\mathbb{K}$ et plaçons-nous dans l'extension galoisienne $\mathbb{K}_s/\mathbb{K}$ et fixons un entier $n \geq 1$, premier à la caractéristique de $\mathbb{K}$. Notons aussi μ_n le groupe des racines n-ièmes de l'unité, qui est contenu dans $\mathbb{K}_s$ par la remarque 3.2.

Corollaire 3.5.
Le premier groupe de cohomologie de l'extension $\mathbb{K}_s/\mathbb{K}$ est

$$H^1(\mathbb{K}, \mu_n) \cong \mathbb{K}^*/(\mathbb{K}^*)^n \ .$$

Démonstration. Notons $G := \mathrm{Gal}(\mathbb{K}_s, \mathbb{K})$. Alors on a une suite exacte de G-modules

$$0 \longrightarrow \mu_n \longrightarrow G_m \xrightarrow{n} G_m \longrightarrow 0$$

où la deuxième flèche est l'injection canonique de μ_n dans G_m. La surjectivité de la troisième flèche a été montrée dans le lemme 3.3 et son noyau est μ_n, d'où exactitude en G_m. La suite exacte longue correspondante en cohomologie est

$$0 \longrightarrow (\mu_n)^G \longrightarrow (G_m)^G \xrightarrow{n} (G_m)^G \xrightarrow{\partial^0} H^1(\mathbb{K}, \mu_n) \longrightarrow H^1(\mathbb{K}, G_m) \longrightarrow \cdots$$

$$\cdots \longrightarrow H^n(\mathbb{K}, G_m) \longrightarrow H^n(\mathbb{K}, G_m) \xrightarrow{\partial^n} H^{n+1}(\mathbb{K}, \mu_n) \longrightarrow \cdots \ .$$

On s'intéresse à la partie

$$(G_m)^G \xrightarrow{n} (G_m)^G \xrightarrow{\partial^0} H^1(\mathbb{K}, \mu_n) \longrightarrow H^1(\mathbb{K}, G_m)$$

où $(G_m)^G = \mathbb{K}^*$ puisque $(\mathbb{K}_s)^{\mathrm{Gal}(\mathbb{K}_s, \mathbb{K})} = \mathbb{K}$ (par la correspondance de Galois) et $H^1(\mathbb{K}, G_m) = 0$ par la proposition ci-dessus. Ainsi on a la suite exacte

$$\mathbb{K}^* \xrightarrow{n} \mathbb{K}^* \xrightarrow{\partial^0} H^1(\mathbb{K}, \mu_n) \longrightarrow 0 \ .$$

Par suite, la deuxième flèche est surjective. On conclut alors par exactitude et par le premier théorème d'isomorphisme que

$$H^1(\mathbb{K}, \mu_n) \cong \mathbb{K}^*/(\mathbb{K}^*)^n \ .$$

□

Remarque 3.6.
Le groupe μ_n étant contenu dans $\mathbb{K}_s^*$, on peut l'identifier à $\mathbb{Z}/n\mathbb{Z}$ en envoyant un générateur de $\mathbb{Z}/n\mathbb{Z}$ sur une racine primitive n-ième de l'unité. On a donc un moyen facile pour calculer $H^1(\mathbb{K}, \mathbb{Z}/n\mathbb{Z})$ puisqu'il est isomorphe, par le corollaire, au quotient

$$\mathbb{K}^*/(\mathbb{K}^*)^n \ .$$

CHAPITRE 4

Approche de la conjecture de Milnor

1. Définition de la K-théorie de Milnor

Commençons par fixer un corps que l'on note $\mathbb{F}$, pour des raisons purement calligraphiques qui s'expliquent d'elles-mêmes 8 lignes plus bas. Alors $(\mathbb{F}^*, \cdot)$ est un groupe abélien que l'on note additivement $K_1\mathbb{F}$ via l'isomorphisme canonique suivant :

$$\begin{array}{rccl} l: & (\mathbb{F}^*, \cdot) & \longrightarrow & (K_1\mathbb{F}, +) \\ & 1 & \longmapsto & 0 \\ & ab & \longmapsto & l(ab) = l(a) + l(b) \\ & a^{-1} & \longmapsto & l(a^{-1}) = -\,l(a) \end{array}$$

Définition 4.1 (Milnor).
La *K-théorie de Milnor* est l'anneau gradué

$$K_*\mathbb{F} = (K_0\mathbb{F}, K_1\mathbb{F}, K_2\mathbb{F}, K_3\mathbb{F}, \ldots)$$

défini comme le quotient de l'algèbre tensorielle

$$T\mathbb{F}^* = (\mathbb{Z}, K_1\mathbb{F}, K_1\mathbb{F} \otimes K_1\mathbb{F}, K_1\mathbb{F} \otimes K_1\mathbb{F} \otimes K_1\mathbb{F}, \ldots)$$

par l'idéal bilatère I engendré par les éléments de la forme $l(a) \otimes l(1-a)$ où $a \in \mathbb{F} \backslash \{0, 1\}$.

Précisions.

(1) L'idéal bilatère I est, par définition, composé de toutes les sommes d'éléments du type

$$l(b_1) \otimes \cdots \otimes l(b_n) \otimes l(a) \otimes l(1-a) \otimes l(c_1) \otimes \cdots \otimes l(c_m)$$

où $n, m \in \mathbb{N}$, $b_1 \ldots, b_m, c_1, c_n \in \mathbb{F}^*$ et $a \in \mathbb{F} \setminus \{0, 1\}$, c'est-à-dire par des sommes d'éléments de $T\mathbb{F}^*$ dont les termes sont des mots tensorisés de longueur au moins 2 et contiennent deux éléments successifs qui somment à 1 dans $\mathbb{F}$.

(2) Le terme homogène de degré $n \geq 2$, $K_n\mathbb{F}$ est le quotient de $(K_1\mathbb{F})^{\otimes n}$ par le sous-groupe engendré par les éléments du type $l(a_1) \otimes \cdots \otimes l(a_n)$ avec $a_i \in \mathbb{F}^*$ pout $i \in \mathbb{N}_n$ et $a_i + a_{i+1} = 1$ pour un $i \in \mathbb{N}_{n-1}$.

(3) La multiplication qui confère à $K_*\mathbb{F}$ sa structure d'anneau gradué est simplement la concaténation sur les élément de $T\mathbb{F}^*$ que l'on fait passer

au quotient. Pour vérification, on a effectivement que $(K_1\mathbb{F})^{\otimes i} \cdot (K_1\mathbb{F})^{\otimes j} \subset (K_1\mathbb{F})^{\otimes(i+j)}$ dans l'algèbre tensorielle $T\mathbb{F}^*$ pour tous $i, j \in \mathbb{N}$, donc cette inclusion passe sans problème au quotient pour donner $K_i\mathbb{F} \cdot K_j\mathbb{F} \subset K_{i+j}\mathbb{F}$ pour tous $i, j \in \mathbb{N}$. Par conséquent, lorsque cela ne porte pas à confusion, on ne note plus les symboles $\otimes$.

Cette définition de K-théorie de Milnor semble, de prime abord, sortir de nulle part, mais sa motivation vient d'un théorème de K-théorie algébrique classique appelé théorème de Matsumoto[1].

Théorème de Matsumoto.
Soit $\mathbb{F}$ un corps. Il existe une surjection

$$\mathbb{F}^* \times \mathbb{F}^* \twoheadrightarrow K_2^Q(\mathbb{F})$$

qui induit un homomorphisme surjectif de groupes abéliens

$$\mathbb{F}^* \otimes_{\mathbb{Z}} \mathbb{F}^* \twoheadrightarrow K_2^Q(\mathbb{F})$$

dont le noyau est le sous-groupe $< u \otimes v \,|\, u + v = 1 >$, de telle sorte que

$$K_2^Q(\mathbb{F}) \;\cong\; \mathbb{F}^* \otimes_{\mathbb{Z}} \mathbb{F}^* / < u \otimes v \,|\, u + v = 1 > \quad .$$

On voit ainsi que l'idée de Milnor était de généraliser cette construction de $K_2^Q(\mathbb{F})$ en degré plus grand, mais il est important de remarquer qu'en dehors du cas $n = 2$ on n'a pas, en général, $K_n^Q(\mathbb{F}) \cong K_n^M(\mathbb{F})$. Pour plus de précisions à ce sujet, ainsi qu'un énoncé de ce théorème en contexte, on peut se référer à [3].

Continuons avec quelques propriétés élémentaires découlant directement de la définition ci-dessus. Il ne s'agit, ici, en aucun cas, de commencer à développer cette théorie, mais d'un simple jeu algébrique sur les symboles formels, afin d'apprivoiser quelque peu le son "K-théorie de Milnor".

Propriétés 4.2.

(1) *Pour tout élément $a \in \mathbb{F}^*$, dans $K_1\mathbb{F}$ on a $l(a)l(-a) = 0$.*
(2) *Pour tout $a \in \mathbb{F}^*$, dans $K_2\mathbb{F}$ on a $l(a)^2 = l(-1)l(a) = l(a)l(-1)$.*
(3) *Pour tout $x \in K_m\mathbb{F}$ et pour tout $y \in K_n\mathbb{F}$ $(m, n \geq 1)$ on a $xy = (-1)^{mn}yx$.*
(4) *Pour tout $n \geq 2$, si $a_1 + \ldots + a_n \in \{0, 1\}$ et $a_i \in \mathbb{F}^*$, alors $l(a_1) \cdots l(a_n) = 0$.*

Démonstration.

(1) Pour $a = 1$ c'est banal car $l(1) = 0$. Pour $a \neq 1$ on écrit $(-a) = (1-a)(1-a^{-1})^{-1}$ et on calcule :
$l(a)l(-a) = l(a)[l(1-a) - l(1-a^{-1})] = l(a)l(1-a) + l(a^{-1})l(1-a^{-1}) = 0$
car chaque terme est nul dans le quotient.

[1] On utilise la notation K^Q pour se référer au groupes de K-théorie développés dans la théorie de D. Quillen et K^M pour se référer à la définition ci-dessus.

(2) On calcul $l(a)l(a) - l(-1)l(a) = (l(a) - l(-1))l(a) = l(-a)l(a) = 0$ par (1). De même pour la deuxième égalité.

(3) Il suffit de voir que pour $a, b \in \mathbb{F}^*$ on a $l(a)l(b) = -l(b)l(a)$. L'assertion suit par récurrence.

$$\begin{aligned} l(a)l(b) + l(b)l(a) &= 0 + l(a)l(b) + l(b)l(a) + 0 \\ &= l(a)l(-a) + l(a)l(b) + l(b)l(a) + l(b)l(-b) \\ &= l(a)[l(-a) + l(b)] + l(b)[(l(a) + l(-b)] = [l(a) + l(b)]l(-ab) \\ &= l(ab)l(-ab) = 0 \end{aligned}$$

(4) On procède par récurrence sur n. Pour $n = 2$, si $a_1 + a_2 = 1$, c'est évident par définition. Si $a_1 + a_2 = 0$, alors $a_2 = -a_1$ et c'est le point (1). Supposons donc $n \geq 3$ et l'assertion vérifiée pour tout $k < n$. Si $a_1 + a_2 = 0$ alors $a_3 + \ldots + a_n \in \{0, 1\}$, la conclusion suit par hypothèse de récurrence. Dans la cas où $a_1 + a_2 \neq 0$ on écrit $1 = a_1(a_1 + a_2)^{-1} + a_2(a_1 + a_2)^{-1}$. Par suite $(l(a_1) - l(a_1 + a_2))(l(a_2) - l(a_1 + a_2)) = 0$ et donc

$$\begin{aligned} 0 &= (l(a_1) - l(a_1 + a_2))(l(a_2) - l(a_1 + a_2))l(a_3) \cdots l(a_n) \\ &= l(a_1) \cdots l(a_n) - l(a_1)l(a_1 + a_2)l(a_3) \cdots l(a_n) \\ &\quad - l(a_1 + a_2)l(a_2)l(a_3) \cdots l(a_n) + l(a_1 + a_2)^2 l(a_3) \cdots l(a_n) \end{aligned}$$

où, puisque $a_1 + a_2$ est supposé non nul, les trois derniers termes sont nuls par hypothèse de récurrence, comme souhaité.

□

2. Lemme de Bass-Tate et Conjecture de Milnor

Replaçons-nous dans le contexte de la fin du chapitre précédent et plus précisément du corollaire 3.5, pour la valeur particulière $n = 2$. Considérons alors un corps $\mathbb{F}$ de caractéristique différente de 2, de clôture séparable $\mathbb{F}_s$ et de groupe de Galois $G = \mathrm{Gal}(\mathbb{F}_s, \mathbb{F})$.

Alors la suite exacte courte

$$0 \longrightarrow \{\pm 1\} \longrightarrow \mathbb{F}_s^* \xrightarrow{2} \mathbb{F}_s^* \longrightarrow 0$$

à laquelle on applique la suite exacte longue correspondante en cohomologie fournit le morceau exact

$$\mathbb{F}^* \xrightarrow{2} \mathbb{F}^* \xrightarrow{\partial} H^1(\mathbb{F}, \mathbb{Z}/2\mathbb{Z}) \longrightarrow 0$$

où l'on a identifié $\{\pm 1\}$ avec $\mathbb{Z}/2\mathbb{Z}$ et ∂ est l'homorphisme de connexion. On obtient finalement l'isomorphisme

$$\begin{array}{ccc} \mathbb{F}^*/(\mathbb{F}^*)^2 & \cong & H^1(\mathbb{F}, \mathbb{Z}/2\mathbb{Z}) \\ [a] & \longmapsto & \partial(a)\ . \end{array}$$

On tire maintenant de la section précédente qu'en passant à la notation additive, on a un isomorphisme canonique

$$\begin{array}{ccc} \mathbb{F}^*/(\mathbb{F}^*)^2 & \cong & K_1\mathbb{F}/2K_1\mathbb{F} \\ [a] & \longmapsto & [l(a)]\ . \end{array}$$

L'isomorphisme qui nous intéresse pour la conjecture de Milnor est par conséquent donné par

$$\begin{array}{ccc} K_1\mathbb{F}/2K_1\mathbb{F} & \cong & H^1(\mathbb{F},\mathbb{Z}/2\mathbb{Z}) \\ [l(a)] & \longmapsto & \partial(a)\ . \end{array}$$

Lemme de Bass-Tate.
L'isomorphisme de $K_1\mathbb{F}/2K_1\mathbb{F}$ dans $H^1(\mathbb{F},\mathbb{Z}/2\mathbb{Z})$ qui envoie $[l(a)] \longmapsto \partial(a)$ s'étend de façon unique en un homomorphisme d'anneaux gradués

$$h_{\mathbb{F}} :\ K_*\mathbb{F}/2K_*\mathbb{F} \longrightarrow H^*(\mathbb{F};\mathbb{Z}/2\mathbb{Z})\ .$$

Esquisse de la preuve.
Pour les degrés n supérieurs à 1, l'idée est de considérer l'homomorphisme

$$(K_1\mathbb{F})^{\otimes n} \longrightarrow H^1(\mathbb{F};\mathbb{Z}/2\mathbb{Z})^{\times n} \longrightarrow H^n(\mathbb{F};\mathbb{Z}/2\mathbb{Z})$$

où la première flèche envoie $a_1\otimes\cdots\otimes a_n$ sur $(\partial(a_1),\ldots,\partial(a_n))$ et la deuxième flèche est une succession de produits cup. On veut alors qu'en passant au quotient $K_n\mathbb{F}/2K_n\mathbb{F}$ les éléments du type $[l(b_1)\otimes\cdots\otimes l(b_r)\otimes l(a)\otimes l(1-a)\otimes l(c_1)\otimes\cdots\otimes l(c_m)]$ où $a\in\mathbb{F}\setminus\{0,1\}$ soient envoyés sur 0 dans $H^n(\mathbb{F};\mathbb{Z}/2\mathbb{Z})$.
La première remarque à faire est alors que vu les relations mises sur le quotient de $T\mathbb{F}^*$ dans la construction de $K_*(\mathbb{F})$, il suffit de vérifier que les relations $[l(a)l(1-a)] = 0$ dans $K_*\mathbb{F}/2K_*\mathbb{F}$ sont envoyées sur des relations valides $\partial(a)\partial(1-a) = 0$ dans $H^2(\mathbb{F},\mathbb{Z}/2\mathbb{Z})$.

La suite de la preuve utilise la notion de groupe de Brauer, qui n'est pas développée dans ce travail pour des raisons de manque de temps, c'est pourquoi je vais simplement donner les idées principales des arguments.

Pour commencer, on définit le groupe de Brauer $\mathrm{Br}(\mathbb{K})$ d'un corps $\mathbb{K}$ comme étant l'ensemble des classes d'équivalence des algèbres simples sur $\mathbb{K}$ de centre exactement $\mathbb{K}$, où deux telles algèbres A et B sont dites équivalentes s'il existe un anneau de division D sur $\mathbb{K}$ ainsi que des nombres naturels n, m tels que A (resp. B), est isomorphe à l'anneau des matrices $n\times n$ (resp. $m\times m$) à coefficient dans D. Un théorème de Brauer dit que pour une algèbre A avec les propriétés ci-dessus, il existe un unique tel couple (D,n).
La loi de groupe sur $\mathrm{Br}(\mathbb{K})$ est donnée par le produit tensoriel sur $\mathbb{K}$, l'élément neutre est donné par la classe de $\mathbb{K}$ et l'inverse d'une algèbre A par son opposé A^{opp}.

Dans [4], Chap. X, J.-P. Serre montre que le groupe $H^2(\mathbb{F},\mathbb{F}_s^*)$ s'identifie à $\mathrm{Br}(\mathbb{F})$. Alors par un argument sur la suite exacte longue en cohomologie similaire à celui de la preuve du corollaire 3.5, il montre aussi que $H^2(\mathbb{F},\mu_2)$ s'identifie au noyau $\mathrm{Br}_2(\mathbb{F})$ de la multiplication par 2 dans $\mathrm{Br}(\mathbb{F})$.

Le prochain pas est de montrer que pour $a, b\in\mathbb{F}^*$, l'élément $\partial(a)\partial(b)$ correspond dans $\mathrm{Br}(\mathbb{F})$ à l'algèbre des quaternions associée à a et b. La relation $\partial(a)\partial(1-a) = 0$ est alors déduite du fait que $\partial(a)\partial(1-a)$ correspond à l'algèbre des quaternions associée avec a et $1-a$ et que cette algèbre est nulle dans $\mathrm{Br}_2(\mathbb{F})$.

La conjecture de Milnor affirme plus précisément que l'homomorphisme décrit dans le lemme de Bass-Tate est un isomorphisme.

Conjecture de Milnor.
Soit $\mathbb{F}$ *un corps de caractéristique différente de* 2. *Alors* $K_*\mathbb{F}/2K_*\mathbb{F}$ *et* $H^*(\mathbb{F}, \mathbb{Z}/2\mathbb{Z})$ *sont isomorphes comme anneaux gradués.*

Une preuve de cette conjecture est donnée en 1996 par Vladimir Voevodsky dans un article qu'il n'a jamais publié. La preuve complète se trouve dans son article *Motivic cohomology with Z/2 coefficient* [7] publié en 2003.

Bibliographie

[1] Kenneth S. Brown. *Cohomology of groups*, volume 87 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1994. Corrected reprint of the 1982 original.

[2] John Milnor. *Algebraic K-theory and quadratic forms*, volume 9 of *Inventiones Mathematicae*. 1969/1970.

[3] Jonathan Rosenberg. *Algebraic K-theory and its applications*, volume 147 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1994.

[4] Jean-Pierre Serre. *Local fields*, volume 67 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1979. Translated from the French by Marvin Jay Greenberg.

[5] Jean-Pierre Serre. *Cohomologie galoisienne*, volume 5 of *Lecture Notes in Mathematics*. Springer-Verlag, Berlin, fifth edition, 1994.

[6] Stephen S. Shatz. *Profinite groups, arithmetic, and geometry*. Princeton University Press, Princeton, N.J., 1972. Annals of Mathematics Studies, No. 67.

[7] Vladimir Voevodsky. Reduced power operations in motivic cohomology. *Publ. Math. Inst. Hautes Études Sci.*, (98) :1–57, 2003.

[8] John S. Wilson. *Profinite groups*, volume 19 of *London Mathematical Society Monographs. New Series*. The Clarendon Press Oxford University Press, New York, 1998.

Index

anneau de groupe, 15

clôture séparable, 25
cochaînes, 18
compatible, 9

différentielles, 18

ensemble
  directif, 9

G-module, 16
  trivial, 16
  discret, 17
  profini, 17
  topologique, 17
groupe
  de Brauer, 32
  profini, 12
groupes
  de cohomologie, 18
  de cohomologie galoisienne, 26

homomorphisme
  induit, 19, 20
homomorphisme de connexion, 21

K-théorie de Milnor, 29

limite projective, 10

n-cobord, 18
n-cocycle, 18

suite exacte
  courte bien ajustée, 19
  longue, 19
système projectif, 9